INFOSEC Skills

Table of contents

Customize your training experience. ................................................................. 1

Live boot camps .............................................................................................................. 3
  Information security boot camps .................................................................................. 3
  AWS certification boot camps ..................................................................................... 6
  ISC2 certification boot camps ..................................................................................... 7
  CompTIA certification boot camps .............................................................................. 8
  ISACA certification boot camps .................................................................................. 9
  CMMC certification boot camps ............................................................................... 10
  IAPP certification boot camps .................................................................................. 11
  Cisco certification boot camps .................................................................................. 12
  Microsoft certification boot camps ........................................................................... 13
  Secure coding boot camps ......................................................................................... 14
  Other boot camps ..................................................................................................... 15

Self-paced certification training .................................................................................. 16

Train for your role ......................................................................................................... 19
  IT and security fundamentals ...................................................................................... 19
  Penetesting and vulnerability management ................................................................. 77
  Threat intelligence, incident response and forensics .................................................. 101
  Security architecture, engineering and management ................................................ 139
  Secure coding and DevSecOps .................................................................................... 232

Hands-on training ....................................................................................................... 265
  Labs ............................................................................................................................ 265
  Projects ....................................................................................................................... 305
  Training mapped to the NICE Workforce Framework for Cybersecurity ...................... 342
  Appendix: NICE knowledge and skill statements ....................................................... 369
INFOSEC Skills

Customize your training experience.
Choose how, when, and where you learn.

Technical training is often more than a development goal — it is a business requirement.
At Infosec, we recognize that your learning journey is unique. Whether you seek to pass your certification exam swiftly or explore a range of cybersecurity topics at your preferred pace, we provide flexible training options that align with your team’s commitments and training requirements.

Infosec Boot Camps
Infosec Boot Camps offer in-person and online live, interactive cybersecurity and IT certification training, led by industry experts with 10+ years of experience. Gain exam readiness and ask questions in a conducive environment. You can access on-demand resources on Infosec Skills for enhanced domain knowledge and hands-on experience.

* Exam Pass Guarantee*: Don't pass the exam on the first try? Get a second attempt free.

* 100% Satisfaction Guarantee*: Not 100% satisfied at the end of day one? You may enroll in a different online or in-person course.

* Knowledge Transfer Guarantee*: If an employee leaves within 3 months of obtaining certification, we provide tuition-free training for another employee.

* Does not apply to CMMC-AB boot camps

Infosec Skills Self-paced Training
Infosec Skills Self-paced Training is engineered to accommodate your busy schedule while providing a high-quality learning experience. With open enrollment, you have the freedom to start training whenever it suits you. Complete your training and obtain your certification at your own pace with extended course access.

* Certification-focus: On-demand* course materials can be accessed anytime, anywhere.

* Exam voucher included*: An easy way to redeem your voucher and take the exam.

* Expert support*: Asynchronous instructor assistance and a dedicated student advisory team give you the guidance you need to pass the exam.

Take control of your cybersecurity education and advance your skills at your own pace. Learn more about certification training with Infosec
Infosec Skills

Infosec Skills provides unlimited access to an extensive library of on-demand cybersecurity training, covering every security role from beginner to advanced. Assign pre-built learning plans or customize your own to ensure training is relevant and impactful and build confidence in your team's technical skills and knowledge.

**Extensive coverage:** Training is mapped to industry standards like the NICE Workforce Framework for Cybersecurity, MITRE ATT&CK® Matrix and DoD 8570/8140, as well as Infosec Skills Roles for pre-built role-based training.

**Guided hands-on labs:** Practice through hands-on experience and real-world scenarios to accelerate skills development and enhance knowledge retention.

**Measurable progress:** Assess knowledge and skills to pinpoint gaps and training needs, then measure progress with team reporting.

---

Try Infosec Skills for $1!
Use code “learnskills” when you sign up to get your first month for $1 — or start a trial for your whole team.
## Information security boot camps

Infosec Skills boot camps are engineered to match the way today’s cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you’ll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

<table>
<thead>
<tr>
<th>Boot camp</th>
<th>Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethical Hacking Dual Cert</td>
<td>5-day boot camp</td>
<td>Discover vulnerabilities before the bad guys do! Our most popular information security and hacking training goes in-depth into the techniques used by malicious, black-hat hackers with attention-getting lectures and hands-on labs. Certification training for CEH and PenTest+.</td>
</tr>
<tr>
<td>Advanced Ethical Hacking</td>
<td>5-day boot camp</td>
<td>Take your penetration testing skills to a new level! The industry’s most advanced ethical hacking training teaches you how to orchestrate and defend against advanced persistent threats (APT) attacks. Certification training for CPT and CEPT.</td>
</tr>
<tr>
<td>Penetration Testing 10-Day</td>
<td>10-day boot camp</td>
<td>Infosec’s penetration testing training — delivered in the form of a 10-day, boot-camp style course — is the information security industry’s most comprehensive penetration testing course available. Certification training for CEH, PenTest+, CPT and CEPT.</td>
</tr>
<tr>
<td>Mobile and Web Application Penetration Testing</td>
<td>5-day boot camp</td>
<td>Learn how to conduct penetration tests on mobile and web applications! This boot camp goes in-depth into the tools and techniques used to exploit and defend web and mobile apps with a combination of hands-on labs and expert instruction. Certification prep for CMWAPT.</td>
</tr>
<tr>
<td>Cloud Penetration Testing</td>
<td>5-day boot camp</td>
<td>Learn how to conduct penetration tests on cloud services and applications! This boot camp goes in-depth into the tools and techniques used to exploit and defend cloud infrastructure components with a combination of hands-on labs and expert instruction. Certification training for CCPT.</td>
</tr>
<tr>
<td>Red Team Operations Training</td>
<td>5-day boot camp</td>
<td>Do good by being bad in this exclusive Red Team Operations training designed to teach you to think like a cybercriminal, help you better defend your organization, and prepare you for the Certified Red Team Operations Professional exam.</td>
</tr>
<tr>
<td>Cyber Threat Hunting</td>
<td>3-day boot camp</td>
<td>Learn how to find, assess and remove threats from your organization in our Cyber Threat Hunting Boot Camp designed to prepare you for the Certified Cyber Threat Hunting Professional exam.</td>
</tr>
<tr>
<td>Incident Response and Networking Forensics</td>
<td>5-day boot camp</td>
<td>Learn how to detect and respond to security incidents! This popular boot camp builds your knowledge around network forensics and incident response with hands-on labs and expert instruction.</td>
</tr>
<tr>
<td>Computer Forensics</td>
<td>5-day boot camp</td>
<td>Learn how to investigate cybercrime! This boot camp goes in-depth into the tools, techniques and processes used by forensics examiners to find and extract evidence from computers. Certification training for CCFE.</td>
</tr>
<tr>
<td><strong>Mobile Forensics</strong></td>
<td><strong>Computer and Mobile Forensics</strong></td>
<td><strong>Data Recovery</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>2-day boot camp</td>
<td>7-day boot camp</td>
<td>5-day boot camp</td>
</tr>
<tr>
<td>Learn how to use mobile forensics to investigate cybercrime! Our Mobile Forensics Boot Camp builds your skills in a hands-on lab environment so you can apply what you learned the day you leave training. Certification training for CMFE.</td>
<td>Learn how to investigate cybercrime! This popular boot camp goes in-depth into the tools, techniques and processes used by forensics examiners to find and extract evidence from computers and mobile devices. Certification training for CCFE and CMFE.</td>
<td>Learn how to recover sensitive data from damaged or partially destroyed hard drives, solid-state media and removable media! A combination of hands-on labs and expert instruction builds your knowledge around data recovery and prepares you to become a Certified Data Recovery Professional (CDRP).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Reverse Engineering Malware</strong></th>
<th><strong>OT/ICS Certified Security Professional (ICSP)</strong></th>
<th><strong>NIST Cybersecurity Framework</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>5-day boot camp</td>
<td>5-day boot camp</td>
<td>3-day boot camp</td>
</tr>
<tr>
<td>Learn how to reverse engineer and analyze malware! Reverse engineering is a vitally important skill for today's expert security professional. Keep your organization safe by digging into the viruses, Trojans and rootkits being used by cybercriminals. Certification training for CREA.</td>
<td>Learn the best practices for securing Operational Technologies (OT) including Industrial Control Systems (ICS) and SCADA networks. This boot camp teaches you how to defend against both internal and external attackers to provide holistic security for critical industrial automation systems.</td>
<td>This three-day boot camp teaches you how to employ the NIST Cybersecurity Framework in order to better manage and reduce your organization's cybersecurity risk.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CSIS Top 20 Critical Security Controls</strong></th>
<th><strong>DOD Risk Management Framework</strong></th>
<th><strong>NERC Critical Infrastructure Protection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>5-day boot camp</td>
<td>4-day boot camp</td>
<td>5-day boot camp</td>
</tr>
<tr>
<td>This boot camp helps you master the 20 Important Security Controls as published by the Center for Strategic and International Studies (CSIS).</td>
<td>Infosec's Risk Management Framework (RMF) Boot Camp is a four-day course in which you delve into the IT system authorization process and gain an understanding of the Risk Management Framework.</td>
<td>This five-day boot camp provides a detailed overview of and teaches how to comply with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards.</td>
</tr>
<tr>
<td><strong>Cybersecurity Foundations</strong></td>
<td><strong>EC-Council's Certified Network Defender</strong></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>3-day boot camp</td>
<td>5-day boot camp</td>
<td></td>
</tr>
<tr>
<td>Learn topics ranging from foundational security concepts and principles to specific topics like common security tools and technologies, key security roles, common attack types, and best practice security controls or mitigation strategies. A comprehensive but beginner-friendly training for those looking to get started or expand their cybersecurity expertise.</td>
<td>Learn to defend your organization's network in five days! This course will cover network defense techniques, incident response strategies, network perimeter and data protection.</td>
<td></td>
</tr>
</tbody>
</table>
Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

**AWS Certified Solutions Architect Training Boot Camp**

3-day boot camp

Utilize AWS services and frameworks to create architectures! This course will cover the fundamentals of AWS architectural principles, including AWS Command Line Interface (CLI) and Virtual Private Cloud (VPC) subsets.

**AWS Certified Security Engineer Training Boot Camp**

3-day boot camp

Learn to mitigate threats and secure AWS Cloud services! With this course, you will understand AWS incident response, security and monitoring.

**AWS Certified Cloud Operations Administrator Training Boot Camp**

3-day boot camp

Implement and operate AWS security systems! This course will cover the basics of cloud networking concepts, cloud architectural requirements, monitoring, logging and troubleshooting systems.

**AWS Certified DevOps Engineer Training Boot Camp**

3-day boot camp

Learn to design and implement AWS infrastructure! This course will cover software development and infrastructure within AWS systems, including Git repositories and CI/CD pipelines.
# ISC2 certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

<table>
<thead>
<tr>
<th>Boot Camp</th>
<th>Description</th>
</tr>
</thead>
</table>
| **CISSP** | 7-day boot camp  
Take your career to the next level by earning one of the most in-demand security certifications. Infosec's Certified Information Systems Security Professional (CISSP) training is more than just a live boot camp. You'll get everything you need to successfully prepare for, earn and maintain your CISSP certification. |
| **CGRC (previously - CAP)** | 3-day boot camp  
Learn how to maintain and authorize information systems within the NIST Risk Management Framework (RMF). You'll leave this boot camp with the knowledge and domain expertise needed to pass the Certified in Governance, Risk and Compliance (CGRC) exam the first time you take it. |
| **CCSP** | 5-day boot camp  
Learn how to design, manage and secure assets in the cloud. This boot camp teaches you best practices around cloud data, applications and infrastructure — and prepares you to become a Certified Cloud Security Practitioner (CCSP). |
| **CSSLP** | 5-day boot camp  
Become a Certified Secure Software Lifecycle Professional (CSSLP). You'll leave this boot camp with the knowledge and domain expertise needed to pass the CSSLP exam the first time you take it. |
| **ISSAP** | 4-day boot camp  
Take your CISSP to the next level by earning your ISSAP concentration. The ISSAP builds on your CISSP knowledge and validates your expertise in developing, designing and analyzing security solutions. |
| **ISSEP** | 4-day boot camp  
Take your CISSP to the next level by earning your ISSEP concentration. The ISSEP builds on your CISSP knowledge and validates your ability to practically apply systems engineering principles and processes to develop secure systems. |
| **ISSMP** | 4-day boot camp  
Take your CISSP to the next level by earning your ISSMP concentration. The ISSMP builds on your CISSP knowledge and validates your expertise in establishing, presenting and governing information security programs. |

Use code “learnskills” to get 30 days for $1  
[GET STARTED]
## CompTIA certification boot camps

Infosec Skills boot camps are engineered to match the way today’s cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you’ll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

<table>
<thead>
<tr>
<th>Boot camps</th>
<th>Learning paths</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>Self-paced</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-day boot camp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Don’t be afraid, beginners! This entry-level boot camp provides the most</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>comprehensive approach to earning your CompTIA A+ certification. A+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>certification leads to career advancement, personal improvement,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>skills enhancement and higher salaries.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-day boot camp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Learn how to configure, troubleshoot and oversee networks! This boot</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>camp provides the most comprehensive approach to earning your CompTIA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network+ certification, one of the most popular certifications an IT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>professional can attain.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-day boot camp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infosec's authorized CompTIA Security+ Boot Camp teaches you information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security theory and reinforces that theory with hands-on exercises to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>help you learn by doing. You will learn how to configure and operate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>many different technical security controls — and leave prepared to pass</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>your Security+ exam.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CySA+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-day boot camp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Learn how to use behavioral analytics to prevent, detect and combat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cyber threats! This boot camp provides the most comprehensive approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to earning CompTIA's intermediate-level Cybersecurity Analyst (CySA+)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>certification.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethical Hacking Dual Cert</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-day boot camp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discover vulnerabilities before the bad guys do! Our most popular</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>information security and hacking training goes in-depth into the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>techniques used by malicious, black-hat hackers with attention-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>getting lectures and hands-on labs. Certification training for CEH and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PenTest+.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CASP+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-day boot camp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take your cybersecurity skills to the next level by becoming a CompTIA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Security Practitioner (CASP+). You’ll learn the “how to” of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>implementing cybersecurity solutions and leave with one of the industries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>most respected certifications.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-day boot camp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infosec's authorized CompTIA Linux+ Boot Camp is a hands-on training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>covering every important facet of the world’s most popular open</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>source operating system. You’ll learn hardware and system configuration,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system maintenance, troubleshooting and diagnostics, security, scripting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and more.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-day boot camp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adopting a vendor-neutral approach, this course provides you with an</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>understanding of essential cloud concepts needed to start or advance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>your career working with cloud technologies. You’ll have the knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>required to pass your Cloud+ exam, the only cloud-focused certification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>approved for DoD 8570.01-M.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-day boot camp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>With data playing an ever-increasing role in today’s business and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>technology landscape, the demand for skilled data professionals is higher</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>than ever. Upon completion of this course, you’ll have the knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>needed to pass the CompTIA Data+ exam as well as valuable data skills</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>for nearly any industry or role.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# ISACA certification boot camps

Isoc Sec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

## CISA

5-day boot camp

Isoc Sec's Certified Information Systems Auditor (CISA) Boot Camp is a five-day training focused on preparing you for the ISACA CISA exam. You'll leave with the knowledge and domain expertise needed to pass the CISA exam the first time you take it.

## CISM

5-day boot camp

Isoc Sec's Certified Information Security Manager (CISM) Boot Camp is a five-day training focused on preparing you for the ISACA CISM exam. You'll leave with the knowledge and domain expertise needed to pass the CISM exam the first time you take it.

## CRISC

3-day boot camp

Learn the principles and practices of IT governance. Build your knowledge around how IT risk relates to your organization and prepare to earn your Certified in Risk and Information Systems Control (CRISC) certification.

## CGEIT

4-day boot camp

Isoc Sec's Certified in the Governance of Enterprise IT (CGEIT) Boot Camp is a four-day training focused on preparing you for the ISACA CGEIT exam. You'll leave with the knowledge and domain expertise needed to pass the CGEIT exam the first time you take it.

## CDPSE

5-day boot camp

Isoc Sec's Certified Data and Privacy Solutions Engineer (CDPSE) Boot Camp offers a natural progression for IT professionals who are tasked with designing, implementing and managing the technology that stores, collects and transports PII, as well as ensuring that privacy is considered in the design.

## COBIT 2019 Foundation

3-day boot camp

Take the first step toward strategic roles in GRC and IT governance with the Control Objectives for Information and Related Technology (COBIT) framework! Plus, the knowledge and skills gained through a deeper understanding of the COBIT framework will prepare you for the COBIT Foundation Certificate exam.

## Implementing the NIST CSF Using COBIT 2019

2-day boot camp

Build on your expertise in not just understanding NIST and COBIT® 2019, but also in implementing the globally accepted frameworks together. Gain the know-how to integrate cybersecurity standards and enterprise governance of Information & technology (EGIT).

## COBIT 2019 Design and Implementation

4-day boot camp

Build on your expertise in not just understanding COBIT®, but also in implementing the globally accepted framework to maximize the value of enterprise information and technology. Gain the know-how to design and implement an effective IT governance system and run governance improvement programs.
CMMC certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

**Certified CMMC 2.0 Professional Boot Camp**

5-day boot camp

The Certified CMMC 2.0 Professional (CCP) is the first step to becoming an assessor. It certifies you as a valuable resource for consulting agencies and organizations seeking CMMC guidance.

**Certified CMMC 2.0 Assessor Boot Camp**

5-day boot camp

Take your career to the next level by becoming one of the first Certified CMMC Assessors (CCA). The CMMC career path contains three levels of assessors based on the different maturity levels.
IAPP certification boot camps

Infosec Skills boot camps are engineered to match the way today’s cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you’ll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

CIPP/US

2-day boot camp
Infosec’s two-day authorized CIPP/US boot camp provides privacy professionals with essential knowledge and understanding of important U.S. laws, regulations and enforcement models.

CIPP/E

2-day boot camp
Infosec’s two-day authorized CIPP/E boot camp provides privacy professionals with essential knowledge and understanding of important European Union laws, regulations and enforcement models.

CIPM

2-day boot camp
Infosec’s two-day authorized CIPM boot camp focuses on the development, implementation and management of privacy policies and frameworks.

CIPT

2-day boot camp
Infosec’s two-day authorized CIPT boot camp helps you gain a deep understanding of the need of privacy in the IT environment and the common challenges enterprises are facing when factoring data privacy into their products and services.

CIPP/US and CIPT

4-day boot camp
Infosec’s four-day authorized CIPP/US and CIPT boot camp provides privacy professionals with essential knowledge and understanding of both important U.S. laws, regulations and enforcement models as well as the common challenges enterprises are facing when factoring data privacy into their products and services.

CIPP/US and CIPM

4-day boot camp
Infosec’s four-day authorized CIPP/US and CIPM boot camp provides privacy professionals with both essential knowledge and understanding of important U.S. laws, regulations and enforcement models as well as information on the development, implementation and management of privacy policies and frameworks.

CIPP/US, CIPT and CIPM

6-day boot camp
Infosec’s six-day authorized CIPP/US, CIPT and CIPM boot camp provides privacy professionals with the essential knowledge and understanding of U.S. privacy laws, technology concerns, and privacy policies and frameworks necessary to successfully pass all three certification exams.
Cisco certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

### CCNA Dual Cert

7-day boot camp

Infosec's authorized CCNA Dual Certification Boot Camp helps you build your knowledge of networking and provides hands-on experience installing, configuring and operating network devices — all while preparing you to earn two Cisco certifications.

### CCNA

5-day boot camp

Infosec's authorized CCNA Boot Camp helps you build your knowledge of networking and provides hands-on experience installing, configuring and operating network devices.

### Cisco Certified CyberOps Associate

2-day boot camp

Infosec's authorized Cisco Certified CyberOps Associate Boot Camp is an intense two-day training designed to build a foundation of skills around cybersecurity operations. You will acquire the skills necessary to begin a career working with associate-level cybersecurity analysts within a security operations center (SOC).

### CCNP Enterprise

10-day boot camp

Take your networking professional career to the next level! Infosec's authorized CCNP Enterprise Boot Camp is a comprehensive 10-day training that prepares you to earn one of Cisco's most prestigious certifications.
# Microsoft certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

## Microsoft Azure Dual Cert
7-day boot camp

Learn how to implement, monitor, maintain and secure Microsoft Azure solutions! This boot camp provides hands-on experience and prepares you to earn two Microsoft certifications: Azure Administrator Associate and Azure Security Engineer Associate.

## Microsoft Azure Configuring Windows Server Hybrid Advanced Services Boot Camp
4-day boot camp

Learn how to configure advanced Windows Server services using on-premises, hybrid and cloud technologies! This boot camp provides hands-on experience and prepares you to earn your Microsoft Azure AZ-801 certification.

## Microsoft Azure Administering Windows Server Hybrid Core Infrastructure Boot Camp
4-day boot camp

Learn how to implement and manage on-premises and hybrid solutions such as identity, management, computer, networking and storage in a Windows Server hybrid environment! This boot camp provides hands-on experience and prepares you to earn your Microsoft Azure AZ-800 certification.

## Microsoft Azure Administrator Training Boot Camp
4-day boot camp

Learn how to implement, monitor, maintain and secure Microsoft Azure solutions! This boot camp provides hands-on experience and prepares you to earn your Microsoft Azure Administrator certification.

## Microsoft Azure Fundamentals Training Boot Camp
1-day boot camp

This course helps new and established IT professionals learn the key concepts, components and benefits of cloud computing with Microsoft Azure.
Secure coding boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

Secure Coding for C/C++
2-day boot camp
Learn the most common programming bugs and their practical mitigation techniques through hands-on exercises that provide full understanding of the root causes of security problems.

Secure Coding for Java
3-day boot camp
Learn how to develop Secure Java applications. This boot camp is designed for developers and designers of Java applications that require effective, real-world secure programming skills they can implement immediately at the workplace.

Secure Coding in PHP
3-day boot camp
Learn how to make PHP applications resistant to attacks from security issues around JavaScript, Ajax and HTML5. This boot camp is designed for PHP developers that require effective, real-world, secure programming skills they can implement immediately at the workplace.

Secure Coding for .NET Training
3-day boot camp
Learn how to develop Secure .NET applications. This boot camp is designed for ASP.NET and C# developers that require effective, real-world, secure programming skills they can implement immediately at the workplace.
Other boot camps

Infosec Skills boot camps are engineered to match the way today’s cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you’ll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

**Project Management Professional (PMP)**

4-day boot camp

Infosec’s Project Management Professional (PMP) Boot Camp provides a quick and convenient approach to PMP certification. You’ll gain the knowledge needed to pass the PMP exam and the project management education hours required for certification all in one boot camp.

**Infosec RHCSA Training Boot Camp**

5-day boot camp

Infosec’s RHCSA Boot Camp helps you gain the essential knowledge and hands-on skills to leverage Linux for your organizational advantage.

Don’t see what you need?

Dozens of other IT and security boot camps are available for private onsites or online group training. 
[Contact us](#) for more information.
Infosec Skills Self-paced Training

Can't take time off? Infosec Skills Self-Paced Training is engineered to accommodate your busy schedule while providing a high-quality learning experience. With open enrollment, you have the freedom to begin your training whenever it suits you. Extended access to the course materials fits the training seamlessly into your routine. Our knowledgeable instructors are available to answer your questions offline, and a dedicated student advisory team is just a message away to support your learning journey.

<table>
<thead>
<tr>
<th>Course Title</th>
<th>Course Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>AZ-104: Microsoft Azure Administrator</td>
<td>60 hours</td>
</tr>
<tr>
<td>AZ-500: Microsoft Azure Security Technologies</td>
<td>50 hours</td>
</tr>
<tr>
<td>AZ-900: Microsoft Azure Fundamentals</td>
<td>40 hours</td>
</tr>
<tr>
<td>Certified AWS Cloud Practitioner</td>
<td>40 hours</td>
</tr>
<tr>
<td>Certified AWS Developer</td>
<td>40 hours</td>
</tr>
<tr>
<td>Certified AWS Solutions Architect</td>
<td>60 hours</td>
</tr>
<tr>
<td>Certified AWS SysOps Administrator</td>
<td>60 hours</td>
</tr>
<tr>
<td>Cloud Engineer Training</td>
<td>220 hours</td>
</tr>
<tr>
<td>CompTIA A+</td>
<td>290 hours</td>
</tr>
</tbody>
</table>

Use code “learnskills” to get 30 days for $1
<table>
<thead>
<tr>
<th>CompTIA Network+</th>
<th>CompTIA Security+</th>
<th>CompTIA Advanced Security Practitioner (CASP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Course</td>
<td>110 hours**</td>
<td>**Course</td>
</tr>
<tr>
<td>A CompTIA Network+ certification course teaches you the basics of networking and prepares you for the certification exam (N10-008). You’ll learn about network design, security, routing and switching, cloud computing, IPv6, and forensics, and have hands-on experience with a lab simulator.</td>
<td>Learn a broad range of security topics, including threat management, identity management, access control, cryptography, and network security. This course will teach you everything you need to take and successfully pass the CompTIA Security+ certification exam.</td>
<td>Prepare for CompTIA Advanced Security Practitioner (CASP) certification, one of the most valuable certifications in the IT field.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CompTIA Cloud+</th>
<th>CompTIA Linux+</th>
<th>Certified Kubernetes Administrator (CKA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Course</td>
<td>75 hours**</td>
<td>**Course</td>
</tr>
<tr>
<td>Cloud computing is a rapidly growing field. This online course is designed for beginners and covers everything you need to know to pass the CompTIA Cloud+ certification exam and pursue a career in cloud computing.</td>
<td>This Linux training course covers operating, maintaining, and troubleshooting Linux operating systems in a systems administrator role.</td>
<td>This course will teach you how to use the container management platform used by companies like Google to manage their application infrastructure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cisco CCNA Certification Training</th>
<th>Cisco CCNP Enterprise: ENCOR &amp; ENARSI</th>
<th>Certified Information Security Manager (CISM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Course</td>
<td>225 hours**</td>
<td>**Course</td>
</tr>
<tr>
<td>Take the next step in your IT career by preparing for the Cisco CCNA certification exam. You’ll master certification-based topics for networking essentials, so you can implement and administer Cisco solutions. Exam voucher included in enrollment.</td>
<td>This course is intended for network engineers, system engineers, network administrators, and those looking to attain their CCNP Enterprise certification.</td>
<td>Prepare for the Certified Information Security Manager (CISM) certification and gain skills in four key areas: management, risk management and compliance, program development, and incident management.</td>
</tr>
<tr>
<td>Certification</td>
<td>Course Duration</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Certified Information Systems Auditor (CISA)</strong></td>
<td>75 hours</td>
<td>This online CISA training course will prepare you for the five key domains: auditing, governance, implementation, management, and protection.</td>
</tr>
<tr>
<td><strong>Certified Information Systems Security Professional (CISSP)</strong></td>
<td>150 hours</td>
<td>In the online world, information security is crucial for all organizations. Earning a CISSP certification can help cyber security professionals stay ahead in this field.</td>
</tr>
<tr>
<td><strong>Certified Ethical Hacker v.12</strong></td>
<td>100 hours</td>
<td>Certified Ethical Hacker CEH v12 will teach you the latest commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization.</td>
</tr>
<tr>
<td><strong>Certified Penetration Testing Professional (CPENT)</strong></td>
<td>200 hours</td>
<td>Learn how to perform an effective penetration test in an enterprise network environment that must be attacked, exploited, evaded, and defended using the EC-Council's Certified Penetration Tester (CPENT) program.</td>
</tr>
<tr>
<td><strong>Linux Foundation Certified System Administrator</strong></td>
<td>90 hours</td>
<td>This course will teach you the critical skills and knowledge needed to take the Linux Foundation Certified System Administrator (LFCS) exam—including all things involved with the Linux operating system.</td>
</tr>
<tr>
<td><strong>Computer Hacking Forensics Investigator (CHFI)</strong></td>
<td>100 hours</td>
<td>This course prepares for Computer Hacking Forensics Investigator (CHFI) certification exam. You will master the security discipline of digital forensics from a vendor-neutral perspective.</td>
</tr>
<tr>
<td><strong>ITIL 4 Foundation</strong></td>
<td>20 hours</td>
<td>Prepare for the ITIL 4 Foundation exam, a key certification for professionals managing modern IT-enabled services.</td>
</tr>
</tbody>
</table>
IT and security fundamentals covers both broad information technology training and entry-level cybersecurity training. It is designed for those building a baseline of IT and security skills, as well as individuals who are looking to transition roles from IT and networking into cybersecurity.

Active Directory with Windows Server 2016

The Active Directory with Windows Server 2016 certification path builds your knowledge of Active Directory and prepares you to pass the Identity with Windows Server 2016 (70-742) certification exam.

Skill Assessment
Skill assessment | 20 questions
See how your Active Directory with Windows Server 2016 skills stack up against other professionals in your field.

Install and Configure Active Directory Domain Services
Course | 2 hours 10 minutes
Get started with Active Directory through this course on installing and configuring Active Directory Domain Services. Take a look at domain controllers, configuration options, managing groups and accounts and more.

NICE Knowledge and Skill Statements:
K0158, K0332, K0608, S0043, S0067, S0158, S0267

Managing and Maintaining Active Directory Domain Services
Course | 1 hour 36 minutes
Explore the intricacies of managing and maintaining AD DS with this course covering MSAs, advanced deployments and more.

NICE Knowledge and Skill Statements:
K0157, K0158, K0608, S0043, S0067, S0267, S0354

Create and Manage Group Policy
Course | 1 hour
Keep a tight rein on your system with this course on creating and managing group policies. Explore GPOs, working with templates, preferences and item-level targeting and more.

NICE Knowledge and Skill Statements:
K0158, K0608, S0043, S0067

Implement Active Directory Certificate Services
Course | 52 minutes
In this course on implementing Active Directory Certificate Services, you'll get to grips with the intricacies of certificates and certificate administration, installation, enrollment and more.

NICE Knowledge and Skill Statements:
K0019, K0056, K0403, S0043, S0067, S0138

Implement Active Directory Federation Services
Course | 36 minutes
Round out your study with this course on implementing Active Directory Federation Services, covering AD FS installation, multi-factor authentication and more.

NICE Knowledge and Skill Statements:
K0007, K0056, K0336, S0043, S0067, S0367
Advanced Intrusion Detection

This course will provide you with the practical, hands-on knowledge you need to fully understand the methodology behind intrusion detection and craft meaningful detection rules and logic.

Skill Assessment

Skill assessment | 20 questions

See how your intrusion detection skills stack up against other professionals in your field.

Advanced Intrusion Detection project

Project | 2 hours 20 minutes

This project consists of reviewing an alert for suspicious AV/Endpoint activity and connecting the dots between the event that occurred and what actions need to be taken to remediate it.

NICE Knowledge and Skill Statements:
K0001, K0004, K0005, K0046, K0332, K0405, K0473, S0025, S0084, S0120, S0192, S0280

Intrusion detection techniques and methods

Course | 50 minutes

We will go over the basics of intrusion detection, why it is needed for every environment, the various types (network. versus host-based) and techniques for crafting detections.

Home Lab Setup

Course | 1 hour 9 minutes

This course is a look at setting up a home detection lab.

NICE Knowledge and Skill Statements:
K0004, K0318, K0324, K0610, S0243

Network- versus host-based detection

Course | 38 minutes

This section provides a deeper dive into host- versus network-based intrusion detection.

NICE Knowledge and Skill Statements:
K0001, K0004, K0005, K0046, K0332, K0405, K0473, S0025, S0084, S0120, S0192, S0280

Anomaly detection

Course | 34 minutes

We will go over the basics of anomaly detection and how it can be used with other detection methods (signature) to identify malicious activity within your environment.

NICE Knowledge and Skill Statements:
K0001, K0004, K0005, K0046, K0332, K0343, K0405, K0473, S0025, S0280
### The ATT&CK Matrix and threat intel

**Course | 35 minutes**

In this course, students explore the MITRE ATT&CK Framework.

**NICE Knowledge and Skill Statements:**
- K0004, K0005, K0047, K0409, K0456, K0460, K0466,
- K0467, K0577, S0147

### Advanced detection through deception technology

**Course | 34 minutes**

This section will explore the world of deception technology and how it can be used to build additional detections.

**NICE Knowledge and Skill Statements:**
- K0001, K0004, K0005, K0046, K0324, K0473,
- K0487, K0561, S0084, S0120, S0192, S0280

### Data management

**Course | 1 hour 7 minutes**

In this course, we will discuss the importance of organizing how to collect, store and process the data you will eventually use for detections.

**NICE Knowledge and Skill Statements:**
- K0043, K0142, K0377, K0382, K0386, K0387, K0389,
- K0404, K0500, K0567, S0017, S0126, S0183, S0217,
- S0218, S0252

### Tactical data

**Course | 51 minutes**

In this course, the student expands on the topic of data management to explore tactical data.

**NICE Knowledge and Skill Statements:**
- K0046, K0054, K0110, K0324, S0025, S0084, S0187
AWS Certified Security Specialist

In this learning path, we will not only review key items of every exam domain but go hands-on with the AWS services that you must know to pass the exam. This course is meant to reinforce the material the exam expects you to know to pass.

AWS Certified Security Specialist Practice exam
Practice Exam | 64 questions
Prepare for your AWS Certified Security Specialist exam and test your domain knowledge.

AWS Certified Security Specialist introduction
Course | 22 minutes
We will look at the exam blueprint and setting up an AWS Free-tier account for the purposes of the course.

Infrastructure security in AWS
Course | 1 hour 10 minutes
In this course, we will review all infrastructure security areas in AWS that you will need to know for the exam.

NICE Knowledge and Skill Statements:
K0001, K0004, K0005, K0033, K0104, K0113, K0194, K0395, K0417, K0470, K0516, K0565, S0059, S0073, S0077, S0121

IAM security in AWS
Course | 1 hour 6 minutes
In this course, we will review all aspects of IAM security for the exam. Having an in-depth understanding of IAM is essential.

NICE Knowledge and Skill Statements:
K0001, K0004, K0005, K0007, K0056, K0065, K0158, K0194, K0336, S0031, S0073

Data protection in AWS
Course | 1 hour
In this course, we will review methods of data protection in AWS and the best way to use native AWS services to increase security.

NICE Knowledge and Skill Statements:
K0003, K0004, K0044, K0196, K0222, K0260, K0261, K0262, K0504, K0524, S0147

Logging and monitoring in AWS
Course | 36 minutes
In this course, we will review logging and monitoring. We will also discuss what aspects of this section will be most prevalent on the exam.
Incident response in AWS

Course | 25 minutes

In this course, we will review potential incident response scenarios that you will come across on the exam.

AWS Certified Security Specialist Exam tips

Course | 11 minutes

In this course, we will review exam resources that everyone should use while preparing them for the exam.
AWS Essentials & Solutions Architect Associate

The AWS Essentials & Solutions Architect Associate certification path begins by building your knowledge of essential AWS terminology, concepts and services before preparing you to pass the AWS Certified Solutions Architect - Associate exam.

**Skill Assessment**

Skill assessment | 20 questions

See how your AWS Essentials & Solutions Architect Associate skills stack up against other professionals in your field.

**AWS Essentials Foundations and Services**

Course | 1 hour 14 minutes

Start off strong with a course on AWS foundations and services such as account creation, bucket creation, using the management console and more.

NICE Knowledge and Skill Statements:
K0373, S0073

**AWS Essentials Security and Costs**

Course | 39 minutes

Explore AWS cost and security with this course and prepare yourself for your certification journey.

NICE Knowledge and Skill Statements:
K0056, S0073

**About AWS and the Exam**

Course | 53 minutes

This course introduces Amazon Web Services (AWS) and discusses the AWS CSA-A exam.

NICE Knowledge and Skill Statements:
S0073

**AWS Cloud Services Overview**

Course | 1 hour 8 minutes

This course provides a detailed overview of AWS Cloud Services.

NICE Knowledge and Skill Statements:
K0194, S0073

**AWS Storage Design**

Course | 2 hours 38 minutes

Keep your organization organized with this course on storage services in AWS.

NICE Knowledge and Skill Statements:
K0038, K0097, K0622, S0073
<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Table of contents</th>
<th>Self-paced training</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
</table>

### Virtual Private Cloud (VPC)

**Course | 1 hour 31 minutes**

This course covers the concept and configuration of the Virtual Private Cloud (VPC).

**NICE Knowledge and Skill Statements:** K0104, S0059, S0073

### Compute Services Design

**Course | 39 minutes**

This course introduces EC2 — the AWS cloud computing service.

**NICE Knowledge and Skill Statements:** K0194, S0073

### Compute Services Implementation

**Course | 1 hour 4 minutes**

This course walks through launching and configuring EC2 instances.

**NICE Knowledge and Skill Statements:** K0073, S0073

### Compute Services Management

**Course | 70 minutes**

Explore the ins and outs of the ongoing EC2 instance management.

**NICE Knowledge and Skill Statements:** K0073, S0073

### Identity and Access Management (IAM)

**Course | 1 hour 26 minutes**

Learn how to control access to your AWS account and the services running in it with Identity and Access Management (IAM).

**NICE Knowledge and Skill Statements:** K0007, K0056, K0065, S0031, S0073

### IAM Best Practices

**Course | 1 hour**

Explore practical application of AWS Identity and Access Management (IAM).

**NICE Knowledge and Skill Statements:** K0007, K0056, K0065, S0031, S0073

### Auto Scaling Solutions

**Course | 51 minutes**

Explore the options for dynamically growing or shrinking a set of servers in AWS.

**NICE Knowledge and Skill Statements:** K0073, S0073

### Virtual Network Services

**Course | 50 minutes**

This course focuses on DNS configuration and also explores Access Control Lists (ACLs) and flow logs.

**NICE Knowledge and Skill Statements:** K0073, K0332, K0565, S0073

### AWS Application Deployment

**Course | 2 hours 24 minutes**

This course covers an array of AWS application and deployment services, from Lambda to Trusted Advisor.

**NICE Knowledge and Skill Statements:** K0049, K0107, K0487, K0561, S0073, S0084
### AWS Database Design

**Course | 1 hour 7 minutes**

Learn how to architect and secure databases in AWS.

**NICE Knowledge and Skill Statements:**
K0073, K0373, K0419, K0420, S0073

### Database Deployment

**Course | 57 minutes**

Practice creating and managing databases in AWS in this hands-on course.

**NICE Knowledge and Skill Statements:**
K0073, K0373, K0419, K0420, S0073

### Additional AWS Services

**Course | 1 hour 17 minutes**

Get familiar with various AWS services developed to serve specific needs.

**NICE Knowledge and Skill Statements:**
K0194, S0073

### Operational Excellence with AWS

**Course | 1 hour 17 minutes**

This scenario-based course illustrates the concepts of operational excellence.

**NICE Knowledge and Skill Statements:**
K0292, S0027, S0073
Cisco Certified Network Associate (CCNA)

The newest version of the Cisco Certified Network Associate (CCNA) covers the latest in the world of Cisco routing and switching. You’ll explore network fundamentals such as routers and endpoints and take a closer look at network access, IP connectivity, IP services, security fundamentals and automation and programmability.

### CCNA Practice Exam

Practice Exam | 569 questions
---
Prepare for your CCNA exam and test your domain knowledge.

### Networking Cyber Range

Cyber range | 36 labs
---
Gain practical experience and develop your real-world networking skills through 36 hands-on labs in the Networking Cyber Range.

**NICE Knowledge and Skill Statements:**
S0007, S0041, S0067, S0097, S0151, S0275

### Network Fundamentals

Course | 4 hours 11 minutes
---
Dig into network components, network topology architectures, interface and cabling (and issues with them), IPv6, IP parameters and more. You’ll explore switching concepts and take a look at the basics of virtual machines.

**NICE Knowledge and Skill Statements:**
K0011, K0034, K0057, K0061, K0108, K0113, K0174, K0221, K0255, K0393, K0395, K0417, K0471, K0486, K0489, K0491, K0516, K0555, K0556, K0565, K0610

### Network Access

Course | 3 hours 13 minutes
---
Take a look at VLANs, inter-switch connectivity, Layer 2 discovery protocols and EtherChannel. You’ll also learn Cisco Wireless Architectures and AP nodes, describe different types of connections and much more.

**NICE Knowledge and Skill Statements:**
K0001, K0007, K0108, K0113, K0221, K0375, K0395, K0446, K0516, K0565, K0600, K0614

### IP Connectivity

Course | 2 hours 16 minutes
---
Explore the different concepts and challenges of IP connectivity: from interpreting the components of a routing table to configuring and verifying IPv4 and IPv6 static routing, exploring first-hop redundancy protocol and more!

**NICE Knowledge and Skill Statements:**
K0001, K0011, K0221, K0296, K0395, K0417, K0470, K0471, K0516, K0565, S0004, S0033, S0041, S0136

### IP Services

Course | 2 hours 59 minutes
---
Explore configuring and verifying inside source NAT, the function of SNMP in network operations, configuring network devices for remote access using SSH, the capabilities and functions of TFTP/FTP in the network and more.

**NICE Knowledge and Skill Statements:**
K0001, K0071, K0111, K0221, K0332, K0334, K0395, K0398, K0452, K0471, K0565, S0004, S0033, S0041, S0136
Security Fundamentals

Course | 3 hours 14 minutes

Learn to define key security concepts, configure device access using local passwords, configure and verify access control lists, describe security program elements and more.

NICE Knowledge and Skill Statements:
K0004, K0007, K0033, K0049, K0056, K0158, K0324, K0336, K0487, K0488, K0561, S0007, S0031, S0077

Automation and Programmability

Course | 1 hour 14 minutes

In this course, you'll explore how automation impacts network management, compare traditional networks with controller-based networking, interpret JSON-encoded data and more.

NICE Knowledge and Skill Statements:
K0086, K0275, S0257
Cisco Certified CyberOps Associate

The CCNA Cyber Ops certification path prepares you to begin a career working with associate-level cybersecurity analysts within security operations centers. You’ll gain the skills needed to pass the Cisco SECFND (210-250) and SECOPS (210-255) certification exams.

**CERTIFICATION PATH**

**Skill Assessment**

Skill assessment | 20 questions
See how your CCNA Cyber Ops skills stack up against other professionals in your field.

**CCNA Cyber Ops Practice Exam**

Practice Exam | 120 questions
Prepare for your CCNA Cyber Ops exams and test your domain knowledge.

**Introduction to Cisco Certified CyberOps Associate**

Course | 10 minutes
This course prepares you for your Cisco Certified CyberOps Associate training. You’ll follow along with the course examples and set up your own cybersecurity lab with Kali Linux.

**NICE Knowledge and Skill Statements:**

K0342

**Network Concepts**

Course | 44 minutes
Networks can be complex, confusing and tricky. With this course, you’ll dive into the devices and protocols used in networking, getting to grips with the basics of what you’ll need to know for a successful security analyst career.

**Security Concepts**

Course | 42 minutes
In this course, you’ll get a closer introduction to some of the basic security concepts and tools that will help you later on in the Cisco Certified CyberOps Associate Learning Path — and in the rest of your career!

**NICE Knowledge and Skill Statements:**

K0001, K0011, K0034, K0058, K0061, K0143, K0174, K0221, K0296, K0332, K0516, K0565

**Cryptography**

Course | 15 minutes
This course will help you understand the differences between things like encryption, hashing and certificates, making it easier for you to understand the intricacies of data protection.

**NICE Knowledge and Skill Statements:**

K0190
## Learning paths

<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Description</th>
<th>Time</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host-Based Analysis</strong></td>
<td>In this course, you'll get to grips with the complexities and challenges of host-based analysis. You'll look at HBA on Microsoft and Linux, including endpoint protection, blacklisting, systems-based sandboxing and more.</td>
<td>39 minutes</td>
<td>K0132, K0440, K0608</td>
</tr>
<tr>
<td><strong>Security Monitoring</strong></td>
<td>The best offense is a good defense ... or is it the other way around? In this course, you will learn how to stop a problem before it starts by detecting potential threats with security monitoring software features.</td>
<td>20 minutes</td>
<td>K0058, K0301, K0493, S0046, S0120, S0221</td>
</tr>
<tr>
<td><strong>Attack Methods</strong></td>
<td>The war between hackers and security experts is ongoing, and the weapons are always evolving. In this course, you'll learn about different strategies used by hackers to attack a network and cause damage.</td>
<td>28 minutes</td>
<td>K0070, K0106, K0160, K0362, K0430, K0493</td>
</tr>
<tr>
<td><strong>Endpoint Threat Analysis and Computer Forensics</strong></td>
<td>In this course, you'll get a chance to explore some of the details of computer forensics. You'll take a closer look at Common Vulnerability Scoring System (CVSS) 3.0, Microsoft Windows and Linux file systems, evidence handling and more.</td>
<td>17 minutes</td>
<td>K0117, K0125, K0191, K0272, K0402</td>
</tr>
<tr>
<td><strong>Network Intrusion Analysis</strong></td>
<td>In this course, you'll discover the types of information that you want to look for during network intrusion analysis. You'll get a look at security analysis with Wireshark, NetFlow version 5 and security events, impact flags and more.</td>
<td>16 minutes</td>
<td>K0046, K0058, K0301, K0324, K0334</td>
</tr>
<tr>
<td><strong>Incident Response and Handling</strong></td>
<td>How you respond to an incident may mean the difference between safety or disaster on a network level. In this course, you'll be introduced to security frameworks and regulations that affect your incident response, including NIST and HIPAA.</td>
<td>34 minutes</td>
<td>K0042, K0222, S0184</td>
</tr>
<tr>
<td><strong>Data and Event Analysis</strong></td>
<td>Once you have the data, you need to analyze it. Explore the details of data and event analysis, including retrospective analysis, data normalization and threat analysis.</td>
<td>21 minutes</td>
<td>K0145, K0301, K0603, S0173</td>
</tr>
</tbody>
</table>

---

**Use code “learnskills” to get 30 days for $1** [GET STARTED]
CompTIA IT Fundamentals (ITF+)

The IT Fundamentals learning path will take you through the essential knowledge, skills, tricks and tools needed to begin mastering the computer. Beginning with the basic hardware, you'll explore maintenance, troubleshooting, networking and much more.

Skill Assessment
Skill assessment | 20 questions
See how your IT Fundamentals (ITF+) skills stack up against other professionals in your field.

How People Use Computers
Course | 16 minutes
Begin your exploration of IT fundamentals with this course on how people use computers.

System Hardware
Course | 24 minutes
System hardware can be complicated. Let's take a look at some different types of hardware.

Device Ports and Peripherals
Course | 13 minutes
Explore device ports, peripherals and video cards with this course.

Data Storage and Sharing
Course | 17 minutes
In this course, you'll get to grips with the technologies of data storage and sharing.

Understanding Operating Systems
Course | 14 minutes
Begin digging into the details of operating systems with this course on OS functions and interfaces.

NICE Knowledge and Skill Statements:
- How People Use Computers: K0036, K0071, K0109, K0113, K0137, K0302
- System Hardware: K0030, K0109, K0321, S0074
- Device Ports and Peripherals: K0109, K0192, K0491
- Data Storage and Sharing: K0097, K0109, K0114, K0373, K0622
- Understanding Operating Systems: K0060, K0318, K0608
<table>
<thead>
<tr>
<th><strong>Setting Up and Configuring a PC</strong></th>
<th><strong>Setting Up and Configuring a Mobile Device</strong></th>
<th><strong>Managing Files</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>16 minutes</td>
<td>Explore the details of PC setup and configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0302</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Using and Managing Application Software</strong></th>
<th><strong>Configuring Network and Internet Connectivity</strong></th>
<th><strong>IT Security Threat Mitigation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>16 minutes</td>
<td>Explore application setup and management with this course.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0229, K0271, K0373, K0444, K0559, K0608</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Computer Maintenance and Management</strong></th>
<th><strong>IT Troubleshooting</strong></th>
<th><strong>Understanding Databases</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>16 minutes</td>
<td>Explore the crucial details of computer maintenance with this course.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0103, K0294, K0302, S0158, S0170</td>
</tr>
</tbody>
</table>
Developing and Implementing Software

Course | 16 minutes

Get ready for a deep dive into the details of programming with this course on developing software.

NICE Knowledge and Skill Statements:
K0016, K0068, K0266, K0372, K0373, K0396, S0060
CompTIA A+

CERTIFICATION PATH

The CompTIA A+ learning path builds a foundation of skills required for entry-level information technology careers. You’ll learn about technical and support issues ranging from networking and operating systems to mobile devices and security.

Skill Assessment

Skill assessment | 20 questions

See how your A+ skills stack up against other professionals in your field.

A+ Practice Exam

Practice Exam | 229 questions

Prepare for your A+ exam and test your domain knowledge.

Introduction to CompTIA A+

Course | 24 minutes

Start your A+ journey off strong with this introductory course on the CompTIA A+ and its structure, uses and what to expect from the exam.

Safety and Professionalism

Course | 37 minutes

Professionalism and safety go hand-in-hand. Take a moment to review the fundamentals of professional communication, physical safety, troubleshooting theory and more.

NICE Knowledge and Skill Statements:

K0030, K0109, K0265, S0070

The Visible Computer

Course | 1 hour 18 minutes

Brush up on your knowledge of computer hardware and software with this course on PC components, OS types, super users and more.

NICE Knowledge and Skill Statements:

K0109, K0224, K0302

CPUs

Course | 1 hour 13 minutes

Get to grips with the details of central processing units, or CPUs, with this course covering CPU cores, caching, sockets and more.

NICE Knowledge and Skill Statements:

K0109, S0146
RAM

Course | 39 minutes

Out of RAM, out of luck. Brush up on your knowledge of RAM with this course covering RAM installation, technology, types and more.

NICE Knowledge and Skill Statements: K0109

Firmware

Course | 35 minutes

Explore one fundamental, permanent aspect of a system: firmware. In this course, you'll look at BIOS, POST, System Setup and more.

NICE Knowledge and Skill Statements: K0109, K0224

Motherboards

Course | 41 minutes

Brush up on your knowledge of the motherboard with this course on motherboard form factors, chipsets, installation and more.

NICE Knowledge and Skill Statements: K0109, K0114

Power Supplies

Course | 1 hour 6 minutes

Power supplies aren't as simple as they appear. Explore the details with this course on power supply design, protection, troubleshooting and more.

NICE Knowledge and Skill Statements: K0109, K0114

Mass Storage Technologies

Course | 39 minutes

Make sure you're storing things the smart way with this course on mass storage technologies, including solid state drives, magnetic disk drives and SCSI.

NICE Knowledge and Skill Statements: K0109, K0114

Implementing Mass Storage

Course | 1 hour 53 minutes

There's more to storage than just keeping a backup. Expand your knowledge of RAID, file systems, dynamic disks and more.

NICE Knowledge and Skill Statements: K0032, K0109, K0114

Essential Peripherals

Course | 1 hour 13 minutes

Update your knowledge of essential peripherals with this course on USB, optical media, Thunderbolt and more.

NICE Knowledge and Skill Statements: K0109, K0114

Building a PC

Course | 54 minutes

Improve your knowledge of booting, installing Windows, post-installation tasks and more.

NICE Knowledge and Skill Statements: K0035, K0036, K0060, K0109, K0114, K0271, K0608

Windows Under the Hood

Course | 1 hour 22 minutes

Take a closer look at Windows with this course covering the Windows registry, services, processes, toolset and more.

NICE Knowledge and Skill Statements: K0116, K0129, K0132, K0192, K0271, K0318, K0608
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>Description</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users, Groups and Permissions</td>
<td>1 hour 4 minutes</td>
<td>Make sure no one has access to the wrong information with this course on users, groups and permissions.</td>
<td>K0117, K0608, S0267</td>
</tr>
<tr>
<td>Maintaining and Optimizing Operating Systems</td>
<td>43 minutes</td>
<td>Get the most out of your OS with this course covering maintaining and optimizing operating systems, system restore, backing up your files and more.</td>
<td>K0060, K0088, K0129, K0318, K0608, S0267</td>
</tr>
<tr>
<td>Working with the Command-Line Interface</td>
<td>1 hour 54 minutes</td>
<td>Get to grips with the complexities of the command-line interface in this course that covers working with drives, files and folders, advanced Windows and Linux commands and more.</td>
<td>K0060, K0068, K0192, K0318, S0267</td>
</tr>
<tr>
<td>Troubleshooting Operating Systems</td>
<td>45 minutes</td>
<td>Explore the art of troubleshooting an OS with this course covering troubleshooting boot problems and applications, kernel panic and more.</td>
<td>K0060, K0224, K0318, S0067, S0142, S0151, S0267</td>
</tr>
<tr>
<td>Display Technologies</td>
<td>53 minutes</td>
<td>Keep an eye out for trouble with this course on display technologies. You'll look at the details of resolutions and aspect ratios, multiple monitors, projects, graphics cards and more.</td>
<td>K0109, K0114, S0142, S0151</td>
</tr>
<tr>
<td>Essentials of Networking</td>
<td>1 hour 15 minutes</td>
<td>Keep your machines talking to each other with this course on the essentials of networking, including hubs and switches, WANs and routers, structured cabling and more.</td>
<td>K0001, K0011, K0029, K0050, K0052, K0061, K0066, K0067, K0073, K0084, K0090, K0091, K0092, K0113, K0137, K0221, K0332, K0395, K0417, K0470, K0471, K0491, K0516, K0556</td>
</tr>
<tr>
<td>Local Area Networking</td>
<td>3 hours 26 minutes</td>
<td>Explore the complexities of LAN with this course covering network IDs and subnet masks, router configuration, port forwarding and more.</td>
<td>K0011, K0029, K0050, K0113, K0221, K0332, K0395, K0491, K0516, K0556, S0168</td>
</tr>
<tr>
<td>Wireless Networking</td>
<td>1 hour 24 minutes</td>
<td>Explore wireless networking with this course covering wireless network hardware, enterprise wireless, troubleshooting connections and more.</td>
<td>K0011, K0108, K0113, K0137, K0138, K0221, K0395, K0446, K0491, K0516, K0556, K0600, K0614</td>
</tr>
<tr>
<td>The Internet</td>
<td>1 hour 36 minutes</td>
<td>Take ninety minutes to deepen your knowledge of the internet’s complexities with this ninety-minute course covering dial-up and broadband, remote desktop connections, FTP, proxy servers and more.</td>
<td>K0011, K0061, K0104, K0113, K0137, K0221, K0274, K0349, K0385, K0444, K0470, K0471, K0491, K0516, K0556, K0603</td>
</tr>
</tbody>
</table>
Virtualization

Course | 48 minutes

Dig deeper into the real details of the virtual world with this course on virtualization, covering cloud computing, virtual machines and more.

NICE Knowledge and Skill Statements: K0104, K0130, K0609, K0610, S0073

Portable Computing

Course | 38 minutes

Laptops aren't as simple as they appear. Improve your knowledge of portable computing with this course on laptop hardware, troubleshooting, displays and more.

NICE Knowledge and Skill Statements: K0109, K0114, K0491

Understanding Mobile Devices

Course | 39 minutes

Brush up on your knowledge of mobile devices with this course covering mobile connections, OSes and more.

NICE Knowledge and Skill Statements: K0109, K0114, K0138, K0224, K0269, K0438, K0600, K0614

Care and Feeding of Mobile Devices

Course | 51 minutes

Dig deeper into mobile devices with this course covering mobile devices and email, synchronization, security and more.

NICE Knowledge and Skill Statements: K0114, K0224, K0283

Printers and Multifunction Devices

Course | 1 hour 18 minutes

Take a closer look at the world of printers with this course covering inkjet, thermal, impact and laser printers, printer installation and troubleshooting, 3D printing and more.

NICE Knowledge and Skill Statements: K0109, K0114, K0142

Securing Computers

Course | 1 hour 31 minutes

Get to grips with system attack and defense through this course on securing computers. Includes modules on physical security, social engineering, malware, incident response and more.

NICE Knowledge and Skill Statements: K0160, K0392, K0412, K0440, K0480, K0612, S0076

Getting Organized

Course | 36 minutes

Review your organization strategies with this course on documents, data, change management, data destruction and more.

NICE Knowledge and Skill Statements: K0038, K0158, K0210, K0260, K0261, K0262
The CompTIA Network+ learning path teaches you how to design, configure, troubleshoot and manage network devices. You’ll learn about implementing networking concepts and using best practices to support and secure devices.

**Skill Assessment**

Skill assessment | 20 questions
See how your Network+ skills stack up against other professionals in your field.

**Network+ Practice Exam**

Practice Exam | 174 questions
Prepare for your Network+ exam and test your domain knowledge.

**Understanding Networks**

Course | 51 minutes
Explore network technology with this course on models, packets, ports and more.

**The Physical Network**

Course | 3 hours 13 minutes
Brush up on the facts of the physical network in a course covering Ethernet, cabling, troubleshooting, Cat ratings and much more.

**The World of TCP/IP**

Course | 3 hours 29 minutes
Take a close look at the world of TCP/IP with this course covering static and dynamic IP addressing, understanding routers and ports, implementing NAT and much more.

**Making TCP/IP Work**

Course | 2 hours 52 minutes
Explore the complexities of making TCP/IP work with this course covering TCP and UDP, netstat, Wireshark and much more.
### Securing TCP/IP

**Course** | 1 hour 19 minutes  
Secure TCP/IP with this course covering encryption, cryptographic hashes, identification and everything else you need to keep your connection safe.

**NICE Knowledge and Skill Statements:**  
K0007, K0018, K0019, K0033, K0056, K0065, K0301, K0332, K0427, K0555, K0565, S0089

### Advanced IP Networking

**Course** | 3 hours 23 minutes  
In this course, you’ll explore the details of advanced IP networking with modules on VLANs, VPNs, ports and more.

**NICE Knowledge and Skill Statements:**  
K0011, K0071, K0104, K0192, K0324, K0417, K0437, K0471, K0516, S0162

### Wireless, Virtual, Cloud and Mobile Networking

**Course** | 3 hours 25 minutes  
Get to grips with the complexities of wireless, virtual, cloud and mobile networking with this course covering wireless security standards, Wi-Fi Protected Setup (WPS), wireless scenarios and much more.

**NICE Knowledge and Skill Statements:**  
K0033, K0108, K0130, K0137, K0194, K0269, K0274, K0283, K0438, K0446, K0610, K0614

### Building a Real-World Network

**Course** | 1 hour  
Explore the building of a real-world network with this course covering network design, unified communications, backups and more.

**NICE Knowledge and Skill Statements:**  
K0021, K0026, K0113, K0159, K0395, K0560, K0599, S0032

### Managing Risk

**Course** | 3 hour 21 minutes  
With this course on managing the network, you’ll look at risk management, access control, network threats, testing network security and more.

**NICE Knowledge and Skill Statements:**  
K0001, K0002, K0004, K0007, K0038, K0044, K0049, K0054, K0056, K0165, K0167, K0177, K0179, K0180, K0205, K0260, K0261, K0262, K0276, K0290, K0342, K0362, K0406, K0452, K0474, K0475, K0480, K0604, K0612, S0041, S0142, S0151
The CompTIA Security+ certification path introduces you to a variety of information security concepts and technical controls. You'll learn about network and application security, compliance, different types of cyber threats and more.

Skill Assessment
Skill assessment | 20 questions
See how your Security+ skills stack up against other professionals in your field.

Security+ Practice Exam
Practice Exam | 525 questions
Prepare for your Security+ exam and test your domain knowledge.

Command Line Basics Cyber Range
Cyber range | 10 labs
Gain practical experience and develop your command line skills through 10 hands-on labs in the Command Line Basics Cyber Range.

Risk Management
Course | 2 hours 9 minutes
Learn key concepts related to risk management, including policies and procedures, business impact analysis and threat and risk assessments.

Cryptography
Course | 2 hours 27 minutes
Build a baseline of cryptography knowledge as you progress through this course covering essential cryptography concepts and use cases.

Identity and Access Management
Course | 1 hour 38 minutes
Learn about one of the most important security concepts related to access management: identification, authentication, authorization and accounting.
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tools of the Trade</strong></td>
<td>1 hour 18 minutes</td>
<td>K0013, K0301, K0318, K0363, K0452, K0488, K0561</td>
</tr>
<tr>
<td><strong>Securing Individual Systems</strong></td>
<td>3 hours 5 minutes</td>
<td>K0005, K0011, K0032, K0046, K0057, K0106, K0109, K0151, K0167, K0205, K0324, K0397, K0480, K0530, K0603</td>
</tr>
<tr>
<td><strong>The Basic LAN</strong></td>
<td>1 hour 44 minutes</td>
<td>K0007, K0033, K0049, K0065, K0104, K0112, K0145, K0179, K0255, K0326, K0336, K0488, K0561</td>
</tr>
<tr>
<td><strong>Beyond the Basic LAN</strong></td>
<td>3 hours 38 minutes</td>
<td>K0033, K0108, K0130, K0167, K0205, K0230, K0322, K0428, K0600, K0603, K0609, K0610</td>
</tr>
<tr>
<td><strong>Secure Protocols</strong></td>
<td>1 hour 23 minutes</td>
<td>K0081, K0091, K0178, K0179, K0221, K0326, K0427</td>
</tr>
<tr>
<td><strong>Testing Your Infrastructure</strong></td>
<td>1 hour 5 minutes</td>
<td>K0005, K0006, K0013, K0070, K0106, K0147, K0151, K0160, K0177, K0244, K0290, K0342, K0362, K0536, K0624</td>
</tr>
<tr>
<td><strong>Dealing with Incidents</strong></td>
<td>36 minutes</td>
<td>K0021, K0026, K0032, K0041, K0042, K0118, K0210, K0433, K0573</td>
</tr>
</tbody>
</table>
The CompTIA Cloud+ certification path introduces you to a variety of information security concepts that affect the cloud. You’ll learn about system requirements, cloud storage, security, troubleshooting and more.

**Skill Assessment**

Skill assessment | 20 questions
See how your Cloud+ skills stack up against other professionals in your field.

**Introducing the Cloud**

Course | 1 hour 17 minutes
Learn what the cloud is, how to set up various cloud accounts, and different cloud service providers.

**System Requirements for Cloud Deployments**

Course | 1 hour 50 minutes
Learn about cloud components, how to deploy the cloud and testing plans.

**Cloud Storage**

Course | 1 hour 3 minutes
Learn about different storage types, how to manage storage and what to do in case the worst should happen.

**Cloud Compute**

Course | 1 hour 6 minutes
Learn about cloud computing and how to run service and applications within the cloud.

**Cloud Networking**

Course | 52 minutes
Learn about cloud networking, ports and protocols, and VPNs and other security technology you’ll need to keep your cloud safe.
### Cloud Security

Course | 1 hour 22 minutes

Take a deep dive into cloud security, the rules and regulations governing security and various tools and services needed to protect the cloud.

**NICE Knowledge and Skill Statements:**
K0004, K0007, K0018, K0019, K0049, K0056, K0065, K0075, K0190, K0194, K0336, K0488, K0561, S0031, S0167

### Migration Types

Course | 41 minutes

Migrating to the cloud requires planning and precision. Learn tools and techniques to consider when planning for migration.

**NICE Knowledge and Skill Statements:**
K0001, K0004, K0072, K0130, K0194, K0609, K0610, S0073

### Planning Patch Management

Course | 1 hour 17 minutes

Get to grips with patch management and how to plan and implement patches from deployment to retirement.

**NICE Knowledge and Skill Statements:**
K0004, K0074, K0194, S0206

### Troubleshooting Cloud Solutions

Course | 49 minutes

Learn everything you need to know about how to troubleshoot in the cloud.

**NICE Knowledge and Skill Statements:**
K0004, K0194, S0124, S0142, S0151
Cybersecurity Foundations

This learning path is an introductory cybersecurity path for people who have not been exposed to cybersecurity concepts in the workplace before. In these courses, a cybersecurity professional will walk the student through foundational concepts, commands and tools.

Cybersecurity Foundations skill assessment
Skill assessment | 20 questions
See how your foundational cybersecurity skills stack up against other professionals in your field.

Introduction to cybersecurity foundations
Course | 2 minutes
Learn what this learning path covers in a short and straightforward introductory video.

Cybersecurity foundations
Course | 39 minutes
This course introduces you to the basic concepts that are usually not covered in other classes and bootcamps for people entering the industry.

Operating system foundations
Course | 31 minutes
This is an introductory course to what an actual operating system is. We talk about Linux, Windows and MacOS.

Windows command line foundations
Course | 40 minutes
This course is an introduction to the Windows command line. There will be almost immediate hands-on exercises.

Linux command line foundations
Course | 33 minutes
This course is designed to get the learner started on using Linux and the Linux command line.

NICE Knowledge and Skill Statements:
K0060, K0129, K0167, K0192, K0205, K0224, K0302, K0318, K0608, S0267

NICE Knowledge and Skill Statements:
K0060, K0129, K0167, K0192, K0205, K0224, K0302, K0318, K0608, S0267
# IT and security fundamentals

<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
</table>

## Network fundamentals

**Course | 30 minutes**

When data moves, it generally moves from one network to another. Here, we teach the learner about the fundamentals of networking.

### NICE Knowledge and Skill Statements:

K0001, K0034, K0050, K0057, K0061, K0093, K0136, K0159, K0170, K0221, K0265, K0274, K0303, K0332, K0333

## Cloud computing fundamentals

**Course | 43 minutes**

This course is an introduction to cloud computing. It builds from the Network Fundamentals course in this path and prepares the learner for learning cloud security.

### NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0179, K0194, K0230, K0255, K0489, S0073

## Cybersecurity auditing

**Course | 12 minutes**

This course is a basic introduction to cybersecurity auditing.

### NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0043, K0090, K0154, K0165, K0198, K0257, K0363, S0038, S0085

## Risk management

**Course | 15 minutes**

This course will take the learner on a quick trip down the road of risk management.

### NICE Knowledge and Skill Statements:

K0002, K0008, K0019, K0021, K0026, K0048, K0065, K0100, K0101, K0126, K0149, K0154, K0165, K0379, K0455, K0622, S0120, S0175, S0252

## Cybersecurity policy framework and guidelines

**Course | 12 minutes**

In this course, the learner will get a good look at what policies and frameworks do to keep the cybersecurity industry on-mission and formal.

### NICE Knowledge and Skill Statements:

K0047, K0048, K0065, K0073, K0087, K0214, K0242, K0432, S0147

## Pentest demonstration: Appetizer for the beginner

**Course | 25 minutes**

In this course, we will take you through all five phases of a penetration test.

### NICE Knowledge and Skill Statements:

K0001, K0004, K0013, K0070, K0342, S0051
Database Security

In the Database Security learning path, you'll learn about applicable rules and regulations and what it takes to protect sensitive data.

### Database Security skill assessment

**Skill assessment | 20 questions**

See how your foundational database security skills stack up against other professionals in your field.

### Who's responsible for data security?

**Course | 20 minutes**

This course discusses the duties of key groups, as well as giving an environment overview.

### What data requires elevated security

**Course | 34 minutes**

Data security is an important part of the modern workplace. This course explores data classification in a security context.

### When is database security important

**Course | 11 minutes**

Explore the three states of data in the context of database security.

### Why is database security necessary

**Course | 20 minutes**

A look at the importance of database security.

### How to secure databases in use

**Course | 2 hours 15 minutes**

Being aware of how to best protect data in use will be covered within this course.

NICE Knowledge and Skill Statements:

K0004, K0023, K0024, K0069, K0278, K0419, K0420, K0421, K0622, S0013, S0042, S0045, S0286
### Policies & procedures

Course | 52 minutes

A look at the importance of policies and procedures, as well as a quick examination of standards and change management.

**NICE Knowledge and Skill Statements:**

K0003, K0004, K0005, K0065, K0087, K0101, K0146, K0157, K0264, S0018, S0145

---

### How to secure databases in motion

Course | 1 hour 15 minutes

This course will be a discussion on how to best protect data in motion, along with labs on encryption, views and triggers.

**NICE Knowledge and Skill Statements:**

K0004, K0023, K0024, K0069, K0278, K0419, K0420, K0421, K0622, S0013, S0042, S0045, S0286

---

### How to secure databases at rest

Course | 1 hour 4 minutes

This course will discuss the best methods on how to protect data in rest, and physical security of databases.

**NICE Knowledge and Skill Statements:**

K0004, K0023, K0024, K0069, K0278, K0419, K0420, K0421, K0622, S0013, S0042, S0045, S0286

---

### Auditing & monitoring

Course | 1 hour 4 minutes

In this course, you’ll explore the intricacies of database and server log monitoring for the purpose of database security.

**NICE Knowledge and Skill Statements:**

K0003, K0004, K0043, K0090, K0120, K0180, K0198, S0085
The ICS/SCADA Security Fundamentals skill path provides you with foundational knowledge about SCADA systems and security, including protocols, access controls, physical security, cybersecurity tools and more.

Skill Assessment

Skill assessment | 20 questions

See how your Linux/Unix stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

ICS/SCADA Security Fundamentals Project

Project | 1 hour 17 minutes

This project contains three parts and requires tasks across the MITRE ATT&CK for ICS Framework, the NIST CSF, risk assessment activities, ICS network architecture design, Packet Capture analysis, and reviewing IDS alert logs.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Industrial Control Systems (ICS) Introduction

Course | 27 minutes

A look at operational technology and ICS, including infrastructure, asset types and environments.

NICE Knowledge and Skill Statements:

K0137, K0437

ICS Fundamentals

Course | 33 minutes

A look at ICS fundamentals such as SCADA, SIS, DCS and ICS communications.

NICE Knowledge and Skill Statements:

K0004, K0137, K0179, K0221, K0332, K0437, K0561

ICS Operational Environment

Course | 36 minutes

A look at the ICS operational environment, exploring policies and standards, configuration management and more.

NICE Knowledge and Skill Statements:

K0002, K0054, K0137, K0154, K0157, K0158, K0200, K0267, K0437, S0167

ICS Networking

Course | 30 minutes

Explore ICS networking, including architecture, industry 4.0 and ICS network protocol analysis.

NICE Knowledge and Skill Statements:

K0027, K0049, K0056, K0075, K0113, K0137, K0170, K0221, K0240, K0322, K0332, K0417, K0437, K0491, K0561, K0565, S0077
ICS Security Introduction

Course | 31 minutes
A look at ICS security, including cybersecurity frameworks, physical security and more.

NICE Knowledge and Skill Statements:
K0007, K0047, K0048, K0049, K0054, K0056, K0065, K0084, K0137, K0170, K0179, K0200, K0233, K0240, K0437, K0561, S0031, S0077, S0144, S0147, S0256

ICS Security Management

Course | 1 hour 4 minutes
Exploring ICS security management, including asset management, mitigating cyber risk in ICS, intrusion detection and prevention and more.

NICE Knowledge and Skill Statements:
K0002, K0007, K0021, K0026, K0032, K0042, K0048, K0056, K0065, K0084, K0137, K0154, K0157, K0170, K0200, K0231, K0240, K0361, K0399, K0437, K0496, K0519, S0079, S0144, S0171
Information Security Fundamentals

The Information Security Fundamentals skill path teaches you critical knowledge of hardware, software and network security. You'll learn about popular security concepts, controls and technologies, as well as an overview of risk management, incident response and disaster recovery.

**Command Line Basics Cyber Range**

Cyber range | 10 labs

Gain practical experience and develop your command line skills through 10 hands-on labs in the Command Line Basics Cyber Range.

**NICE Knowledge and Skill Statements:**
S0046, S0081, S0158, S0241, S0267, S0294

**Access Control Fundamentals**

Course | 21 minutes

Explore the essential concepts of access control in this four-video course covering access control models, implementation, concepts and enforcement.

**NICE Knowledge and Skill Statements:**
K0007, K0065, K0158, K0336

**Secure Network Design**

Course | 14 minutes

Learn the basics of designing secure networks, from an overview of network topologies to foundational security concepts such as segmentation and isolation.

**NICE Knowledge and Skill Statements:**
K0001, K0111, K0179, K0255, K0326, K0487, K0489

**Identification and AAA**

Course | 16 minutes

Learn about one of the most important information security concepts related to access management: identification, authentication, authorization and accounting (IAAA).

**NICE Knowledge and Skill Statements:**
K0007, K0056, K0336

**Hardware and OS Security**

Course | 16 minutes

Gain an entry-level understanding of essential hardware, firmware and operating system security concepts in this three-video introductory course.

**NICE Knowledge and Skill Statements:**
K0060, K0115, K0129, K0167, K0205, K0318

**Software and Application Security**

Course | 23 minutes

Learn the basics of secure software and application development, including secure staging, secure coding techniques, and code quality and testing.

**NICE Knowledge and Skill Statements:**
K0039, K0081, K0153, K0178
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>9 minutes</td>
<td>Course</td>
<td>60 minutes</td>
<td>Course</td>
<td>30 minutes</td>
<td>Course</td>
<td>17 minutes</td>
</tr>
<tr>
<td>Discover how common physical and environment security controls relate to information security in this brief overview course.</td>
<td>Explore the uses of common information security technology and tools as you progress through this nine-video introductory course.</td>
<td>Build a baseline of cryptography knowledge as you progress through this nine-video introductory course.</td>
<td>Get an overview of common security control categories and types, and learn about important concepts such as data sanitation and data sensitivity.</td>
<td>Learn the key concepts related to risk management, including policies and procedures, business impact analysis, and threat and risk assessments.</td>
<td>Build your knowledge of popular threats, including malware and social engineering as well as application, wireless and cryptographic attacks.</td>
<td>Learn the planning, procedures and concepts that go into business continuity and disaster recovery in this introductory course.</td>
<td>NICE Knowledge and Skill Statements: K0007</td>
</tr>
</tbody>
</table>
Introduction to x86 Disassembly

Explore the foundations of x86 assembly, one of the most common assembly architectures in the world. Whether you’re looking to become a better programmer or reverse engineer, a knowledge of assembly and how processors work is invaluable.

Skill Assessment

Skill assessment | 20 questions
See how your x86 disassembly skills stack up against other professionals in your field.

x86 Disassembly Project

Project | 3 challenges
Practice your x86 disassembly skills as your progress through five challenges.

What is x86 Assembly?

Course | 20 minutes
Dive into the world of assembly by learning a little about its history and some of the key differences between different assembly languages. This course takes you through a brief history of x86 Assembly and explores how it’s used.

NICE Knowledge and Skill Statements:
K0051, K0139, K0227, K0372

x86 Basics

Course | 51 minutes
Learn the fundamentals of x86 Assembly. Explore the syntax, how data is represented, how to address memory and how to store information.

NICE Knowledge and Skill Statements:
K0051, K0139, K0372, S0239

Programming in x86

Course | 1 hour 13 minutes
Learn the most common x86 instructions and how to use them. With the basics down, you’ll learn how to assemble and run an application fully written in x86 Assembly.

NICE Knowledge and Skill Statements:
K0139

Calls, Strings and Codes

Course | 1 hour 16 minutes
Learn how to do basic input and output, work with strings and condition codes at the x86 Assembly level. Then try your hand at your first project by building your own x86 Assembly program.

NICE Knowledge and Skill Statements:
K0051, K0068, K0139, K0372, S0239, S0257
Debugging

Course | 38 minutes

Learn how to debug at the assembly level and how to recover the assembly code from already-built binaries. Practice identifying common assembly fault conditions, then finish with a debugging project.

NICE Knowledge and Skill Statements:
K0051, K0068, K0079, K0139, K0186, K0372, K0396, S0014, S0239, S0257

Logic Flows

Course | 1 hour 2 minutes

Learn how to use logical flows in assembly to create code branches and optional code paths.

NICE Knowledge and Skill Statements:
K0051, K0068, K0139, K0372, K0396, S0239, S0257
ISACA CISA

Certification Path

The Certified Information Systems Auditor (CISA) certification path builds your knowledge of auditing information systems. You'll learn the tools and guidelines involved in the IT auditing process as well as concepts such as business continuity, enterprise IT governance, common security controls and more.

Skill Assessment
Skill assessment | 20 questions
See how your skills stack up against other professionals in your field.

Custom CISA Practice Exam
Practice Exam | 800 questions
Prepare for your ISACA CISA exam and test your domain knowledge.

CISA Introduction
Course | 19 minutes
Introduce yourself to CISA with this course introduction covering study plans, CISA stats and details, and more.

IS Audit Functions
Course | 8 minutes
Explore the functions of an information security audit with this course looking at auditor practices, IS audit purposes and more.

Business Process Applications and Controls
Course | 42 minutes
Explore the Business Process section and the controls you'll need to understand during your CISA study.

Types of Controls and Risk Assessments
Course | 21 minutes
Explore the types of controls and risk assessments in four parts, beginning with Control Objectives and Control Measures.

NICE Knowledge and Skill Statements:
K0003, K0004, K0005, K0044, K0047, K0146, K0263, K0264, S0085

NICE Knowledge and Skill Statements:
K0002, K0004, K0005, K0044, K0047, K0065, K0264, S0034, S0085, S0147, S0171
Continuous Auditing

Course | 39 minutes

In this course, you'll look at the five parts of the Audit Project Management section, as well as sampling, audit report objectives and more.

NICE Knowledge and Skill Statements:
K0002, K0005, K0047, K0121, K0432, S0085

Governance and Management of IT

Course | 39 minutes

Dig deep into the details of governance and management of IT.

NICE Knowledge and Skill Statements:
K0002, K0027, K0044, K0146, K0154, K0198, K0429, K0501, K0504, S0085

IT Organizational Structure

Course | 32 minutes

Explore IT organizational structure and the critical associated concepts.

NICE Knowledge and Skill Statements:
K0002, K0004, K0027, K0043, K0044, K0047, K0267, K0429, K0504, S0085

IT Management

Course | 39 minutes

In this course, you’ll review the details of IT management and more.

NICE Knowledge and Skill Statements:
K0004, K0027, K0044, K0053, K0101, K0154, K0198, K0257, K0265, K0267, K0270, K0429, S0085

CISA Day 1 Review Quiz

Skill assessment | 100 questions

Assess your new skills with a review quiz.

Information Systems Acquisition

Course | 32 minutes

Take a closer look at the first part of the Information Systems Acquisition and Development subdomain.

NICE Knowledge and Skill Statements:
K0290, K0101, K0121, K0154, K0257, K0270, S0085, S0273

Business Cases and Development

Course | 1 hour 4 minutes

Take some time to explore the second part of Information Systems Acquisition and Development.

NICE Knowledge and Skill Statements:
K0004, K0044, K0080, K0081, K0121, K0140, K0183, K0267, K0429, K0622, S0085, S0273

Information Systems Implementation

Course | 42 minutes

Wrap up Domain 3 of CISA with this course covering Control Identification and Design and Information Systems Implementation.

NICE Knowledge and Skill Statements:
K0004, K0044, K0074, K0091, K0178, K0267, K0275, K0290, K0531, K0622, S0085, S0273

CISA Day 2 Review Quiz

Skill assessment | 100 questions

Assess your new skills with a review quiz.
Information Systems Operations

Course | 1 hour 18 minutes

Dive into Part A of CISA Domain 4 in this course covering Common Technology Components and more.

NICE Knowledge and Skill Statements:
K0002, K0074, K0109, K0275, K0317, K0361, K0419, K0589, K0622, S0085, S0273

CISA Day 3 Review Quiz

Skill assessment | 100 questions

Assess your new skills with a review quiz.

Asset Security Frameworks, Standards and Guidelines

Course | 41 minutes

In this course, you’ll start on CISA Domain 5 by covering Information Asset Security and Control topics.

NICE Knowledge and Skill Statements:
K0005, K0007, K0261, K0262, K0263, K0622, S0085

Identity and Access Management

Course | 1 hour 6 minutes

Continue with Domain 5, Part A of CISA in this course covering identification and authentication topics.

NICE Knowledge and Skill Statements:
K0004, K0007, K0056, K0065, S0085

Network Infrastructure Security

Course | 52 minutes

Network infrastructure security has no secrets in this three-video course. Covers structure, auditing and more.

NICE Knowledge and Skill Statements:
K0004, K0005, K0010, K0044, K0061, K0108, K0113, K0221, K0286, K0417, K0556, K0560, K0561, K0660, S0085, S0192

Asset Security

Course | 51 minutes

Wrap up Part A of CISA Domain 5 with this course covering asset security topics.

NICE Knowledge and Skill Statements:
K0004, K0005, K0018, K0019, K0044, K0065, K0113, K0136, K0159, K0190, K0195, K0230, K0287, K0322, K0427, K0609, K0622, S0085

Security Event Management

Course | 42 minutes

Explore Part B of CISA Domain 5 with this course on security event management.

NICE Knowledge and Skill Statements:
K0003, K0005, K0042, K0118, K0145, K0150, K0215, K0243, K0245, K0290, K0324, K0474, K0503, K0548, K0603, S0085, S0273
CISA Day 4 Review Quiz

Skill assessment | 100 questions

Assess your new skills with a review quiz.
ISC2 System Security Certified Practitioner (SSCP)

The System Security Certified Practitioner (SSCP) certification path will provide students with an overview of foundational information security concepts. The course will cover the seven domains that encompass the SSCP, with topics ranging from securing information systems and data to overall security operations.

### CERTIFICATION PATH

<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSCP Practice Exam</strong></td>
<td>Practice exam</td>
<td>Prepare for your ISC2 System Security Certified Practitioner exam and test your domain knowledge.</td>
</tr>
<tr>
<td><strong>Security Operations</strong></td>
<td>1 hour 37 minutes</td>
<td>This course will take a closer look at different aspects of security operations from code of ethics to the security controls needed to ensure the confidentiality, integrity and availability (CIA framework) of an organization's information systems. The CIA framework will be a common reference throughout the entirety of the course. The CIA framework will be a common reference throughout the entirety of the course.</td>
</tr>
<tr>
<td><strong>Access Controls</strong></td>
<td>52 minutes</td>
<td>This course will walk through how organizations implement and maintain various authentication methods to those systems. We will discuss various techniques used by organizations such as single vs. multi-factor authentication and how single sign-on works.</td>
</tr>
<tr>
<td><strong>Risk Identification, Monitoring and Analysis</strong></td>
<td>1 hour 2 minutes</td>
<td>We'll look at how organizations identify their risk and choose how they want to treat their risk, whether they opt to accept it, mitigate it or transfer the risk to a third-party entity. We will also walk through various regulatory concerns that information security teams must be aware of, especially if organizations decide to operate in different counties or jurisdictions.</td>
</tr>
<tr>
<td><strong>Incident Response and Recovery</strong></td>
<td>49 minutes</td>
<td>The establishment of an incident response process will ensure that an organization can recover following the identification of a security incident. And while all alerts are not considered incidents, this section focuses on how to properly identify a security event in order to potentially declare it as an incident. In this course, you will learn how to truly define security incidents versus security events.</td>
</tr>
<tr>
<td><strong>Overview of Cryptography</strong></td>
<td>55 minutes</td>
<td>This course will review the core aspects of cryptography and the need for it. We take a pragmatic approach to understanding how and why cryptography and information security go hand-in-hand.</td>
</tr>
</tbody>
</table>
**Network and Communications Security**

Course | 1 hour 58 minutes

The security in your organization's network is just as important as the devices that sit on that network. In this section, we will discuss the various fundamental concepts of networking, starting with a model that helps describe a network at a logical level.

**System and Application Security**

Course | 1 hour and 41 minutes

Domain 7 will discuss the fundamentals of malware and the steps organizations may take to prevent or mitigate it.
Linux Fundamentals

The Linux Fundamentals learning path provides the fundamental skills and knowledge needed to successfully configure, manage and troubleshoot Linux systems. You will learn hands-on skills that are relevant for any Linux distribution (e.g., Red Hat, Ubuntu, Fedora, openSUSE).

**Linux Cyber Range**

Cyber range | 31 labs

Gain practical experience and build your real-world Linux skills through 31 hands-on labs in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0007, S0067, S0084, S0158, S0267

**Installing Linux**

Course | 14 minutes

Get an overview of the Linux platform and learn about its installation.

NICE Knowledge and Skill Statements:
K0192

**Using Linux**

Course | 38 minutes

Explore the basics of the Linux GUI and using command lines.

NICE Knowledge and Skill Statements:
K0192

**File and Directory Management**

Course | 1 hour 8 minutes

Everything you need to know about working with Linux files and directories.

NICE Knowledge and Skill Statements:
K0192

**System Administration**

Course | 1 hour 2 minutes

Get an comprehensive view of system admin tasks such as user and group management.

NICE Knowledge and Skill Statements:
K0192

**User Environment Configuration**

Course | 48 minutes

Understand the shell and environmental variables that store different information.

NICE Knowledge and Skill Statements:
K0192
# Application Management

**Course | 34 minutes**

Learn how software installation and packages work in Linux.

**NICE Knowledge and Skill Statements:**
K0192

---

# System Configuration

**Course | 1 hour 4 minutes**

Know what's involved in installing and managing new drives.

**NICE Knowledge and Skill Statements:**
S0067

---

# Process and Module Management

**Course | 45 minutes**

See how processes carry out tasks within Linux.

**NICE Knowledge and Skill Statements:**
K0192

---

# System Maintenance

**Course | 1 hour 23 minutes**

An overview of core maintenance tasks such as data backup and performance monitoring.

**NICE Knowledge and Skill Statements:**
K0021

---

# Networking

**Course | 1 hour 34 minutes**

The fundamentals of networking, from components and addresses to protocols and DNS.

**NICE Knowledge and Skill Statements:**
K0221

---

# File Sharing and Printing

**Course | 20 minutes**

See how NFS (network file system) is configured in the Linux system.

**NICE Knowledge and Skill Statements:**
K0192

---

# Accessibility and Localization

**Course | 20 minutes**

Features and assistive technologies that make Linux more accessible and available to a variety of users.

**NICE Knowledge and Skill Statements:**
S0067

---

# Security

**Course | 1 hour 1 minute**

Make your Linux system more secure with these tools and techniques.

**NICE Knowledge and Skill Statements:**
K0192

---

# Web Environment

**Course | 37 minutes**

Learn about the modern web technologies that Linux supports.

**NICE Knowledge and Skill Statements:**
K0192
FTP and Email Services

Course | 47 minutes

A multi-part course introduces you to FTP, SSH and email configuration basics.

NICE Knowledge and Skill Statements:
K0192

Troubleshooting and Maintenance

Course | 1 hour 8 minutes

Take a dive into various issues you may encounter, and how to solve them.

NICE Knowledge and Skill Statements:
K0192
Network Security Fundamentals

Network security is a highly in-demand skill in the infosec world, and this learning path will teach you the fundamentals of networking and how to secure your networks.

Skill Assessment

Skill assessment | 20 questions
See how your network security fundamentals skills stack up against other professionals in your field.

Networking Fundamentals

Course | 1 hour 39 minutes
Learn about the OSI and TCP/IP models, AAA services and IAM (Identity and Access Management), and find out more about network traffic and how to secure it.

NICE Knowledge and Skill Statements:
K0001, K0007, K0056, K0061, K0221, K0332, K0395, K0471, K0565

Wireless Networks and Security

Course | 53 minutes
Uncover new information about wireless networks and security, with a focus on both Wi-Fi and cellular networks.

NICE Knowledge and Skill Statements:
K0001, K0108, K0113, K0137, K0446, K0556, K0614

Firewalls and IDS/IPS

Course | 30 minutes
Understand the fundamentals of both firewalls and IDS/IPSes, including types and architecture and what they can do to protect your network.

NICE Knowledge and Skill Statements:
K0033, K0038, K0044, K0324, K0561

VPNs and Remote Access Technologies

Course | 25 minutes
VPNs (virtual private networks) are essential to secure remote access of your network, and in this course we’ll be focused on how to lock down your network using VPN tunnels and different remote access technologies.

NICE Knowledge and Skill Statements:
K0071, K0104, K0247, K0561

Endpoint Security

Course | 32 minutes
In this course, we will discuss protecting the endpoint, anti-malware and host-based IDS/IPSes, endpoint hardening and using mobile device management to lock down mobile devices.

NICE Knowledge and Skill Statements:
K0033, K0324, K0440, K0488, K0561
<table>
<thead>
<tr>
<th><strong>Preventing and Mitigating Network Attacks</strong></th>
<th><strong>Network Security Principles</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>20 minutes</td>
</tr>
<tr>
<td>In this course, we cover real-world network attacks and how to mitigate these potential risks.</td>
<td>In this course, we go over some general concepts related to network security as well as how to establish these principles through policies and procedures.</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**
K0033, K0106, K0160, K0165, K0324, K0362, K0408, K0440, K0488, K0561, K0612

**NICE Knowledge and Skill Statements:**
K0021, K0112, K0157, K0159, K0179, K0622
The OWASP Top Ten learning path will help you understand each of the security risks listed in the OWASP Top Ten. The “Top Ten” is a list of the most serious and prevalent security risks that exist for web applications today.

**Skill Assessment**

Skill assessment | 20 questions

See how your OWASP Top Ten skills stack up against other professionals in your field.

**OWASP Top 10 Cyber Range**

Cyber Range | 20 labs

Gain hands-on experience with the ten categories of web application security risks presented by OWASP.

NICE Knowledge and Skill Statements:
S0022, S0025, S0051, S0084, S0172, S0174, S0293

**OWASP Top Ten Overview**

Course | 29 minutes

An overview of the OWASP organization and their methodology for creating and publishing the Top Ten list.

NICE Knowledge and Skill Statements: K0004

**OWASP Top Ten: Risks One through Five**

Course | 3 hours 36 minutes

Explore the details of security risks one through five in the OWASP Top Ten list.

NICE Knowledge and Skill Statements: K0004

**OWASP Top Ten: Risks Six through 10**

Course | 2 hours 49 minutes

Explore the details of security risks six through 10 in the OWASP Top Ten list.

NICE Knowledge and Skill Statements: K0004, K0009

**OWASP Top Ten: Scenarios**

Course | 10 minutes

Take a look at five different Web application vulnerability or attack scenarios and answer challenging questions to test your OWASP Top Ten understanding.

NICE Knowledge and Skill Statements: K0009, K0070, K0140, K0624
# Python for Cybersecurity

This Python for Cybersecurity skills path helps you to master the use of Python for a wide variety of cybersecurity tasks.

## Python for Cybersecurity Project

**Project | 58 minutes**

This project tests the understanding of the concepts and code demonstrated in this learning path.

## Secure Coding - Python

**Cyber range | 45 minutes**

This lab covers multiple secure coding errors commonly found in Python, including deserialization and XML based attacks.

## Introduction to Python for cybersecurity

**Course | 26 minutes**

This course provides an introduction to the Python for Cybersecurity Learning Path and introduces Python and the MITRE ATT&CK framework.

### NICE Knowledge and Skill Statements:

K0004, K0039, K0068, K0070, K0079, K0080, K0082, K0139, K0140, K0236, K0559, K0624, S0060, S0130, S0172, S0266

## Python for PRE-ATT&CK

**Course | 59 minutes**

The course demonstrates the use of Python to achieve the objectives outlined in the MITRE PRE-ATT&CK matrix.

### NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0624, S0060, S0130, S0266

## Python for initial access

**Course | 38 minutes**

This course demonstrates the use of Python to achieve initial access to a target system.

### NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

## Python for execution

**Course | 23 minutes**

This course demonstrates the use of Python to achieve code execution on a system.

### NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

---

Use code "learnskills" to get 30 days for $1  
[GET STARTED]
Python for credential access

Course | 44 minutes

This course demonstrates the use of Python to gain access to user credentials.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for discovery

Course | 35 minutes

This course demonstrates the use of Python to perform discovery on a target system.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for lateral movement

Course | 27 minutes

This course demonstrates the use of Python to move laterally through a target network.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for collection

Course | 25 minutes

This course demonstrates the use of Python for collection of data on a target system.

NICE Knowledge and Skill Statements:
K0040, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for command-and-control

Course | 37 minutes

This course demonstrates the use of Python for command-and-control infrastructure.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0266

Python for privilege escalation

Course | 36 minutes

This course demonstrates the use of Python to achieve privilege escalation.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for defense evasion

Course | 30 minutes

In this course, you'll explore the details of using Python for defense evasion.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, K0430, K0493, S0051, S0060, S0130, S0266

Python for persistence

Course | 41 minutes

This course demonstrates the use of Python to achieve persistence on a target system.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for collection

Course | 25 minutes

This course demonstrates the use of Python for collection of data on a target system.

NICE Knowledge and Skill Statements:
K0040, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for persistence

Course | 41 minutes

This course demonstrates the use of Python to achieve persistence on a target system.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for privilege escalation

Course | 36 minutes

This course demonstrates the use of Python to achieve privilege escalation.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for defense evasion

Course | 30 minutes

In this course, you'll explore the details of using Python for defense evasion.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, K0430, K0493, S0051, S0060, S0130, S0266

Python for collection

Course | 25 minutes

This course demonstrates the use of Python for collection of data on a target system.

NICE Knowledge and Skill Statements:
K0040, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266
Python for impact

Course | 31 minutes
This course demonstrates the use of Python to achieve an attacker's final objectives on a target system.

NICE Knowledge and Skill Statements:
K0004, K0018, K0068, K0070, K0139, K0140, K0177, K0190, K0236, K0342, K0427, S0051, S0060, S0130, S0266

Python for active defense: Decoys

Course | 48 minutes
This course demonstrates the use of Python for developing decoys for active defense.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0487, K0561, S0060, S0130, S0266

Python for active defense: Network

Course | 58 minutes
This course demonstrates the use of Python at the network level for active defense.

NICE Knowledge and Skill Statements:
K0004, K0068, K0070, K0116, K0139, K0140, K0177, K0179, K0236, K0255, K0487, K0561, K0565, S0060, S0130, S0266

Python for active defense: Monitoring

Course | 57 minutes
This course demonstrates the use of Python for monitoring for active defense.

NICE Knowledge and Skill Statements:
K0004, K0139, K0140, K0180, K0236, S0060, S0130, S0136, S0266
Securing Linux/UNIX

The Securing Linux/UNIX Learning Path will show you many facets of securing the Linux operating system. We will cover various topics, including understanding Linux users and groups, UIDs and GUIDs, file-level permissions and more.

Skill Assessment
Skill assessment | 20 questions
See how your Linux/Unix stack up against other professionals in your field.

Securing Linux/UNIX Project
Project | 2 hours 5 minutes
Get hands-on experience using sudo, configuring OpenSSH, identifying and configuring access to TCP ports, decrypting and encrypting with GPG, and using SELinux.

NICE Knowledge and Skill Statements:
S0121

Linux Users
Course | 44 minutes
This course will go over the basics of file permissions in Linux.

NICE Knowledge and Skill Statements:
K0060, K0192, K0318, K0397, K0608, S0067

All About SSH
Course | 52 minutes
We will look at some basics of SSH and how to use it to authenticate to remote servers, both with and without passwords. Securing SSH servers is very important, and we will review the various ways to lock down this critical service.

NICE Knowledge and Skill Statements:
K0071, K0167, K0192, K0205, K0608, S0067, S0121

Linux and open ports with daemons
Course | 17 minutes
Learn what you need to know if ports on your server or a remote server are exposed. Explore why it is a bad idea to run services that expose ports as the root user.

NICE Knowledge and Skill Statements:
K0167, K0192, K0205, K0342, K0491, K0608, S0067, S0121

TLS/SSL Certificates
Course | 29 minutes
TLS certs are an important part of securing traffic for applications that transfer data over the internet. Learn how to generate TLS certificates and use them on your servers.

NICE Knowledge and Skill Statements:
K0077, K0192, K0444, K0491, K0603, K0608, S0067, S0155
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls on Linux</td>
<td>24 minutes</td>
<td>K0005, K0049, K0192, K0202, K0624, S0067, S0076</td>
<td>Learn the basics of setting up Layer 3 firewall rules on a Linux server. These days, applications need protection from attacks as well, so we'll also look at Web Application Firewalls.</td>
</tr>
<tr>
<td>IDS/IPS on Linux</td>
<td>30 minutes</td>
<td>K0049, K0192, K0324, K0488, S0067, S0076</td>
<td>Learn about how Host Intrusion Detection Systems can alert you when critical changes are made to your systems. We will also cover how to stop brute-force attacks on applications running on your Linux systems by using the IPS Fail2Ban.</td>
</tr>
<tr>
<td>Encryption using GPG</td>
<td>19 minutes</td>
<td>K0038, K0049, K0192, K0427, S0067, S0076</td>
<td>Email is one of the most widely used communication mediums on the internet and is typically sent in cleartext. GPG will help ensure that your communications are safe from unwanted eyes.</td>
</tr>
<tr>
<td>SELinux</td>
<td>32 minutes</td>
<td>K0049, K0060, K0167, K0192, K0205, K0397, S0067, S0121</td>
<td>SELinux was designed to make Linux more secure but most people end up disabling it. Take a look at the basics of SELinux and how it works so that you don't have to change it.</td>
</tr>
<tr>
<td>Security Scanning</td>
<td>16 minutes</td>
<td>K0073, K0205, S0121, S0167, S0242</td>
<td>Dive into the world of securing Linux systems and their apps (as suggested by the Department of Defense) with STIGs. We'll also cover automating system hardening with an OpenSCAP application.</td>
</tr>
</tbody>
</table>
Web Server Protection

The web server protection learning path helps you to understand the different activities and processes to implement and monitor the security of a web server or web application. You will learn the basic concepts and tools to design, evaluate and monitor your web server.

Skill Assessment

Skill assessment | 20 questions
See how your web server protection stack up against other professionals in your field.

Web Server Protection Project

Project | 2 hours 42 minutes
Work with an Apache web server to implement network filtering, add cookies to access log, harden the host OS, identify tampered binary files and complete other tasks to ensure that your web server is properly protected.

NICE Knowledge and Skill Statements:
K0135, S0051, S0078, S0137, S0167

Introduction to the Web

Course | 1 hour 55 minutes
Get an introduction to the web, how it works and the basic protocols required to use it.

NICE Knowledge and Skill Statements:
K0061, K0221, K0395, K0470, K0471, K0491, K0565,

Infrastructure Components

Course | 2 hours 18 minutes
This serves as an introduction to some of the most common infrastructure components and how are they used for providing web server services.

NICE Knowledge and Skill Statements:
K0113, K0202, K0324, K0452, K0488, K0516, K0561,
K0565, S0084

Preparation – Design Considerations

Course | 1 hour 9 minutes
Learn the basic considerations and implementation of diverse controls for web server platform design.

NICE Knowledge and Skill Statements:
K0011, K0057, K0170, K0180, K0286, K0322, K0333,
K0491, K0516, K0560, S0152

Preparation – Hardening

Course | 2 hours 19 minutes
Learn what hardening is and identify the different components that require hardening.

NICE Knowledge and Skill Statements:
K0167, K0205, K0406, S0121
Logs

Course | 1 hour 36 minutes

Explore some of the common log formats and how to customize the web server configuration.

NICE Knowledge and Skill Statements:
K0132, K0412, S0120

Command Line

Course | 2 hours 19 minutes

Learn the purpose of some of the basic command-line tools and how to use them.

NICE Knowledge and Skill Statements:
K0129, K0318, S0019, S0267

Web Application Firewalls

Course | 1 hour 58 minutes

Learn about the different types of WAF configurations, as well as the OWASP CRS and its capabilities.

NICE Knowledge and Skill Statements:
K0049, K0202, K0487, K0561, K0624, S0170

Monitoring

Course | 2 hours 40 minutes

In this course, you'll explore the different elements involved in planning the monitoring of a web server, as well as what to look for on the logs and alarms.

NICE Knowledge and Skill Statements:
K0054, K0180, S0136, S0155

Active Defense

Course | 52 minutes

Understand how to deploy active defense mechanisms that would allow the web server to prevent or delay attacks.

NICE Knowledge and Skill Statements:
K0005, K0006, K0013
Windows 10 Host Security

This learning path is for anyone who works with Windows computers and wants to gain insights on protecting their hosts both in SOHO and enterprise environments. See how your organization can benefit by protecting your Windows 10 computers from malware, wireless hacking, open firewall ports, browsing the web and much more.

Skill Assessment

Skill assessment | 20 questions
See how your Windows 10 host security skills stack up against other professionals in your field.

Windows 10 Host Security Project

Project | 2 hours 24 minutes
Practice your Windows 10 Host Security skills by solving challenges.

NICE Knowledge and Skill Statements:
S0067, S0076, S0079, S0158, S0267, S0268

Introduction and Overview of Windows 10 Host Security

Course | 10 minutes
An introduction on the Windows 10 operating system and a history of Windows security issues and features in Windows 10 that can protect your host.

NICE Knowledge and Skill Statements:
K0060

Data Security

Course | 1 hour 13 minutes
Data security in these videos is about protecting access from people who shouldn't have access. NTFS security and share permissions are covered so you know how to properly share files and folders securely for your Windows hosts.

NICE Knowledge and Skill Statements:
K0117, K0062, S0067

Authentication Mechanisms

Course | 37 minutes
There are policies in place to allow you to log into a computer and set the security to keep non-authorized personnel from accessing that data. These policies and procedures are demonstrated in this course.

NICE Knowledge and Skill Statements:
K0065, K0336, K0452, K0608, S0067

Hardening Techniques

Course | 46 minutes
Learn how to update and patch your Windows 10 hosts both locally and through Active Directory automatically. You'll also learn about firewalls and Windows Defender.

NICE Knowledge and Skill Statements:
K0406, K0452, K0608, S0067, S0076, S0084, S0121
<table>
<thead>
<tr>
<th><strong>Local Group and Security Policy</strong></th>
<th><strong>Web Browser Security</strong></th>
<th><strong>User Account Management</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>16 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Local policies drive security in Windows 10 in ways many don't realize. Learn how to configure them in a few simple steps.</td>
<td>Browsing the web is one of the two biggest malware risks with Windows 10, with email being the second. Learn how to secure the Edge web browser in your Windows 10 hosts to keep malware away from your computer.</td>
<td>There are many types of accounts, but do you know the best policy for what type you should use when logging onto your Windows 10 host? In this course, we explain and demonstrate these features and options.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0065, K0608, S0043, S0067, S0121</td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0349, K0608, S0067</td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0608, S0067, S0121</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Application Management</strong></th>
<th><strong>Certificates</strong></th>
<th><strong>Auditing Features</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>30 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Let's talk about keeping your computer safe while loading applications. Utilizing AppLocker, isolation and assigned access can help you do that. These concepts are discussed and demonstrated in this course.</td>
<td>Why do we need certificates on our Windows 10 host? This course covers the many different reasons for and types of certificates, helping you understand how and why you need them.</td>
<td>Windows logs tell us how our computer is doing and whether we should focus on any piece of hardware or software to fix an impending issue that could result in a breach.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0480, K0608, K0610, S0067, S0121</td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0056, K0608, S0067, S0121, S0138</td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0363, K0452, K0608, S0067</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Backup and Recovery</strong></th>
<th><strong>Wireless Security</strong></th>
<th><strong>Remote Access Security</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>56 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>In case of disaster, encryption or other malady, you can use the different types of Windows backups to bring your data back as soon as possible to your Windows 10 hosts.</td>
<td>More computers connect wirelessly to their corporate LAN and the internet than ever before. Learn about the different encryption types and the most secure way to connect.</td>
<td>Road warriors keep companies running by being able to sell anywhere. You need a secure platform from which to do this, and in this course we discuss and demonstrate these concepts.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0021, K0210, K0440, K0480, K0608, S0067</td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0071, K0104, K0375, K0428, K0452, K0608, S0067</td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0071, K0104, K0247, K0375, K0608, S0067, S0267</td>
</tr>
</tbody>
</table>
Windows Server Security

Windows Server Security provides an in-depth introduction to the details of securing and handling your Windows server. You’ll look at access control networks, passwords, authentication, firewall security, Edge browsing security, physical security, disaster recovery and more.

Skill Assessment
Skill assessment | 20 questions
See how your Windows Server security skills stack up against other professionals in your field.

Windows Server Security Project
Project | 2 hours 13 minutes
Practice your Windows Server security skills by solving challenges.

NICE Knowledge and Skill Statements:
S0136, S0158, S0367

Introduction and Overview of Windows Server Security
Course | 18 minutes
Microsoft has increased the amount of diversity of security features, but many of them are not well-advertised or enabled by default. In this course, you'll be introduced to the Windows Server OS and basic security.

NICE Knowledge and Skill Statements:
K0060, K0077

Access Control Network
Course | 51 minutes
Explore data security, NTFS security and share permissions so that you know how to properly share files and folders securely for your Windows servers.

NICE Knowledge and Skill Statements:
K0007, K0033, K0049, K0065, K0117, K0622, S0067

Password and Authentication
Course | 40 minutes
There are many ways to log into a computer such as two-factor authentication (2FA), picture passwords and PINs. In this course, you'll explore discussions and demos show the security values of each type.

NICE Knowledge and Skill Statements:
K0065, K0336, K0452, K0608, S0067

Updating Your Server for Security
Course | 25 minutes
WSUS can alleviate many pressures on IT administrators by allowing the approval, push and removal of updates instead of relying on Microsoft to do it for them. Explore the details of server updates in this course.

NICE Knowledge and Skill Statements:
S0067, S0121
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Security, Routing and VPNs</strong></td>
<td>69 minutes</td>
<td>K0104, K0406, K0452, K0608, S0067, S0076, S0084, S0121</td>
</tr>
<tr>
<td><strong>Edge Browsing Security</strong></td>
<td>17 minutes</td>
<td>K0349, K0608, S0067</td>
</tr>
<tr>
<td><strong>Local Account Security</strong></td>
<td>24 minutes</td>
<td>K0608, S0067, S0121</td>
</tr>
<tr>
<td><strong>Malware and Certificates</strong></td>
<td>67 minutes</td>
<td>K0056, K0480, K0608, S0067, S0121, S0138</td>
</tr>
<tr>
<td><strong>Event Logs</strong></td>
<td>25 minutes</td>
<td>K0363, K0452, K0608, S0067</td>
</tr>
<tr>
<td><strong>Backups and Disaster Recovery</strong></td>
<td>41 minutes</td>
<td>K0021, K0210, K0440, K0480, K0608, S0067</td>
</tr>
<tr>
<td><strong>Physical Security</strong></td>
<td>11 minutes</td>
<td>K0026, K0065, K0487</td>
</tr>
<tr>
<td><strong>Hyper-V Security</strong></td>
<td>14 minutes</td>
<td>K0130, K0610</td>
</tr>
</tbody>
</table>

Learn to protect your servers by blocking open ports in your firewall and making sure your computer is up to date. You'll also learn how to create custom firewall rules and what types of ports are most vulnerable to your host computer.

Learn how to install and secure the Chromium Edge web browser, as well as utilizing local policies to protect everyone who uses your computer even when you're away from it.

Administrator and non-administrator accounts are used for different reasons. Learn how to use policies, single sign-on and UAC to protect yourself and anyone else who uses your computer.

Learn how to install a CA root server and have clients trust your certificates in order to avoid paying for costly public ones. You'll also learn about how to detect malware and protect your server from various attacks.

Using Windows logs is a quick way to view the status of our Windows server. In this course, you'll look at the various types of logs in Windows operating systems and how to use them to troubleshoot programs and services.

When all else fails, Windows and third-party backup systems can protect your Windows servers by restoring data to new or existing server equipment. Learn how to restore and use shadow copies to enable users to restore their own files.

Not everyone knows that there are actually multiple types of backup schemes. Learn about backup types, shadow copies and the quickest ways to restore data after a disaster.

There are multiple ways to protect your physical and virtual servers. Many of these are not enabled and some cause conflicts with other options. Learn what works well together and how they can protect your server environment.
Pentesting and vulnerability management training is focused on identifying, classifying, prioritizing, remediating and mitigating weaknesses in systems. It covers pentesting methodologies and vulnerability assessments, as well as exploiting systems and effectively communicating findings to key stakeholders.

Advanced Cybersecurity Concepts

The Advanced Cybersecurity Concepts skill path goes beyond the topics covered in entry-level security courses. You'll learn about reverse engineering malware, ethical hacking, Web application penetration testing and popular security frameworks.

---

**Purple Team Privilege Escalation Project**

- **Project** | 2 hours 9 minutes
- This project contains three labs focused on understanding, exploiting and mitigating vulnerabilities that allow a user to escalate their privileges.

**NICE Knowledge and Skill Statements:**

50266, 50267

---

**Introduction to Reverse Engineering**

- **Course** | 47 minutes
- Take a closer look at the art and science of reverse-engineering with a course on machine code, assembly language, system-level reversing and more.

**NICE Knowledge and Skill Statements:**

K0175, K0372

---

**Introduction to Ethical Hacking**

- **Course** | 38 minutes
- Discover the basics of ethical hacking in this introductory course covering penetration testing methodologies and tools as well as an introduction to Linux.

**NICE Knowledge and Skill Statements:**

K0119, K0151, K0161, K0177, K0295, K0310, K0344, K0474, K0548

---

**Introduction to Web Application Pentesting**

- **Course** | 19 minutes
- Begin your pentesting path with this foundational introduction to Web application pentesting, covering common threats, methodologies and more.

**NICE Knowledge and Skill Statements:**

K0004, K0070, K0119, K0342, K0624

---

**Information Security Frameworks**

- **Course** | 21 minutes
- Get insight into a number of popular security frameworks and learn how they're used to implement controls and manage risk.

**NICE Knowledge and Skill Statements:**

K0002, K0047, K0165, K0261, K0297, K0527

---
Cloud Pentesting

Learn the basics of penetration testing in the cloud.

AWS Cloud Pentesting

Course | 40 minutes

The Cloud Pentesting with AWS learning path will give you hands-on experience with navigating, identifying, and exploiting targets located in the cloud.

NICE Knowledge and Skill Statements:
K0004, K0194, K0230, K0342, K0447, S0051, S0073, S0263

Azure Cloud Pentesting

Course | 36 minutes

The Cloud Pentesting with Azure learning path will give you hands-on experience with navigating, identifying, and exploiting targets located in the cloud.

NICE Knowledge and Skill Statements:
K0004, K0194, K0230, K0342, K0447, K0449, S0051, S0073, S0263

Use code "learnskills" to get 30 days for $1
CompTIA PenTest+

The CompTIA PenTest+ certification path teaches you how to successfully plan, carry out and report the results of a penetration test. You’ll learn the process behind penetration testing, tools and techniques used by pentesters, legal and compliance issues and more.

**Skill Assessment**

Skill assessment | 20 questions

See how your PenTest+ skills stack up against other professionals in your field.

**PenTest+ Practice Exam**

Practice Exam | 71 questions

Prepare for your PenTest+ exam and test your domain knowledge.

**Introduction to PenTest+**

Course | 8 minutes

This course serves as an introduction to the CompTIA PenTest+ certification.

**Planning for an Engagement**

Course | 29 minutes

Review the art of planning for a pentesting engagement with five videos on methodology, scoping and more.

**Scoping an Engagement**

Course | 35 minutes

Learn about scoping a pentesting engagement in six videos covering assessment types, target selection and more.

**Information Gathering**

Course | 1 hour 4 minutes

Ten videos take you through the many methods of information gathering, including scanning, enumeration, cryptographic inspection and eavesdropping. Includes demonstrations.

NICE Knowledge and Skill Statements:

- K0003, K0004, K0005, K0119, K0177, K0206, K0342, K0474, K0527
- K0004, K0005, K0119, K0177, K0206, K0342, K0409, K0536, S0051, S0081
### Vulnerability Scanning

**Course** | 24 minutes

Review the process of vulnerability scanning, common vulnerability scanning tools and scan analysis with this four-video course.

**NICE Knowledge and Skill Statements:**
K0113, K0202, K0324, K0452, K0488, K0516, K0561, K0565, S0084

---

### Preparing for Exploitation

**Course** | 20 minutes

Three videos help you prepare for exploitation with an in-depth review of common attack techniques, leveraging information for exploitation and weaknesses in specialized systems.

**NICE Knowledge and Skill Statements:**
K0005, K0070, K0106, K0119, K0147, K0177, K0206, K0314, K0322, K0342, K0437, K0536, S0051, S0242

---

### Social Engineering and Physical Attacks

**Course** | 26 minutes

Social engineering takes center stage in this four-video course covering social engineering attack methods, motivation factors and physical security attacks.

**NICE Knowledge and Skill Statements:**
K0119, K0206, K0234, K0342, S0052

---

### Exploiting Network and Application Vulnerabilities

**Course** | 47 minutes

Explore system weak points and methods of attack with this four-video course on exploiting network and application vulnerabilities.

**NICE Knowledge and Skill Statements:**
K0005, K0009, K0070, K0106, K0119, K0192, K0206, K0342, K0362, K0536, K0565, K0624, S0051

---

### Exploiting Host-based Vulnerabilities

**Course** | 28 minutes

Learn about host-based vulnerabilities in this five-video course covering privilege escalation and escalation techniques.

**NICE Knowledge and Skill Statements:**
K0060, K0119, K0177, K0206, K0314, K0342, K0536, S0051

---

### Post-exploitation Activities

**Course** | 29 minutes

Take a look at post-exploitation activities with four videos on lateral movement, persistence and covering your tracks.

**NICE Knowledge and Skill Statements:**
K0071, K0119, K0177, K0192, K0206, K0342, K0392, K0536, S0051, S0293

---

### Using Nmap for Pentesting

**Course** | 24 minutes

Get to grips with the power of Nmap in this three-video course on using Nmap for pentesting.

**NICE Knowledge and Skill Statements:**
K0192, K0206, K0342, K0536, S0051, S0081

---

### Use Cases of Pentesting Tools

**Course** | 41 minutes

Explore pentesting tools with thirteen videos on Web proxies, debuggers, exploitation frameworks and more.

**NICE Knowledge and Skill Statements:**
K0177, K0188, K0206, K0301, K0334, K0342, K0536, S0051

---

### Basic Script Analysis

**Course** | 40 minutes

Python Code Security Cyber Range
Reporting and Communication

Course | 30 minutes

Make sure that critical findings reach the client with the help of this five-video course on reporting and communication.

NICE Knowledge and Skill Statements:
K0177, K0315, K0342, K0394, S0278

PenTest+ Conclusion

Course | 11 minutes

Wrap up your survey of pentesting with a tutorial on setting up your home pentesting lab.

NICE Knowledge and Skill Statements:
EC-Council CEH

CERTIFICATION PATH

The Certified Ethical Hacker (CEH) certification path teaches you the hacking skills necessary to successfully perform a penetration test. You’ll learn the techniques and tools used by cybercriminals and how to apply them to conduct security assessments and report your findings.

**Skill Assessment**

Skill assessment | 20 questions

See how your CEH skills stack up against other professionals in your field.

**CEH Practice Exam**

Practice Exam | 1017 questions

Prepare for your CEH exam and test your domain knowledge.

**Penetration Testing Cyber Range**

Cyber range | 34 labs

Gain practical experience and build your real-world pentesting skills through 34 hands-on labs in the Penetration Testing Cyber Range.

**Introduction to Ethical Hacking**

Course | 38 minutes

Discover the basics of ethical hacking in this introductory course covering penetration testing methodologies and tools as well as an introduction to Linux.

*NICE Knowledge and Skill Statements:*
K0119, K0151, K0161, K0177, K0295, K0310, K0344, K0474, K0548

**Passive Intelligence Gathering**

Course | 1 hour 17 minutes

Learn about passive intelligence gathering, one of the key aspects of ethical hacking, in this four-video overview course.

*NICE Knowledge and Skill Statements:*
K0061, K0301, K0332, K0409, K0544, K0555, K0565, S0295

**Network Recon**

Course | 39 minutes

Learn the process of network reconnaissance and how it relates to ethical hacking, including tools, scan types and identifying vulnerable systems.

*NICE Knowledge and Skill Statements:*
K001, K0177, K0192, K0300, K0339, S0081, S0167, S0242, S0291, S0294
<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fundamentals of Exploitation</strong></td>
<td>47 minutes</td>
</tr>
<tr>
<td><strong>Breaking Password Security</strong></td>
<td>27 minutes</td>
</tr>
<tr>
<td><strong>Attacking Web Servers and Applications</strong></td>
<td>35 minutes</td>
</tr>
<tr>
<td><strong>Post-Exploitation Techniques</strong></td>
<td>43 minutes</td>
</tr>
<tr>
<td><strong>Attacking Wireless Networks</strong></td>
<td>21 minutes</td>
</tr>
<tr>
<td><strong>IoT Security</strong></td>
<td>11 minutes</td>
</tr>
<tr>
<td><strong>Covering Tracks</strong></td>
<td>11 minutes</td>
</tr>
<tr>
<td><strong>Cryptography Fundamentals</strong></td>
<td>38 minutes</td>
</tr>
<tr>
<td><strong>Information Security Frameworks</strong></td>
<td>21 minutes</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**

- **Fundamentals of Exploitation:** K0070, K0106, K0160, K0177, K0362, K0536, S0078
- **Breaking Password Security:** K0362, K0536
- **Attacking Web Servers and Applications:** K0009, K0070, K0373, K0398, K0624
- **Post-Exploitation Techniques:** K0070, K0177, K0188, K0191, K0209, K0259, K0324, K0392, K0430, K0479, K0480, S0293
- **Attacking Wireless Networks:** K0375, K0428
- **IoT Security:** K0115, K0147, K0309
- **Covering Tracks:** K0177, K0184
- **Cryptography Fundamentals:** K0018, K0019, K0305, K0308, K0427
- **Information Security Frameworks:** K0002, K0047, K0165, K0261, K0297, K0527

**Use code “learnskills” to get 30 days for $1**

**GET STARTED**
Ethical Hacking

The Ethical Hacking skill path helps you master a repeatable, documentable penetration testing methodology. You'll learn how to use the same techniques used by malicious hackers to carry out an ethical hack and assess your organization's vulnerabilities.

Penetration Testing Cyber Range

Cyber range | 34 labs

Gain practical experience and build your real-world pentesting skills through 34 hands-on labs in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:
S0001, S0025, S0046, S0051, S0052, S0078, S0081, S0094, S0137, S0156, S0221, S0267, S0293, S0295

Purple Team Web Application Security Project

Project | 2 hours 34 minutes

This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application.

NICE Knowledge and Skill Statements:
S0022, S0025, S0051, S0084, S0172, S0174, S0293

Ethical Hacking Process

Course | 1 hour 8 minutes

Introduce yourself to ethical hacking with this course covering concepts, terminology and the ethical hacking process, step-by-step from passive reconnaissance to post-exploitation and reporting.

NICE Knowledge and Skill Statements:
K0004, K0119, K0177, K0206, K0342

Passive Intelligence Sources, Tools and Techniques

Course | 1 hour 29 minutes

Get to grips with the crucial tools and techniques associated with passive intelligence gathering. Explore intelligence-gathering goals, sources and concepts. Includes vocabulary and definitions.

NICE Knowledge and Skill Statements:
K0119, K0206, K0342, K0409, S0051

Understanding TCP/IP Communications

Course | 52 minutes

In this course, you'll explore TCP/IP communications specifically for ethical hackers. You'll take a look at TCP, UDP and ICMP, and examine TCP communications through in-depth demonstrations in Wireshark.

NICE Knowledge and Skill Statements:
K0119, K0206, K0221, K0301, K0342, K0471, S0046, S0051

Network Reconnaissance

Course | 38 minutes

You can't launch an attack without some careful reconnaissance. In this course, you'll look at network reconnaissance goals and concepts, including host discovery, port scanning and service identification.

NICE Knowledge and Skill Statements:
K0119, K0177, K0206, K0221, K0318, K0342, K0565, S0001, S0051, S0081
<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Table of contents</th>
<th>Boot camps</th>
<th>Self-paced training</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
</table>

### Stealthy Network Reconnaissance

**Course | 30 minutes**

Reconnaissance isn't much good if you're spotted while you're doing it. Explore what it takes to carry out stealthy network reconnaissance with this course covering strategies and stealthy scanning methods.

**NICE Knowledge and Skill Statements:**
K0111, K0119, K0177, K0206, K0221, K0318, K0342, K0565, S0001, S0051, S0081

### Finding and Exploiting Vulnerabilities

**Course | 53 minutes**

A vulnerability is as good as another tool for an ethical hacker. Learn the fundamentals of finding and exploiting vulnerabilities with this course covering exploits, buffer overflows, DLL hijacking and much more.

**NICE Knowledge and Skill Statements:**
K0070, K0119, K0165, K0177, K0342, K0362, K0480, K0536, K0604, S0001, S0051

### Sniffing

**Course | 1 hour 2 minutes**

There are a number of ways to carry out sniffing. In this course, you'll explore what it takes to sniff internet traffic, as well as sniffing techniques with packetrecorder, useful tips for sniffing on public Wi-Fi networks and more.

**NICE Knowledge and Skill Statements:**
K0058, K0061, K0108, K0111, K0119, K0177, K0342, K0446, K0536, S0001, S0051, S0156

### Cracking Passwords

**Course | 36 minutes**

Cracking a password effectively opens the door into an account or system. Explore the details of cracking passwords, including understanding and capturing Windows passwords and useful tools such as Cain & Abel.

**NICE Knowledge and Skill Statements:**
K0177, K0342, K0362, K0536, S0001, S0051, S0067

### Covert Channels and IDS Evasion

**Course | 39 minutes**

An intrusion detection system, or IDS, can be a problem for an ethical hacker. In this course, you'll get to grips with the use of covert channels and evading an intrusion detection system. Includes demonstrations.

**NICE Knowledge and Skill Statements:**
K0177, K0184, K0305, K0324, K0342, K0403, K0472, K0493, K0536, S0001, S0051, S0092

### Using Trojans and Backdoors

**Course | 31 minutes**

Ethical hackers need to be familiar with hackers’ tricks, and even be able to use them for helpful purposes. With this course, you'll look at using Trojans and backdoors in an ethical hack, both hiding and detecting backdoor activity.

**NICE Knowledge and Skill Statements:**
K0129, K0177, K0318, K0342, K0536, S0001, S0051, S0267

### Exploit Writing Fundamentals: Basic Buffer Overflow Exploit

**Course | 53 minutes**

Get to grips with the basic buffer overflow exploit in this course. Modules cover understanding memory, initial discovery, fuzzing, vulnerability identification and more. Includes demonstrations.

**NICE Knowledge and Skill Statements:**
K0070, K0119, K0177, K0206, K0318, K0342, S0001, S0051, S0081

### Exploiting Common Web Application Vulnerabilities

**Course | 51 minutes**

Learn how to carry out ethical hacks such as cross-site scripting and SQL injection.

**NICE Knowledge and Skill Statements:**
K0070, K0119, K0177, K0206, K0318, K0342, K0624, S0001, S0051, S0081
Certified Expert Penetration Tester (CEPT)

The Certified Expert Penetration Tester (CEPT) certification path teaches you advanced hacking tools and techniques. You’ll learn how to successfully attack fully patched and hardened systems, how to circumvent common security controls, and how to defend your organization against advanced persistent threats.

**Certification Path**

**Skill Assessment**

Skill assessment | 20 questions

See how your CEPT skills stack up against other professionals in your field.

**CEPT Practice Exam**

Practice Exam | 75 questions

Prepare for your CEPT exam and test your domain knowledge.

**Purple Team Privilege Escalation Project**

Project | 2 hours 9 minutes

This project contains three labs focused on understanding, exploiting and mitigating vulnerabilities that allow a user to escalate their privileges.

NICE Knowledge and Skill Statements:

S0266, S0267

**Introduction to Advanced Hacking**

Course | 7 minutes

A brief overview of the topics that you need to know about advanced hacking.

NICE Knowledge and Skill Statements:

K0003, K0004, K0119, K0177, K0206, K0342

**Advanced Reconnaissance**

Course | 26 minutes

Discover some of the techniques pentesters can use in complex environments.

NICE Knowledge and Skill Statements:

K0004, K0005, K0061, K0119, K0129, K0177, K0179, K0206, K0255, K0318, K0324, K0342, K0486, K0489, K0529, K0536, S0051, S0081

**Finding Vulnerabilities in Software**

Course | 57 minutes

Learn both manual and automated techniques for discovering vulnerabilities in apps.

NICE Knowledge and Skill Statements:

K0004, K0005, K0013, K0119, K0177, K0186, K0188, K0206, K0342, K0529, K0536, S0051, S0081, S0137, S0167, S0242
<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Exploit Writing</strong></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>47 minutes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Explore various exploits and how to choose the right Metasploit payload.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0005, K0016, K0068, K0070, K0119, K0177, K0186, K0188, K0206, K0234, K0342, K0372, K0536, S0019, S0051, S0130</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Advanced Exploitation</strong></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>34 minutes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Learn concepts of advanced threats and how to use them in pentesting.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0004, K0069, K0070, K0115, K0119, K0129, K0162, K0177, K0206, K0342, K0447, K0452, K0529, K0536, K0624, S0051, S0167, S0267</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>AEH Wrap Up</strong></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>3 minutes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The key takeaways you need for becoming an ethical hacker.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0119, K0206, K0342</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Certified Mobile and Web App Penetration Tester

The Certified Mobile and Web App Penetration Tester (CMWAPT) certification path teaches you the skills, tools and techniques required for conducting comprehensive security tests of mobile and Web applications.

**Skill Assessment**

Skill assessment | 20 questions

See how your CMWAPT skills stack up against other professionals in your field.

**CMWAPT Practice Exam**

Practice Exam | 44 questions

Prepare for your CMWAPT exam and test your domain knowledge.

**Purple Team Web Application Security Project**

Project | 2 hours 34 minutes

This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application.

**NICE Knowledge and Skill Statements:**

S0022, S0025, S0051, S0084, S0172, S0174, S0293

**Introduction to Web Application Pentesting**

Course | 19 minutes

Begin your pentesting path with this foundational introduction to Web application pentesting, covering common threats, methodologies and more.

**NICE Knowledge and Skill Statements:**

K0004, K0070, K0119, K0342, K0624

**Target Identification and Application Mapping**

Course | 54 minutes

Take a closer look at target identification and application mapping with this course covering service identification, core defense mechanisms and more. Includes vocabulary and tools.

**NICE Knowledge and Skill Statements:**

K0070, K0077, K0286, K0342, K0408, K0624, S0051, S0081

**Attacking Web Application Access Controls**

Course | 27 minutes

Learn to attack web application access controls with this course on attacking access control, attacking authentication, attacking session management and more.

**NICE Knowledge and Skill Statements:**

K0007, K0070, K0077, K0105, K0177, K0286, K0336, K0342, K0624, S0051
Injection Attacks

Course | 19 minutes
Learn what you need to know about injecting code or SQL queries into vulnerable applications in order to circumvent access controls. Includes vocabulary and examples.

NICE Knowledge and Skill Statements:
K0070, K0105, K0177, K0342, K0624, S0051

Common Attack Methods

Course | 37 minutes
Think like a hacker with this course on common attack methods used for pentesting, including attacking Web services, cross-site scripting and exploiting logic flaws.

NICE Knowledge and Skill Statements:
K0070, K0105, K0177, K0342, K0624, S0051

Introduction to iOS App Pentesting

Course | 33 minutes
Get an introduction to iOS app pentesting with this course covering analyzing an iOS app, binary analysis, iOS app security measures and more.

NICE Knowledge and Skill Statements:
K0060, K0070, K0224, K0269, K0342, K0438, K0624

iOS App Pentesting Tools and Techniques

Course | 45 minutes
Be ready for action with this course on iOS app pentesting tools and techniques. Covers runtime manipulation, insecure data storage, broken cryptography and other ways to get into a target system.

NICE Knowledge and Skill Statements:
K0060, K0070, K0140, K0177, K0224, K0269, K0342, K0438, K0624, S0051

Introduction to Android App Pentesting

Course | 20 minutes
Prepare for the challenge of Android app pentesting with this introductory course covering reversing Android applications, Drozer and more.

NICE Knowledge and Skill Statements:
K0060, K0070, K0224, K0269, K0342, K0438, K0624

Android App Pentesting Tools and Techniques

Course | 30 minutes
Dive deeper into Android app pentesting with this course on Android app pentesting tools and techniques. Includes vocabulary, walkthroughs and a close look at the Frida pentesting toolkit.

NICE Knowledge and Skill Statements:
K0060, K0070, K0140, K0177, K0224, K0269, K0342, K0438, K0624, S0051
Introduction to Vulnerability Management

The Introduction to Vulnerability Management Learning Path will enable you to master a repeatable, documented and continuously improving vulnerability management program. You will learn how to use the same techniques used by organizations with mature vulnerability management programs covering tens of thousands of endpoints.

**Skill Assessment**

Skill assessment | 20 questions

See how your vulnerability management skills stack up against other professionals in your field.

**Vulnerability Management Project**

Project | 2 hours 34 minutes

Put your skills to the test as you identify risky open ports, find vulnerabilities in the operating system and SMB service, verify vulnerabilities and find their CVSS score, investigate how to remediate the vulnerabilities and more.

**Introduction to Vulnerability Management**

Course | 23 minutes

In the first course, we will take a look at what this learning path is all about. We will discuss what we will learn, how we will learn it and what you will be able to do with that knowledge.

**Setting Up Your System**

Course | 22 minutes

This course will go over setting up the VirtualBox environment with the Kali Linux and Metasploitable 2 and 3 VMs. You will also set up Nessus, nmap and OpenVAS.

**Vulnerability Management Process**

Course | 1 hour 3 minutes

Explore the vulnerability management process in detail. We go over determining the scope of the program, defining the strategy, selecting the methodology and selecting the tools, as well as engaging management and stakeholders.

**Automated Vulnerability Scanners**

Course | 36 minutes

In this course, we will look at what automated vulnerability scanners are, how to use them and why they are useful.
Manual Vulnerability

Course | 1 hour 3 minutes

In this course, we will look at how to manually verify the existence of several different vulnerabilities with a wide array of tools. We will look at Metasploit, nmap, netcat and Wireshark.

NICE Knowledge and Skill Statements:
K0005, K0013, K0070, K0342

Prioritizing Vulnerabilities

Course | 14 minutes

This course will cover how to prioritize vulnerabilities in our environment based on industry standard metrics (CVSS) as well as a risk-based approach based on what is important to our organization.

NICE Knowledge and Skill Statements:
K0165

Remediation

Course | 27 minutes

In this course, we will look at best practices for establishing and running an effective patch management program.

NICE Knowledge and Skill Statements:
K0002, K0040, K0074

Web Application Vulnerabilities

Course | 53 minutes

This course will look at some of the most common web application vulnerabilities, as well as open-source and commercial scanners that can be used to detect them.

NICE Knowledge and Skill Statements:
K0009, K0013, K0070, K0624

Frameworks

Course | 47 minutes

This course will examine what role vulnerability management plays in different industry frameworks. We will accomplish this by looking at specific requirements and controls from each of the frameworks discussed.

NICE Knowledge and Skill Statements:
K0047, K0048, K0261

Vulnerability Management Summary

Course | 1 hour 19 minutes

This course will recap everything we have learned throughout the path, including the VM process, automated scanning, manual verification (with demo), prioritization, remediation and web application vulnerabilities.

NICE Knowledge and Skill Statements:
Machine Learning for Red Team Hackers

Learn the ins and outs of hacking machine learning. The learning path covers topics such as hacking a CAPTCHA system, fuzzing a target, evading malware detection and attacking machine learning systems. You will also learn about deepfakes and how to perform backdoor attacks on machine learning.

Skill Assessment

Skill assessment | 20 questions

See how your Machine Learning for Red Team Hackers skills stack up against other professionals in your field.

Introduction to Machine Learning for Red Team Hackers

Course | 2 minutes

Get an overview of what to expect in the Machine Learning for Red Team Hackers Learning Path, including highlights of course topics and a brief description of the path's hands-on assignments.

NICE Knowledge and Skill Statements:
K0004

Hacking CAPTCHA Systems

Course | 1 hour 57 minutes

Learn how to implement and use a CAPTCHA-evading bot from scratch, including training and designing a deep neural network, using selenium to automate the CAPTCHA evasion and using the created bot on a webpage designed to be attacked.

NICE Knowledge and Skill Statements:
K0238

Smart Fuzzing

Course | 49 minutes

In this course, you'll write a custom evolutionary fuzzer that employs machine learning to fuzz a target. You'll also learn the machine learning behind, as well as how to use, AFL.

NICE Knowledge and Skill Statements:
K0238

Evading Machine Learning Malware Classifiers

Course | 21 minutes

In this course, you'll learn how to modify malware so it is able to get past neural network and gradient boosting machine learning malware classifiers.

NICE Knowledge and Skill Statements:
K0238

Adversarial Machine Learning

Course | 33 minutes

Learn how to perform white-box and black-box attacks on machine learning classifiers in this course.

NICE Knowledge and Skill Statements:
K0238
Deepfake

Course | 26 minutes
This course helps you understand the implications of the deepfake technology, setup an environment for performing deepfakes and then create a deepfake video.

NICE Knowledge and Skill Statements:
K0238

Hacking Machine Learning

Course | 14 minutes
This course will teach you some of the darker, less publicized attacks on machine learning, including how to poison, backdoor and steal machine learning models.

NICE Knowledge and Skill Statements:
K0238
Mobile Application Pentesting

The Mobile Application Pentesting skill path teaches you how to discover and exploit vulnerabilities in mobile apps. You’ll learn how to use popular penetration testing tools to perform an analysis of mobile applications, assess their weaknesses and better defend them from malicious attacks.

<table>
<thead>
<tr>
<th>SKILL PATH</th>
<th>SKILL PATH</th>
<th>SKILL PATH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile Application Pentesting Project</strong></td>
<td><strong>Introduction to iOS App Pentesting</strong></td>
<td><strong>iOS App Pentesting Tools and Techniques</strong></td>
</tr>
<tr>
<td>Project</td>
<td>Course</td>
<td>Course</td>
</tr>
<tr>
<td>4 hours</td>
<td>33 minutes</td>
<td>45 minutes</td>
</tr>
</tbody>
</table>

**Mobile Application Pentesting Project**

Practice your mobile application pentesting skills by working on hands-on exercises.

**NICE Knowledge and Skill Statements:**

S0001, S0137

---

**Introduction to iOS App Pentesting**

Get an introduction to iOS app pentesting with this course covering analyzing an iOS app, binary analysis, iOS app security measures and more.

**NICE Knowledge and Skill Statements:**

K0060, K0070, K0224, K0269, K0342, K0438, K0624

---

**iOS App Pentesting Tools and Techniques**

Be ready for action with this course on iOS app pentesting tools and techniques. Covers runtime manipulation, insecure data storage, broken cryptography and other ways to get into a target system.

**NICE Knowledge and Skill Statements:**

K0060, K0070, K0140, K0177, K0224, K0269, K0342, K0438, K0624, S0051

---

**Introduction to Android App Pentesting**

Prepare for the challenge of Android app pentesting with this introductory course covering reversing Android applications, Drozer and more.

**NICE Knowledge and Skill Statements:**

K0060, K0070, K0224, K0269, K0342, K0438, K0624

---

**Android App Pentesting Tools and Techniques**

Dive deeper into Android app pentesting with this course on Android app pentesting tools and techniques. Includes vocabulary, walkthroughs and a close look at the Frida pentesting toolkit.

**NICE Knowledge and Skill Statements:**

K0060, K0070, K0140, K0177, K0224, K0269, K0342, K0624, S0051
Offensive Bash Scripting

The Offensive Bash Scripting Learning Path is aimed at beginners and helps you learn one of the many fundamental skills of ethical hacking.
### File Permission and Process

**Course | 26 minutes**

In this course, we will segue from user and group management to focusing on file processes and permissions. We will go into the meaning of read, write and execute and more useful terms.

**NICE Knowledge and Skill Statements:**
K0016, K0068, K0116, K0129, K0224, K0396, K0529, K0608, S0067, S0130

### Network Reconnaissance

**Course | 28 minutes**

Explore the uses of Bash scripts for network reconnaissance, as well as how to edit these scanning tools for class B and class C networks and their subnets.

**NICE Knowledge and Skill Statements:**
K0177, K0342, K0529, S0051, S0130, S0162

### Scripting to Scan Web Applications

**Course | 1 hour 2 minutes**

In this course, we will utilize the same tools that we created in the previous course and apply them to scanning web applications and discovering vulnerabilities.

**NICE Knowledge and Skill Statements:**
K0009, K0070, K0339, K0342, K0529, K0624, S0001, S0051, S0081, S0130

### Privilege Escalation

**Course | 19 minutes**

A virtual machine named Kioptrix 4 will be used to demonstrate the process of privilege escalation. You’ll walk through a hands-on exercise to learn what is going on and how the process works.

**NICE Knowledge and Skill Statements:**
K0129, K0177, K0342, K0362, K0529, S0051, S0130
Python for Pentesters

Learn the basics of penetration testing in the cloud.

Skill Assessment

Skill assessment | 20 questions
See how your Python pentesting skills stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

Python for Pentesters Project

Project | 43 minutes
Test your skills in this project consisting of five challenges: create an email sender, create a buffer overflow exploit, write commands to conduct a Wi-Fi attack, start a new web scraping project and write a line of smtp code.

NICE Knowledge and Skill Statements:
K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266

Refresher on Python

Course | 3 hours 53 minutes
An introduction to the course and some refreshers on Python.

NICE Knowledge and Skill Statements:
K0004, K0016, K0068, K0372, K0396, S0060, S0266

Common Vulnerabilities Exploitable by Python

Course | 2 hours 20 minutes
This course explores common vulnerabilities and vulnerability exploitation in Python.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0016, K0068, K0070, K0372, K0396, S0060, S0266

Using Python for Network Penetration

Course | 4 hours 19 minutes
In this course, we will explore the uses of Python in penetration testing and attacking.

NICE Knowledge and Skill Statements:
K0004, K0016, K0068, K0070, K0160, K0177, K0221, K0234, K0332, K0362, K0372, K0396, K0408, S0060, S0266

Attacking Web Applications

Course | 1 hour 57 minutes
In this course, you’ll explore the ins and outs of attacking web applications with Python.

NICE Knowledge and Skill Statements:
K0004, K0005, K0009, K0016, K0068, K0070, K0372, K0396, K0624, S0060, S0266
Reverse Engineering

The Reverse Engineering skill path will enable you to identify malware types, characteristics and behaviors. You will be able to detect, analyze and mitigate malware from any network.

Reverse Engineering Project

Project | 2 hours 57 minutes

Get to grips with a real-world challenge as you reverse-engineer a malware sample.

NICE Knowledge and Skill Statements:
K0171, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270

Malware analysis introduction

Course | 48 minutes

This course is the student's introduction to reverse engineering and malware.

NICE Knowledge and Skill Statements:
K0183, K0184, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131

Basic static analysis

Course | 1 hour 3 minutes

Learn how to conduct basic static analysis on a malicious file to gather information about the malware prior to conducting any dynamic analysis.

NICE Knowledge and Skill Statements:
K0175, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270

Advanced static analysis

Course | 1 hour 29 minutes

VPNs (virtual private networks) are essential to secure remote access of your network, and in this course we’ll be focused on how to lock down your network using VPN tunnels and different remote access technologies.

NICE Knowledge and Skill Statements:
K0175, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270

Basic dynamic analysis

Course | 1 hour 20 minutes

In this course, you'll get to grips with malware and basic dynamic analysis.

NICE Knowledge and Skill Statements:
K0175, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270

Advanced dynamic analysis

Course | 2 hours 33 minutes

Complete understanding of a malicious file can be best achieved during advanced dynamic analysis.

NICE Knowledge and Skill Statements:
K0175, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270
Reporting and mitigation

Course | 21 minutes

In this course, the student will explore reporting, mitigation techniques and demonstrating mitigation.

NICE Knowledge and Skill Statements:
K0315, K0354, K0355, K0451, K0468, S0003
Web Application Pentesting

The web application penetration testing path will cover all of the essentials for those wanting to become a web app pentester. You'll learn how to ethically emulate real-world attacks in order to discover and responsibly disclose an organization's vulnerabilities.

**Skill Assessment**

Skill assessment | 20 questions

See how your web application pentesting skills stack up against other professionals in your field.

**Purple Team Web Application Security Project**

Project | 2 hours 34 minutes

This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application.

NICE Knowledge and Skill Statements:
S0022, S0025, S0051, S0084, S0172, S0174, S0293

**Introduction to Web Application Pentesting**

Course | 60 minutes

This course introduces students to the learning path and walks them through getting their own workstation set up and configured for use throughout the rest of the path's courses.

NICE Knowledge and Skill Statements:
K0206, K0342, K0624

**OWASP Top Ten**

Course | 9 hours 16 minutes

In the second course, many real-world vulnerabilities are showcased for each of the ten topics and various demos are given on how to solve related challenges in both OWASP Juice Shop and Portswigger's Web Security Academy.

NICE Knowledge and Skill Statements:
K0005, K0007, K0069, K0070, K0624, S0001, S0130

**Tool Setup and Usage**

Course | 2 hours 29 minutes

The third course covers a variety of pentesting tools and Burp extensions, such as Autorize, C02, Backslash Powered Scanner, Turbo Intruder, Intruder File Payload Generator, SQLMap and many more.

NICE Knowledge and Skill Statements:
K0131, K0182, K0301, K0342, S0051, S0057, S0081, S0173

**Conclusion to Web App Pentesting**

Course | 1 hour 36 minutes

This course offers the student important advice on pentesting, a path recap and a close look at the learning path's final project.

NICE Knowledge and Skill Statements:
K0005, K0206, K0342, K0624
Threat intelligence, incident response and forensics

Threat intelligence, incident response and forensics training includes a variety skills related to identifying, responding to and analyzing cybersecurity incidents. It covers different types of cyberattacks and threats, the processes and policies to mitigate those threats, how to extract and report on cybercrime evidence, and more.

Advanced Adversary Tactics

The Advanced Adversary Tactics Path will give an overview of techniques and tactics used by real-world adversaries. Through completely hands-on exercises you'll get experience with some of the most common methods adversary groups use to gain access to networks and machines by trying them out yourself.

<table>
<thead>
<tr>
<th>Reconnaissance and Resource Development</th>
<th>Initial Access, Execution, and Persistence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>29 minutes</td>
</tr>
<tr>
<td>Learn some of the techniques attackers use to gain information and phish before an attack.</td>
<td>Get hands-on experience with some of the methods used to gain initial access to a system, execute code, and gain persistence. Learn how to implant a trojanized binary, hide a reverse shell in start-up folders and files, pivot between networks, and more.</td>
</tr>
</tbody>
</table>
CERT-Certified Computer Security Incident Handler (CSIH)

The Certified Computer Security Incident Handler (CSIH) certification path covers the essential information you need to know in order to properly detect, contain and mitigate security incidents. You’ll learn the ins and outs of incident response, as well as the tools of the trade used by incident responders on a daily basis.

CSIH Practice Exam

Practice Exam | 30 questions
Prepare for your CSIH exam and test your domain knowledge.

Network Traffic Analysis Cyber Range

Cyber range | 12 labs
Gain practical experience and build your real-world network traffic analysis skills through 12 hands-on labs in the Network Traffic Analysis Cyber Range.

NICE Knowledge and Skill Statements:
S0046, S0120, S0156, S0199, S0221

Building Incident Response Team

Course | 31 minutes
Review the most important aspects of incident response team members, such as technical skills, personal skills and critical knowledge.

NICE Knowledge and Skill Statements:
K0004, K0231, K0292

Reverse Engineering Concepts

Course | 33 minutes
Get to grips with the details of reverse-engineering concepts in this three-video course. Includes demonstration and tool lists.

NICE Knowledge and Skill Statements:
K0004, K0171, K0175, S0270

Cell Phone Forensics

Course | 28 minutes
Refresh your knowledge of cell phone forensics with this course covering Android and iPhone forensics challenges and best practices.

NICE Knowledge and Skill Statements:
K0004, K0017, K0118, K0122, K0128, K0269, K0433, K0438, K0573, S0075, S0090, S0091

Windows Swap File

Course | 27 minutes
Get familiar with the Windows swap file, a great place for evidence to hide. Includes tools and demonstration video.

NICE Knowledge and Skill Statements:
K0004, K0017, K0118, K0122, K0128, K0192, K0433, K0573, S0067, S0075
### Memory Forensics

**Course | 1 hour 19 minutes**

Two videos take you through the fundamentals of memory forensics, including tools, techniques for dumping memory and an in-depth demonstration.

**NICE Knowledge and Skill Statements:**
K0004, K0017, K0118, K0122, K0128, K0433, K0573, S0062, S0075, S0091

### Dealing with Passwords and Encryption

**Course | 33 minutes**

Deal with passwords and encryption with the help of this course covering password-cracking, public and private keys, Kerberos and more.

**NICE Knowledge and Skill Statements:**
K0004, K0007, K0018, K0019, K0056, K0060, K0427, S0043, S0098

### Disk Forensics

**Course | 55 minutes**

Dive into disk forensics with this course covering bit images, restoring disk images, slack, steganography and more.

**NICE Knowledge and Skill Statements:**
K0004, K0017, K0038, K0117, K0118, K0122, K0128, K0129, K0132, K0133, K0304, K0433, K0573, K0622

### Role of the Computer Forensic Examiner

**Course | 40 minutes**

Get to grips with the role of the computer forensics examiner, including duties and potential legal concerns.

**NICE Knowledge and Skill Statements:**
K0004, K0150, K0233, K0579

### Cyber Attacks Overview

**Course | 1 hour 14 minutes**

Review the fundamentals of cyber-attacks with two videos on risks, attack types and the anatomy of an attack.

**NICE Knowledge and Skill Statements:**
K0004, K0070, K0106, K0160, K0161, K0162, K0177, K0362, K0436, K0480, K0604

### Incident Response Process

**Course | 1 hour 1 minute**

Six videos take you through the details of the incident response process, including important tools, policies, strategies and legal concerns.

**NICE Knowledge and Skill Statements:**
K0004, K0042, K0231, K0292, K0317, K0399, S0365

### Introduction to Incident Response

**Course | 56 minutes**

Get on overview of incident response, including how to respond to security incidents and common incident response definitions and concepts.

**NICE Knowledge and Skill Statements:**
K0004

### Stages of Incident Response

**Course | 1 hour**

Review the stages of incident response in two separate models, covering the details and concerns for each phase.

**NICE Knowledge and Skill Statements:**
K0004, K0042, K0231, K0292, K0317, K0399, S0365

### Email Analysis

**Course | 21 minutes**

Explore forensic email analysis with this course covering the structure, function and details of email.

**NICE Knowledge and Skill Statements:**
K0004, K0192, K0268, K0332, K0444, K0447, K0449, K0565, S0071
Web Traffic Analysis

Course | 13 minutes

Dig into Web traffic analysis with this course covering write protection, Web forensics and cookies.

NICE Knowledge and Skill Statements:
K0004, K0061, K0179, K0255, K0274, K0332, K0444, K0471, K0486, K0489, K0565, K0603

Wireless Analysis

Course | 38 minutes

Take a moment to refresh your knowledge of wireless analysis. Includes vocabulary, examples and diagrams.

NICE Knowledge and Skill Statements:
K0004, K0056, K0093, K0108, K0113, K0137, K0138, K0274, K0375, K0428, K0438, K0445, K0446, K0556, K0560, K0614, S0138

Protocol Analysis

Course | 19 minutes

Get to grips with protocol analysis through this course on TCP/IP concepts, routing, vocabulary and functions.

NICE Knowledge and Skill Statements:
K0004, K0061, K0185, K0192, K0332, K0471, K0555, K0565, S0081

Log Analysis

Course | 39 minutes

Log analysis counts for a lot in an investigation. Learn to maximize your analysis process with this course covering log management, auditing, steps, concerns and more.

NICE Knowledge and Skill Statements:
K0004, K0061, K0084, K0132, K0145, K0177, K0301, K0318, K0363, K0452, S0046, S0081, S0173, S0192, S0267

Network Security Technologies

Course | 30 minutes

Two videos reintroduce you to network security technologies, including tool families, uses and examples.

NICE Knowledge and Skill Statements:
K0004, K0007, K0111, K0056, K0110, K0111, K0158, K0180, K0221, K0324, K0334, K0336, K0452, K0516, S0136

Network Forensics Concepts

Course | 50 minutes

Develop your knowledge of network forensics concepts, tools and techniques as you progress through this five-video course.

NICE Knowledge and Skill Statements:
K0004, K0017, K0118, K0122, K0128, K0129, K0132, K0133, K0179, K0255, K0304, K0433, K0486, K0489, K0573

Networking Fundamentals

Course | 31 minutes

Build a foundational knowledge of networking in this overview course covering key networking concepts and practices.

NICE Knowledge and Skill Statements:
K0001, K0004, K0007, K0011, K0034, K0047, K0056, K0061, K0065, K0179, K0221, K0255, K0332, K0395, K0471, K0486, K0489, K0491, K0565
ComptIA Cybersecurity Analyst (CySA+)

The ComptIA Cybersecurity Analyst (CySA+) certification path teaches you how to use behavioral analytics to prevent, detect and combat cyber threats. You'll learn how to configure and use threat detection tools, perform data analysis to identify threats and secure applications and systems.

**CERTIFICATION PATH**

**CySA+ Practice Exam**

Practice Exam | 150 questions

Prepare for your CySA+ exam and test your domain knowledge.

**Introduction to CySA+**

Course | 7 minutes

This two-video course is a brief introduction to the CySA+ course pathway, including the four CySA+ domains.

**Introduction to Threat Management**

Course | 41 minutes

Explore threat management with nine videos on key concepts such as the CIA triad, risk management controls and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0151, K0162, K0165, K0339, K0344, K0362, K0474, K0527, K0548, K0604, K0612

**Network Based Threats**

Course | 26 minutes

Five videos give you a step up on network-based threats. Includes information on secure endpoint management, firewall types and types of risk controls.

NICE Knowledge and Skill Statements:

K0007, K0049, K0065, K0167, K0205, K0487, K0488, K0561, K0603, K0612

**Securing Corporate Environment**

Course | 16 minutes

Refresh your knowledge of securing corporate environments, with a special focus on pentesting and analysis.

NICE Knowledge and Skill Statements:

K0175, K0183, K0342

**Environmental Reconnaissance Techniques and Analysis**

Course | 57 minutes

Sixteen videos take you through the details of environmental reconnaissance techniques and analysis, including tools and vocabulary.

NICE Knowledge and Skill Statements:

K0177, K0191, K0192, K0342, K0409, K0447, K0460, K0535, K0536, K0565
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Management Process</strong></td>
<td>55 minutes</td>
<td>K0002, K0003, K0013, K0040, K0065, K0070, K0106, K0161, K0162, K0177, K0272, K0339, K0624, S0167</td>
</tr>
<tr>
<td><strong>Analyzing Vulnerability Scan Results</strong></td>
<td>28 minutes</td>
<td>K0272, K0339, S0167</td>
</tr>
<tr>
<td><strong>Common Vulnerabilities</strong></td>
<td>28 minutes</td>
<td>K0009, K0070, K0106, K0362, K0603, K0604, K0624</td>
</tr>
<tr>
<td><strong>Incident Response Process</strong></td>
<td>41 minutes</td>
<td>K0041, K0042, K0150, K0292, K0317</td>
</tr>
<tr>
<td><strong>Analyzing Common Symptoms</strong></td>
<td>34 minutes</td>
<td>K0106, K0145, K0301, K0339, K0362, K0567, K0603</td>
</tr>
<tr>
<td><strong>Digital Forensics Tools and Investigation Techniques</strong></td>
<td>32 minutes</td>
<td>K0017, K0118, K0122, K0128, K0129, K0132, K0133, K0134, K0304, K0433, K0573</td>
</tr>
<tr>
<td><strong>Incident Recovery and Post-Incident Response Process</strong></td>
<td>18 minutes</td>
<td>K0026, K0042, K0150, K0292, K0317, K0381</td>
</tr>
<tr>
<td><strong>Frameworks, Policies, Controls and Procedures</strong></td>
<td>36 minutes</td>
<td>K0003, K0004, K0047, K0065, K0112, K0199, K0242, K0432, K0504</td>
</tr>
<tr>
<td><strong>Security Architecture Review and Compensating Controls</strong></td>
<td>32 minutes</td>
<td>K0004, K0033, K0065, K0112, K0145, K0165, K0179, K0245, K0333</td>
</tr>
</tbody>
</table>
## Identity and Access Management Security

Course | 58 minutes

Eleven videos reintroduce you to the details of identity and access management security.

NICE Knowledge and Skill Statements: K0007, K0032, K0044, K0056, K0112, K0158, K0336, K0362, K0452

## Implementing Security Best Practices in SDLC

Course | 44 minutes

Review and update your knowledge of implementing best practices in software development with six videos on coding for security, software development models and more.

NICE Knowledge and Skill Statements: K0039, K0079, K0080, K0081, K0082, K0153, K0178, K0186, K0624

## CySA+ Conclusion

Course | 18 minutes

Top off your CySA+ study with a review of performance-based questions.

NICE Knowledge and Skill Statements:
# Computer Forensics

The Computer Forensics skill path teaches you critical techniques about identifying, preserving, extracting, analyzing and reporting forensic evidence through use of the most popular computer forensic tools.

<table>
<thead>
<tr>
<th>Skill Assessment</th>
<th>Computer Forensics Cyber Range</th>
<th>Computer Forensics as a Profession</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill assessment</td>
<td>Cyber range</td>
<td>Course</td>
</tr>
<tr>
<td>20 questions</td>
<td>6 labs</td>
<td>27 minutes</td>
</tr>
<tr>
<td>See how your computer forensics skills stack up against other professionals in your field.</td>
<td>Gain practical experience and develop your command line skills through 10 hands-on labs in the Command Line Basics Cyber Range.</td>
<td>Learn what it’s like to be a computer forensics professional in this introductory course covering duties, procedures and practical advice.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Digital Evidence and Legal Issues</th>
<th>Computer Forensics Investigations</th>
<th>Aspects of Hard Drives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>Course</td>
<td>Course</td>
</tr>
<tr>
<td>1 hour 52 minutes</td>
<td>2 hours 21 minutes</td>
<td>44 minutes</td>
</tr>
<tr>
<td>Explore potential legal issues related to digital evidence, review citizens’ rights and gain insight into real-world cases in this computer forensics course.</td>
<td>Take a deep dive into the process of conducting computer forensics investigations, including procedures, methodology, tools and reporting.</td>
<td>Learn about technical aspects of hard drives and how they relate to computer forensics as you progress through this course.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NICE Knowledge and Skill Statements:</th>
<th>NICE Knowledge and Skill Statements:</th>
<th>NICE Knowledge and Skill Statements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0062, S0071, S0091, S0267</td>
<td>K0017, K0118, K0304</td>
<td>K0122, K0128, K0133, K0449</td>
</tr>
<tr>
<td>K0123, K0156, K0168</td>
<td>K0017, K0107, K0118, K0125, K0133, K0185, K0304, K0573, S0047, S0068, S0071</td>
<td>K0122, K0128, K0133, K0449</td>
</tr>
<tr>
<td><strong>File Systems</strong></td>
<td><strong>Email and Browser Forensics</strong></td>
<td><strong>Network Forensics Concepts</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td><strong>Course</strong></td>
<td>45 minutes</td>
<td><strong>Course</strong></td>
</tr>
<tr>
<td>Learn all about file systems, including essential topics related to finding and uncovering data, as well as the tools used to do so.</td>
<td>Explore a variety of concepts around email and browser forensics and learn how those concepts are applied in this eleven-video course.</td>
<td>Develop your knowledge of network forensics concepts, tools and techniques as you progress through this five-video course.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>K0117, K0122, K0128, K0132, K0182</td>
<td>K0131, K0133, S0065</td>
<td>K0001, K0100, K0122, K0371, S0120</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Data Hiding</strong></th>
<th><strong>Memory Forensics</strong></th>
<th><strong>Passwords and Encryption</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Course</strong></td>
<td>40 minutes</td>
<td><strong>Course</strong></td>
</tr>
<tr>
<td>Explore how cryptographic hashing, stenography and other techniques are used to hide data, as well as how that data can be discovered.</td>
<td>Learn all about memory forensics, including using popular tools, conducting live analysis and carrying out basic forensics processes in this brief course.</td>
<td>Discover key forensics concepts and best practices related to passwords and encryption, including how to gain access to a suspect's device.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>K0184, K0305, S0071, S0092</td>
<td>K0268, S0062, S0090, S0091</td>
<td>K0017, K0132</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>New and Emerging Technologies</strong></th>
<th><strong>Introduction to Mobile Forensics</strong></th>
<th><strong>File and Operating System Forensics</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Course</strong></td>
<td>1 hour 5 minutes</td>
<td><strong>Course</strong></td>
</tr>
<tr>
<td>Explore how new and emerging technologies are affecting forensics, including virtualization, social networks and gaming.</td>
<td>Get an introduction to mobile forensics and the challenges mobile devices present to investigators in this overview course.</td>
<td>Explore a variety of concepts around file and operating forensics and learn how those concepts are applied in this eight-video course.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>K0130, K0610, S0090</td>
<td>K0438, S0075</td>
<td>K0122, K0132, K0449, K0573</td>
</tr>
</tbody>
</table>
## Cyber Threat Hunting

The Cyber Threat Hunting Learning Path helps you master a repeatable, documentable cyber threat hunting methodology. You'll learn how to leverage a variety of tools to assist with your cyber threat hunting activities.

### Skill Assessment

**Skill assessment | 20 questions**

See how your cyber threat hunting skills stack up against other professionals in your field.

### Cyber Threat Hunting Project

**Project | 2 hours 31 minutes**

Use your cyber threat hunting skills to identify network traffic patterns for anomalies and investigate malware. You'll use Wireshark to examine packet capture files for potential red flags. Then you'll attempt to piece together the threat.

**NICE Knowledge and Skill Statements:**

- S0199, S0221, S0258

### Introduction to Cyber Threat Hunting Techniques

**Course | 57 minutes**

Increase your knowledge of cyber threat hunting techniques and resources available. Here, we will introduce you to the Cyber Threat Hunter.

**NICE Knowledge and Skill Statements:**

- K0004, K0579

### Detection

**Course | 2 hours 24 minutes**

In order to have an effective threat-hunting program, the hunter needs access to the tools and data necessary to perform these tasks. The best open-source tools are free and only work on Linux. Let's talk about some of those tools.

**NICE Knowledge and Skill Statements:**

- K0004, K0013, K0111, K0129, K0145, K0229, K0318, K0334, K0339, K0603, S0081

### Investigation Process

**Course | 1 hour 10 minutes**

The purpose of this course is to help the threat hunter to identify whether the anomalous activity is a threat. Explore how to investigate, walking through the information and identifying any issues right away.

**NICE Knowledge and Skill Statements:**

- K0058, K0107, K0122, K0334, K0362, K0481, K0523, K0603, S0184, S0258

### Remediate the Malware

**Course | 25 minutes**

Go through the skills and tools needed to identify and remediate malware. You'll look at identifying malware propagation techniques, ensuring it doesn't spread, preventing future infiltration attempts and more.

**NICE Knowledge and Skill Statements:**

- K0026, K0205, K0231, K0362, K0406, K0479, K0480, K0481, K0523
**Attack Simulators and Exercises**

**Course** | 1 hour 2 minutes

In this course, we will be looking at attack simulators, which will be used to test your monitoring and alerting solutions.

**NICE Knowledge and Skill Statements:**
K0106, K0117, K0161, K0469, S0044, S0078

---

**Cyber Threat Hunting Review**

**Course** | 9 minutes

Review the steps of cyber threat hunting: Detect, Investigate and Response/Remediation. Finally, you'll recap on the threat hunter's duties and responsibilities in preparation for the final project.

**NICE Knowledge and Skill Statements:**
K0150
Digital Forensics Concepts

In the Digital Forensics Concepts path, the student will learn about legal considerations applicable to computer forensics and how to identify, collect and preserve digital evidence.

Digital Forensics Project
Project | 2 hours 38 minutes
Practice your digital forensics knowledge with this project.

NICE Knowledge and Skill Statements:
K0005, K0017, K0118, K0128, K0133, K0134, K0182, K0187, K0304, S0047, S0065, S0071

Introduction to Digital Forensics
Course | 33 minutes
This intro course provides a broad overview of computer forensics as an occupation by exploring methodologies used surrounding digital forensics.

NICE Knowledge and Skill Statements:
K0001, K0004, K0017, K0060, K0304, S0131

Legal considerations and search authority
Course | 39 minutes
This course demonstrates information commonly needed in a search warrant and a preservation request.

NICE Knowledge and Skill Statements:
K0003, K0017, K0123, K0125, K0155, K0156, K0168, K0304, S0047, S0133

The investigative process
Course | 16 minutes
This course covers scientific principles that apply to digital forensics.

NICE Knowledge and Skill Statements:
K0005, K0017, K0078, K0118, K0119, K0122, K0132, K0133, K0134, K0304, S0032, S0047, S0069, S0091, S0133

Recognizing and collecting digital evidence
Course | 27 minutes
This course explores what to bring to a scene and how to prepare and label digital evidence for documentation purposes.

NICE Knowledge and Skill Statements:
K0001, K0004, K0005, K0122, K0125, K0128, K0131, K0132, K0133, K0145, K0182, S0065, S0068, S0071, S0075, S0090, S0091

Preservation of evidence/On scene triage
Course | 27 minutes
This course discusses capturing RAM, recognizing and dealing with encryption and destructive processes and triaging devices with a forensic boot media.

NICE Knowledge and Skill Statements:
K0002, K0004, K0042, K0060, K0070, K0078, K0109, K0117, K0119, K0118, K0183, K0186, K0187, K0188, K0254, K0301, K0372, K0573, S0062, S0067, S0069, S0074, S0087, S0091, S0131, S0156, S0266
<table>
<thead>
<tr>
<th>Topic</th>
<th>Duration</th>
<th>Description</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash values and file hashing</td>
<td>20 minutes</td>
<td>In this course, the student learns how to use hash values as a way to include or exclude files from an investigation.</td>
<td>K0070, K0117, K0187, K0277, K0396, S0089, S0298</td>
</tr>
<tr>
<td>Creating a disk image</td>
<td>1 hour 1 minute</td>
<td>This course explains the importance of sterilizing media, how to validate tools, proper application of the write-blocker and validating the forensic bit-stream copy.</td>
<td>K0017, K0070, K0118, K0119, K0128, K0132, K0182, K0185, K0187, K0372, K0573, S0047, S0065, S0071, S0075, S0091</td>
</tr>
<tr>
<td>Key word and grep searches</td>
<td>33 minutes</td>
<td>Explore the details of keyword and grep searches.</td>
<td>K0070, K0131, K0185, K0535, S0011, S0195, S0220</td>
</tr>
<tr>
<td>Network basics</td>
<td>25 minutes</td>
<td>A look at network basics for the computer forensics investigator.</td>
<td>K0001, K0004, K0034, K0058, K0106, K0179, K0221, K0332, K0393, K0471, K0489, K0565, S0187, S0236</td>
</tr>
<tr>
<td>Reporting and peer review</td>
<td>28 minutes</td>
<td>In this course, the student examiner learns what information to include and what does not belong in a final report.</td>
<td>K0215, K0354, K0451, S0003</td>
</tr>
</tbody>
</table>

Threat intelligence, incident response and forensics
Cybersecurity Data Science

Learn everything you need to employ the latest cutting edge tools in cybersecurity data science in this hands-on, comprehensive skill path. You will set up a cybersecurity lab, construct classifiers to detect malware, utilize deep learning technology and even hack security systems with the help of machine learning.

Skill Assessment

Skill assessment | 20 questions
See how your cybersecurity data science skills stack up against other professionals in your field.

Cybersecurity Data Science Project

Project | 2 hours 12 minutes
Practice your Cybersecurity Data Science skills by solving challenges.

NICE Knowledge and Skill Statements:
S0087, S0252, S0257

Preparation for Cybersecurity Data Science

Course | 42 minutes
Set up your cybersecurity lab and acquire the background knowledge essential to success in Cybersecurity Data Science.

NICE Knowledge and Skill Statements:
K0238, K0476, K0609, K0610, S0073

Malware Detection via Machine Learning

Course | 43 minutes
Gain a practical understanding of the most successful techniques used by Cybersecurity Data Science experts for the crafting of malware classifiers.

NICE Knowledge and Skill Statements:
K0189, K0238, K0259, K0479, K0480, S0131

Machine Learning for Intrusion Detection

Course | 11 minutes
Master the most important use cases for preventing hackers, spammers and criminals from entering your network uninvited.

NICE Knowledge and Skill Statements:
K0046, K0058, K0238, K0301, K0334, S0258, S0280

Machine Learning for Social Engineering

Course | 16 minutes
Expand the impact of your social engineering by arming yourself with the latest machine learning-based social engineering tools and methods.

NICE Knowledge and Skill Statements:
K0238, K0476, K0603, S0052
Machine Learning for Pentesting

Course | 17 minutes

Employ machine learning to take your penetration testing to the next level by unlocking information and access thought impenetrable before.

NICE Knowledge and Skill Statements:
K0177, K0238, K0342, K0493, K0603, S0051, S0081
Certified Computer Forensics Examiner (CCFE)

The Certified Computer Forensics Examiner (CCFE) certification path teaches you the skills needed to investigate computer threats. You'll learn about performing forensics on hard drives, file systems and networks as well as the legal and ethical issues of investigating cybercrime.

Skill Assessment
Skill assessment | 20 questions
See how your CCFE skills stack up against other professionals in your field.

CCFE Practice Exam
Practice Exam | 50 questions
Prepare for your CCFE exam and test your domain knowledge.

Computer Forensics Cyber Range
Cyber range | 6 labs
Gain practical experience and develop your computer forensics skills through six hands-on labs in the Computer Forensics Cyber Range.

NICE Knowledge and Skill Statements:
S0062, S0071, S0091, S0267

Computer Forensics as a Profession
Course | 27 minutes
Learn what it's like to be a computer forensics professional in this introductory course covering duties, procedures and practical advice.

NICE Knowledge and Skill Statements:
K0017, K0118, K0304

Digital Evidence and Legal Issues
Course | 1 hour 52 minutes
Explore potential legal issues related to digital evidence, review citizens’ rights and gain insight into real-world cases in this computer forensics course.

NICE Knowledge and Skill Statements:
K0123, K0156, K0168

Aspects of Hard Drives
Course | 44 minutes
Learn about technical aspects of hard drives and how they relate to computer forensics as you progress through this course.

NICE Knowledge and Skill Statements:
K0122, K0128, K0133, K0449
<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Table of contents</th>
<th>Boot camps</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
</table>

**File Systems**

Course | 45 minutes
---
Learn all about file systems, including essential topics related to finding and uncovering data, as well as the tools used to do so.

NICE Knowledge and Skill Statements:
K0117, K0122, K0128, K0132, K0182

**Email and Browser Forensics**

Course | 2 hours
---
Explore a variety of concepts around email and browser forensics and learn how those concepts are applied in this eleven-video course.

NICE Knowledge and Skill Statements:
K0131, K0133, S0065

**Network Forensics Concepts**

Course | 50 minutes
---
Develop your knowledge of network forensics concepts, tools and techniques as you progress through this five-video course.

NICE Knowledge and Skill Statements:
K0001, K0100, K0122, K0371, S0120

**Data Hiding**

Course | 40 minutes
---
Explore how cryptographic hashing, stenography and other techniques are used to hide data, as well as how that data can be discovered.

NICE Knowledge and Skill Statements:
K0184, K0305, S0071, S0092

**Memory Forensics**

Course | 19 minutes
---
Learn all about memory forensics, including using popular tools, conducting live analysis and carrying out basic forensics processes in this brief course.

NICE Knowledge and Skill Statements:
K0268, S0062, S0090, S0091

**Passwords and Encryption**

Course | 49 minutes
---
Discover key forensics concepts and best practices related to passwords and encryption, including how to gain access to a suspect's device.

NICE Knowledge and Skill Statements:
K0017, K0132

**New and Emerging Technologies**

Course | 1 hour 5 minutes
---
Explore how new and emerging technologies are affecting forensics, including virtualization, social networks and gaming.

NICE Knowledge and Skill Statements:
K0130, K0610, S0090

**Introduction to Mobile Forensics**

Course | 43 minutes
---
Get an introduction to mobile forensics and the challenges mobile devices present to investigators in this overview course.

NICE Knowledge and Skill Statements:
K0438, S0075

**File and Operating System Forensics**

Course | 1 hour 24 minutes
---
Explore a variety of concepts around file and operating forensics and learn how those concepts are applied in this eight-video course.

NICE Knowledge and Skill Statements:
K0122, K0132, K0449, K0573
Computer Forensics Investigations

Course | 2 hours 21 minutes

Take a deep dive into the process of conducting computer forensics investigations, including procedures, methodology, tools and reporting.

NICE Knowledge and Skill Statements:
K0017, K0107, K0118, K0125, K0133, K0185, K0304, K0573, S0047, S0068, S0071
Certified Mobile Forensics Examiner (CMFE)

The Certified Mobile Forensics Examiner (CMFE) certification path prepares you for the CMFE certification exam by teaching the necessary skills to investigate mobile threats and mobile cybercrime.

### Skill Assessment
- **Skill assessment | 20 questions**
  - See how your CMFE skills stack up against other professionals in your field.

### CMFE Practice Exam
- **Practice Exam | 75 minutes**
  - Prepare for your CMFE exam and test your domain knowledge.

### Introduction to Mobile Forensics
- **Course | 43 minutes**
  - Get an introduction to mobile forensics and the challenges mobile devices present to investigators in this overview course.
  - **NICE Knowledge and Skill Statements:**
    - K0138, K0269, K0438

### Mobile Forensics Process
- **Course | 1 hour 30 minutes**
  - Mobile forensics comes with a unique set of challenges. Explore those challenges with this course on the mobile forensics process, including phone types, volatile data recovery and evidence handling.
  - **NICE Knowledge and Skill Statements:**
    - K0017, K0060, K0118, K0122, K0128, K0133, K0134, K0269, K0433, K0438, K0449, K0573, S0047

### Android Forensics
- **Course | 2 hours 2 minutes**
  - Explore the challenges of Android mobile forensics with this course covering Android security, structure, challenges and more.
  - **NICE Knowledge and Skill Statements:**
    - K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091

### iOS Forensics
- **Course | 1 hour 22 minutes**
  - Dive deep into the details of iOS forensics with this course covering iOS structure, system security, passcodes and more.
  - **NICE Knowledge and Skill Statements:**
    - K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091
Windows Phone and Feature Phone Forensics

Course | 51 minutes

Discover the possible difficulties of rare models with this course on Windows Phone and feature phone forensics.

NICE Knowledge and Skill Statements:
K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091
Certified Reverse Engineering Analyst (CREA)

The Certified Reverse Engineering Analyst (CREA) certification path teaches you the analysis skills to discover the true nature of any Windows binary. You'll learn how to analyze hostile code and malware, vulnerabilities in binaries, and business intelligence used by hackers and Trojan writers.

### Skill Assessment

**Skill assessment | 20 questions**

See how your CREA skills stack up against other professionals in your field.

### CREA Practice Exam

**Practice Exam | 50 questions**

Prepare for your CREA exam and test your domain knowledge.

### Introduction to Malware Analysis

**Course | 28 minutes**

Explore malware analysis with a course covering static and dynamic analysis, tools, malware types and analysis methodologies.

**NICE Knowledge and Skill Statements:**

K0259

### Introduction to Reverse Engineering

**Course | 47 minutes**

Take a closer look at the art and science of reverse-engineering with a course on machine code, assembly language, system-level reversing and more.

**NICE Knowledge and Skill Statements:**

K0175, K0372

### Disassembly

**Course | 47 minutes**

Examine the intricacies of assembly and disassembly in an X86 context. Includes videos on arithmetic instructions, logical instructions and operands.

**NICE Knowledge and Skill Statements:**

K0051

### Reversing Tools

**Course | 32 minutes**

Explore the intricacies of multiple reversing tools, beginning with a close look at Interactive Disassembler (IDA).

**NICE Knowledge and Skill Statements:**

K0188
### C Code in Assembly

**Course | 48 minutes**

Take a closer look at C code in assembly, including loops, linked lists, stacks and heaps.

**NICE Knowledge and Skill Statements:**

K0068

---

### Windows Internals

**Course | 33 minutes**

Explore the reverse-engineering of Windows with this course on Windows internals such as network APIs and services.

**NICE Knowledge and Skill Statements:**

K0608

---

### Debugging

**Course | 41 minutes**

A close and personal look at debugging, with nine videos taking you through stepping, breakpoints and exceptions and more. Includes in-depth examples.

**NICE Knowledge and Skill Statements:**

K0079, K0186, S0014, S0093

---

### Common Malware Behavior

**Course | 55 minutes**

Improve your malware-hunting skills with a course on injection types, network functions and other fundamentals of malware behavior.

**NICE Knowledge and Skill Statements:**

K0259, K0392, K0479, K0480, K0536, S0087, S0131

---

### Reversing Rootkits

**Course | 11 minutes**

Look more closely at the challenge of reversing rootkits with four videos on rootkit structure and behavior.

**NICE Knowledge and Skill Statements:**

K0392, K0479

---

### Anti-Disassembly, Anti-Debugging and Anti-VM

**Course | 32 minutes**

Malware doesn't want to be disassembled, and it's going to fight you. Seven videos examine anti-disassembly, anti-debugging and anti-VM strategies used by malware.

**NICE Knowledge and Skill Statements:**

K0189, K0479, S0093

---

### Packed Malware

**Course | 16 minutes**

Sometimes, malware is just hiding. Four videos examine the issue of packed malware, including tools, tricks and popular packers.

**NICE Knowledge and Skill Statements:**

K0479, S0093, S0270

---

### Obfuscation, Encoding and Encryption

**Course | 40 minutes**

Reintroduce yourself to three ways malware disguises itself: obfuscation, encoding and encryption.

**NICE Knowledge and Skill Statements:**

S0092, S0093, S0095

---

### Reversing C++

**Course | 27 minutes**

Our four-video course will reintroduce you to the art of reversing C++.

**NICE Knowledge and Skill Statements:**

K0068

---
Reversing 64-bit Malware

Course | 14 minutes

Two videos take you through the ins and outs of reversing 64-bit malware, including functions, code samples and tools.

NICE Knowledge and Skill Statements:
K0479
Incident Response

The Incident Response Learning Path will give students the understanding of how incidents are responded to at a high level, as well as allow them to build important technical skills through the hands-on labs and projects.

**Skill Assessment**
Skill assessment | 20 questions
See how your incident response skills stack up against other professionals in your field.

**Network Traffic Analysis Cyber Range**
Cyber range | 12 labs
Gain practical experience and build your real-world network traffic analysis skills through 12 hands-on labs in the Network Traffic Analysis Cyber Range.

**NICE Knowledge and Skill Statements:**
S0046, S0051, S0120, S0156, S0199, S0221

**Incident Response Project**
Project | 3 hours 6 minutes
Use your incident response skills along with tools like Wireshark, Zeek and Volatility to respond to real-world scenarios.

**NICE Knowledge and Skill Statements:**
S0199, S0221, S0258, S0269

**Introduction to Incident Response**
Course | 55 minutes
Review the fundamentals of incident response and learn how to build an IR team and effective playbook for handling incidents.

**NICE Knowledge and Skill Statements:**
K0026, K0042, K0150, K0412

**Stage 1 – Preparation**
Course | 33 minutes
This course deals briefly with some common definitions and severity criteria related to incident response. It ends with a high-level explanation of asset inventory and identification.

**NICE Knowledge and Skill Statements:**
K0004, K0005, K0041, K0106, K0162, K0295, K0361, K0612, S0364

**Stage 2 – Identification**
Course | 38 minutes
This course explores the process of identifying when there has been an event that falls into the category of becoming an incident. It also touches on classification levels for incidents.

**NICE Knowledge and Skill Statements:**
K0041, K0381, K0451
<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><strong>Stage 3 – Containment</strong>&lt;br&gt;Course</td>
<td>37 minutes</td>
<td>NICE Knowledge and Skill Statements:&lt;br&gt;K0041, K0042, K0110, K0480, K0586</td>
</tr>
<tr>
<td>4</td>
<td><strong>Stage 4 – Investigation</strong>&lt;br&gt;Course</td>
<td>23 minutes</td>
<td>NICE Knowledge and Skill Statements:&lt;br&gt;K0132, K0150, K0292</td>
</tr>
<tr>
<td>5</td>
<td><strong>Stage 5 – Eradication</strong>&lt;br&gt;Course</td>
<td>27 minutes</td>
<td>NICE Knowledge and Skill Statements:&lt;br&gt;K0150, K0210, K0354</td>
</tr>
<tr>
<td>6</td>
<td><strong>Stage 6 – Recovery</strong>&lt;br&gt;Course</td>
<td>27 minutes</td>
<td>NICE Knowledge and Skill Statements:&lt;br&gt;K0026, K0210, K0292, K0381</td>
</tr>
<tr>
<td>7</td>
<td><strong>Stage 7 – Follow Up/Lessons Learned</strong>&lt;br&gt;Course</td>
<td>13 minutes</td>
<td>NICE Knowledge and Skill Statements:&lt;br&gt;K0003, K0287</td>
</tr>
<tr>
<td></td>
<td><strong>Technical Deep Dives with Tools of the Trade</strong>&lt;br&gt;Course</td>
<td>4 hours 1 minute</td>
<td>NICE Knowledge and Skill Statements:&lt;br&gt;K0017, K0046, K0058, K0062, K0272, K0343, K0392, S0003, S0046, S0062, S0120, S0199, S0221, S0258, S0261</td>
</tr>
</tbody>
</table>
Malware Analysis & Reverse Engineering

This learning path takes a deep dive into taking apart and analyzing malware. As you progress through 12 courses, you’ll build your skills and knowledge around the inner-workings of malware, the tools used by malware analysts, and the ins and outs of reversing different types of malware.

Disassembly

Course | 47 minutes
Examine the intricacies of assembly and disassembly in an X86 context. Includes videos on arithmetic instructions, logical instructions and operands.

NICE Knowledge and Skill Statements:
K0051

Reversing Tools

Course | 32 minutes
Explore the intricacies of multiple reversing tools, beginning with a close look at Interactive Dissassembler (IDA).

NICE Knowledge and Skill Statements:
K0188

C Code in Assembly

Course | 48 minutes
Take a closer look at C code in assembly, including loops, linked lists, stacks and heaps.

NICE Knowledge and Skill Statements:
K0068

Windows Internals

Course | 33 minutes
Explore the reverse-engineering of Windows with this course on Windows internals such as network APIs and services.

NICE Knowledge and Skill Statements:
K0608

Debugging

Course | 41 minutes
A close and personal look at debugging, with nine videos taking you through stepping, breakpoints and exceptions and more. Includes in-depth examples.

NICE Knowledge and Skill Statements:
K0079, K0186, S0014, S0093

Common Malware Behavior

Course | 55 minutes
Improve your malware-hunting skills with a course on injection types, network functions and other fundamentals of malware behavior.

NICE Knowledge and Skill Statements:
K0259, K0392, K0479, K0480, K0536, S0087, S0131
### Reversing Rootkits

**Course | 11 minutes**

Look more closely at the challenge of reversing rootkits with four videos on rootkit structure and behavior.

**NICE Knowledge and Skill Statements:**

K0392, K0479

### Anti-Disassembly, Anti-Debugging and Anti-VM

**Course | 32 minutes**

Malware doesn't want to be disassembled, and it's going to fight you. Seven videos examine anti-disassembly, anti-debugging and anti-VM strategies used by malware.

**NICE Knowledge and Skill Statements:**

K0189, K0479, S0093

### Packed Malware

**Course | 16 minutes**

Sometimes, malware is just hiding. Four videos examine the issue of packed malware, including tools, tricks and popular packers.

**NICE Knowledge and Skill Statements:**

K0479, S0093, S0270

### Obfuscation, Encoding and Encryption

**Course | 40 minutes**

Reintroduce yourself to three ways malware disguises itself: obfuscation, encoding and encryption.

**NICE Knowledge and Skill Statements:**

S0092, S0093, S0095

### Reversing C++

**Course | 27 minutes**

Our four-video course will reintroduce you to the art of reversing C++.

**NICE Knowledge and Skill Statements:**

K0068

### Reversing 64-bit Malware

**Course | 14 minutes**

Two videos take you through the ins and outs of reversing 64-bit malware, including functions, code samples and tools.

**NICE Knowledge and Skill Statements:**

K0479
Mobile Forensics

The Mobile Forensics skill path teaches you critical techniques about identifying, preserving, extracting, analyzing and reporting forensic evidence found on mobile devices, including Android, iOS, Windows Phone and Feature Phone.

Skill Assessment

Skill assessment | 20 questions
See how your mobile forensics skills stack up against other professionals in your field.

Introduction to Mobile Forensics

Course | 43 minutes
Get an introduction to mobile forensics and the challenges mobile devices present to investigators in this overview course.

NICE Knowledge and Skill Statements:
K0138, K0269, K0438

Mobile Forensics Process

Course | 1 hour 30 minutes
Mobile forensics comes with a unique set of challenges. Explore those challenges with this course on the mobile forensics process, including phone types, volatile data recovery and evidence handling.

NICE Knowledge and Skill Statements:
K0017, K0060, K0118, K0122, K0128, K0133, K0134, K0269, K0433, K0438, K0449, K0573, S0047

Android Forensics

Course | 2 hours 2 minutes
Explore the challenges of Android mobile forensics with this course covering Android security, structure, challenges and more.

NICE Knowledge and Skill Statements:
K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091

iOS Forensics

Course | 1 hour 22 minutes
Dive deep into the details of iOS forensics with this course covering iOS structure, system security, passcodes and more.

NICE Knowledge and Skill Statements:
K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091

Windows Phone and Feature Phone Forensics

Course | 51 minutes
Discover the possible difficulties of rare models with this course on Windows Phone and feature phone forensics.

NICE Knowledge and Skill Statements:
K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091
# Network Forensics

The Network Forensics skill path helps you fully understand how systems are compromised and what traces are left behind by attackers on the network. You’ll learn the concepts, techniques and tools used to analyze logs, protocols, wireless, web traffic and email.

## Network Traffic Analysis Cyber Range

**Cyber range | 12 labs**

Gain practical experience and build your real-world network traffic analysis skills through 12 hands-on labs in the Network Traffic Analysis Cyber Range.

**NICE Knowledge and Skill Statements:**
S0046, S0120, S0156, S0199, S0221, S0258, S0267

## Networking Fundamentals

**Course | 31 minutes**

Build a foundational knowledge of networking in this overview course covering key networking concepts and practices.

**NICE Knowledge and Skill Statements:**
K0001, K0004, K0007, K0011, K0034, K0047, K0056, K0061, K0065, K0179, K0221, K0255, K0332, K0395, K0471, K0486, K0489, K0491, K0565

## Network Forensics Concepts

**Course | 50 minutes**

Develop your knowledge of network forensics concepts, tools and techniques as you progress through this five-video course.

**NICE Knowledge and Skill Statements:**
K0004, K0017, K0118, K0122, K0128, K0129, K0132, K0133, K0179, K0255, K0304, K0433, K0486, K0489, K0573

## Network Security Technologies

**Course | 30 minutes**

Two videos reintroduce you to network security technologies, including tool families, uses and examples.

**NICE Knowledge and Skill Statements:**
K0004, K0007, K0011, K0034, K0036, K0111, K0158, K0180, K0221, K0324, K0334, K0336, K0452, K0516, S0136

## Log Analysis

**Course | 39 minutes**

Log analysis counts for a lot in an investigation. Learn to maximize your analysis process with this course covering log management, auditing, steps, concerns and more.

**NICE Knowledge and Skill Statements:**
K0004, K0061, K0084, K0132, K0145, K0177, K0301, K0318, K0363, K0452, S0046, S0081, S0173, S0192, S0267

## Protocol Analysis

**Course | 19 minutes**

Get to grips with protocol analysis through this course on TCP/IP concepts, routing, vocabulary and functions.

**NICE Knowledge and Skill Statements:**
K0004, K0061, K0185, K0192, K0301, K0332, K0471, K0555, K0565, S0081
### Wireless Analysis

**Course** | 38 minutes
---
Take a moment to refresh your knowledge of wireless analysis. Includes vocabulary, examples and diagrams.

**NICE Knowledge and Skill Statements:**
K0004, K0056, K0093, K0108, K0113, K0137, K0138, K0274, K0375, K0428, K0438, K0445, K0446, K0556, K0560, K0614, S0138

### Web Traffic Analysis

**Course** | 13 minutes
---
Dig into Web traffic analysis with this course covering write protection, Web forensics and cookies.

**NICE Knowledge and Skill Statements:**
K0004, K0061, K0179, K0255, K0274, K0332, K0444, K0471, K0486, K0489, K0565, K0603

### Email Analysis

**Course** | 21 minutes
---
Explore forensic email analysis with this course covering the structure, function and details of email.

**NICE Knowledge and Skill Statements:**
K0004, K0192, K0268, K0332, K0444, K0447, K0449, K0565, S0071
Network Traffic Analysis for Incident Response

This learning path covers identification and analysis of benign and malicious traffic, examples and case studies of extracting intelligence from traffic data, considerations when building a network monitoring program, and techniques for collecting and analyzing traffic data.

**Skill Assessment**

Skill assessment | 20 questions

See how your network traffic analysis skills stack up against other professionals in your field.

**Network Traffic Analysis Cyber Range**

Cyber range | 12 labs

Gain practical experience and build your real-world network traffic analysis skills through 12 hands-on labs in the Network Traffic Analysis Cyber Range.

NICE Knowledge and Skill Statements:
S0046, S0051, S0120, S0156, S0199, S0221

**Network Traffic Analysis Project**

Project | 1 hour 29 minutes

Practice your network traffic analysis skills by solving challenges.

NICE Knowledge and Skill Statements:
S0092, S0156, S0199, S0221, S0258, S0269

**Introduction to Network Traffic Analysis**

Course | 41 minutes

This course provides an introduction to network traffic analysis and describes its primary applications.

NICE Knowledge and Skill Statements:
K0042, K0058, K0334

**Fundamentals of Networking**

Course | 56 minutes

This course covers the fundamentals of networking and the purposes of various low-level and high-level networking protocols.

NICE Knowledge and Skill Statements:
K0004, K0034, K0061, K0221, K0332, K0471

**Hands-On Traffic Analysis in Wireshark**

Course | 1 hour 45 minutes

This course provides an introduction to Wireshark and an analysis of some common protocols in Wireshark.

NICE Knowledge and Skill Statements:
K0301, S0046
<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Learning paths</th>
<th>Learning paths</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alternatives to Wireshark</strong></td>
<td><strong>Network Traffic Intelligence Collection</strong></td>
<td><strong>Common Network Threats</strong></td>
</tr>
<tr>
<td><strong>Course</strong></td>
<td><strong>Course</strong></td>
<td><strong>Course</strong></td>
</tr>
<tr>
<td>31 minutes</td>
<td>1 hour 44 minutes</td>
<td>1 hour 23 minutes</td>
</tr>
<tr>
<td>This course demonstrates some of the features of tools other than Wireshark for network traffic analysis.</td>
<td>This course demonstrates tools and techniques for extracting useful intelligence from a network traffic capture.</td>
<td>This course demonstrates how scanning, data exfiltration, DDoS attacks and attacks against IoT devices can appear in network traffic.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>K0301, S0046</td>
<td>K0301, K0573, S0046</td>
<td>K0005, K0160, K0177, K0362, K0392, K0603, K0612</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Learning paths</th>
<th>Learning paths</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traffic Analysis Case Studies</strong></td>
<td><strong>Data Collection for Network Traffic Analysis</strong></td>
<td><strong>Data Analysis for Network Traffic Analysis</strong></td>
</tr>
<tr>
<td><strong>Course</strong></td>
<td><strong>Course</strong></td>
<td><strong>Course</strong></td>
</tr>
<tr>
<td>1 hour 6 minutes</td>
<td>1 hour</td>
<td>2 hours 21 minutes</td>
</tr>
<tr>
<td>This course provides four demonstrations of analysis of network traffic from different malware types.</td>
<td>This course discusses the considerations and available technologies for developing a network traffic analysis program.</td>
<td>This course covers the fundamentals of connection and statistical and event-based analysis of network traffic data.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>K0191, K0259, K0392, K0479, K0480</td>
<td>K0058, K0061, K0143, K0334, K0424</td>
<td>K0058, K0129, K0301, K0318, K0334, S0046</td>
</tr>
</tbody>
</table>
The path to becoming a mobile forensic investigator requires fundamental knowledge of devices and the operation of the specialized tools required to process data. The learning path will go through those specialized skills for the operation of Paraben's E3 Forensic Platform in the capture of mobile data as forensic evidence.

**Installation**

Course | 6 minutes

This introductory certification is designed for those just getting started with mobile forensics and want to learn the process using Paraben's E3 Forensic Platform.

**Licensing**

Course | 3 minutes

This section will walk you through the licensing options available for the E3 Forensic Platform. Licensing is determined based on each individual lab design and setup.

**E3:DS Interface**

Course | 4 minutes

The interface portion of this course will review the layout of the E3 Forensic Platform and how to do basic navigation in the primary interface.

**Cases and Adding Evidence**

Course | 4 minutes

The Cases and Adding Evidence portion of this course will focus on the creation of cases, addition of investigator details and continue to focus on the addition of evidence.

**Acquiring Phones**

Course | 13 minutes

The Acquisition portion of this course looks at the primary methods to be able to acquire and process a variety of mobile devices in a forensically sound manner.

**Importing Backups**

Course | 2 minutes

The process of importing backups can offer a valuable perspective in an acquisition with iOS devices.
<table>
<thead>
<tr>
<th>Section</th>
<th>Course</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reviewing the Data</strong></td>
<td>4 minutes</td>
<td>K0108, K0114, K0118, K0125, K0155, K0182, K0304, K0447, K0449, S0047, S0069, S0133, S0263</td>
<td></td>
</tr>
<tr>
<td><strong>Cloud Data</strong></td>
<td>3 minutes</td>
<td>K0007, K0108, K0114, K0118, K0125, K0155, K0182, K0304, S0047, S0069, S0073, S0133</td>
<td></td>
</tr>
<tr>
<td><strong>Searching</strong></td>
<td>3 minutes</td>
<td>K0007, K0108, K0114, K0118, K0125, K0131, K0155, K0182, K0304, S0047, S0069, S0073, S0133</td>
<td></td>
</tr>
<tr>
<td><strong>Bookmarks and Reporting</strong></td>
<td>3 minutes</td>
<td>K0004, K0182, K0185, K0304, S0069, S0071</td>
<td></td>
</tr>
<tr>
<td><strong>Additional Features</strong></td>
<td>2 minutes</td>
<td>K0118, K0125, K0182, K0304, S0047, S0069, S0133</td>
<td></td>
</tr>
</tbody>
</table>

This section will focus on the methods for reviewing the data to ensure the most valuable information can be found in an examination.

This section will cover unique features that are available when working with mobile devices in forensic investigations.
Paraben P2C Operator Certification

This in-depth learning path leads you on an exploration of the many features and uses of the Paraben E3 Forensic Platform.

### Introduction to P2C

**Course** | 3 minutes

This course will introduce you to the basics of the Paraben E3 Forensic Platform.

**NICE Knowledge and Skill Statements:**
K0004, K0182, K0185, K0304, S0069

### Licensing

**Course** | 3 minutes

A look at licensing the E3 Forensic Platform.

**NICE Knowledge and Skill Statements:**
K0004, K0182, K0185, K0304, S0069

### Interface

**Course** | 4 minutes

A look at E3 Forensic Platform layout and navigation.

**NICE Knowledge and Skill Statements:**
K0004, K0182, K0304, S0069, S0071

### Adding evidence

**Course** | 4 minutes

This course looks at cases and adding evidence.

**NICE Knowledge and Skill Statements:**
K0004, K0109, K0118, K0125, K0155, K0182, K0185, K0304, K0447, K0449, S0047, S0069, S0071, S0074, S0120, S0133, S0263

### Drive triage

**Course** | 1 minute

A look at data triage.

**NICE Knowledge and Skill Statements:**
K0004, K0017, K0118, K0122, K0182, K0185, K0304, K0608, S0047, S0065, S0069, S0071, S0133

### Registry

**Course** | 1 minute

Exploring the artifacts in a Windows system registry.

**NICE Knowledge and Skill Statements:**
K0004, K0017, K0122, K0132, K0185, K0304, K0608, S0065, S0069, S0091, S0133
Data processing

Course | 7 minutes
A look at data optimization techniques.

NICE Knowledge and Skill Statements:
K0004, K0017, K0122, K0182, K0185, K0304, K0608, S0065, S0068, S0069, S0071, S0090, S0091, S0133

Forensic containers

Course | 2 minutes
Data carving in digital forensics.

NICE Knowledge and Skill Statements:
K0004, K0017, K0122, K0182, K0185, K0304, K0608, S0065, S0068, S0069, S0071, S0090, S0091

Searching and sorting data

Course | 6 minutes
Data carving in digital forensics.

NICE Knowledge and Skill Statements:
K0004, K0017, K0122, K0182, K0185, K0608, S0065, S0068, S0069, S0071, S0090, S0091

Data processing

Course | 7 minutes
A look at data optimization techniques.

NICE Knowledge and Skill Statements:
K0004, K0017, K0122, K0182, K0185, K0304, K0608, S0065, S0068, S0069, S0071, S0090, S0091, S0133

Forensic containers

Course | 2 minutes
Data carving in digital forensics.

NICE Knowledge and Skill Statements:
K0004, K0017, K0122, K0182, K0185, K0304, K0608, S0065, S0068, S0069, S0071, S0090, S0091

Searching and sorting data

Course | 6 minutes
Data carving in digital forensics.

NICE Knowledge and Skill Statements:
K0004, K0017, K0122, K0182, K0185, K0608, S0065, S0068, S0069, S0071, S0090, S0091

Bookmarks

Course | 2 minutes
Exploring bookmarking and filtering data.

NICE Knowledge and Skill Statements:
K0004, K0182, K0185, K0304, S0069, S0071

Reporting

Course | 2 minutes
A look at data reporting.

NICE Knowledge and Skill Statements:
K0004, K0182, K0185, K0304, S0069, S0071
Windows Registry Forensics

The Windows Registry Forensics learning path will enable you to understand the purpose and structure of the files that create the Windows Registry. You will learn to identify, extract and interpret important data from a live and non-live Windows Registry.

Skill Assessment
Skill assessment | 20 questions
See how your Windows Registry forensics skills stack up against other professionals in your field.

Windows Registry Forensics Project
Project | 2 hours 37 minutes
Practice your Windows Registry forensics skills by solving challenges.

NICE Knowledge and Skill Statements:
S0071, S0091

Introduction to the Windows Registry
Course | 16 minutes
Discover what the Windows Registry is and why it is important in digital forensic investigations.

NICE Knowledge and Skill Statements:
K0060, K0133, K0433

Preparing to Examine the Windows Registry
Course | 57 minutes
This course takes a look at the location of the Registry files within the Windows OS and the many tools freely available to view the file structure and artifacts contained within the Windows Registry.

NICE Knowledge and Skill Statements:
K0132, K0133, K0433, S0069, S0071

NTUser.Dat Hive File Analysis
Course | 2 hours 26 minutes
This course demonstrates an in-depth analysis of the artifacts contained within the NTUser.Dat hive file.

NICE Knowledge and Skill Statements:
K0116, K0128, K0132, K0133, K0433, K0479, S0091

SAM Hive File
Course | 50 minutes
This course explains forensic artifacts found in the SAM (Security Account Manager) file, which stores and organizes information about each user on a system.

NICE Knowledge and Skill Statements:
K0128, K0132, K0133, K0433, S0091
### Software Hive File

Course | 1 hour 4 minutes

This course will show examiners how to locate information of forensic value relating to application execution and installation contained within the software hive file.

**NICE Knowledge and Skill Statements:**

K0128, K0132, K0133, K0433, K0449, S0091

### System Hive File

Course | 1 hour 13 minutes

This course will demonstrate evidence of forensic value contained within the system hive file.

**NICE Knowledge and Skill Statements:**

K0128, K0132, K0133, K0433, K0449, S0091

### USRClass.dat Hive File

Course | 33 minutes

This course identifies and explains forensic artifacts found in the UsrClass.dat hive file.

**NICE Knowledge and Skill Statements:**

K0116, K0128, K0132, K0133, K0433, K0449, S0091

### AmCache Hive File

Course | 32 minutes

This course will examine the AmCache hive file, which stores information relating to the execution of applications.

**NICE Knowledge and Skill Statements:**

K0128, K0132, K0133, K0433, K0449, S0089, S0091
Security architecture, engineering and management

Security architecture, engineering and management training focuses on the design, implementation and maintenance of cybersecurity systems and programs. It covers advanced understanding of information security concepts, security operations and information assurance, as well as risk management and project management skills.

Azure Security Engineer Associate

Students will explore the necessary skills and knowledge to make use of Microsoft Azure. Students will learn how to implement security controls and threat protection, managing identity and access and protecting data, applications and networks in cloud and hybrid environments as part of an end-to-end infrastructure.

---

**Azure Security Engineer Associate Practice Exam**

Practice Exam | 21 questions

Prepare for your Azure Security Engineer Associate exam and test your knowledge.

**Manage Identity and Access**

Course | 1 hour 28 minutes

In this course, students will learn to work with subscriptions, users and groups by configuring Microsoft Azure Active Directory.

**Implement platform protection**

Course | 3 hours 26 minutes

Learn to implement platform protection.
Manage security operations

Course | 1 hour 48 minutes

Learn how to configure security policies and manage security alerts with the tools and services in Azure.

Secure data and applications

Course | 1 hour 36 minutes

In this course, you will learn harden Azure apps and secure data with encryption, certificates and policies.
Fundamentals of Zero Trust

Zero trust changes how we architect and secure digital systems. It is still a relatively young but fast-maturing field. This learning path aims to give you the fundamentals of zero trust, focusing on the architecture itself. You can start your zero trust journey right here or learn to support your organization's zero trust program.

Introduction to Zero Trust
Course | 2 hours 19 minutes
Explore zero trust, including how current traditional security architectures developed, zero trust's roots, core principles and tenets.

Zero trust threat reduction: a ransomware killer?
Course | 30 minutes
Learn how to reduce your enterprise's threat landscape by up to 95% and discover what the White House sees in zero trust for reducing threats to critical national infrastructure. In this course, we assess the threat vectors that zero trust can mitigate and see it in practice with a live demo of how ransomware can be immobilized by micro-segmentation.

Zero trust tenets and NIST high-level architecture
Course | 1 hour 19 minutes
Learn how to understand zero trust architectures via the NIST High Level Design (an abstract conceptual model) as well as how the core principles of zero trust come to life in the tenets of zero trust.

Zero trust enterprise architecture: what are you protecting?
Course | 54 minutes
Zero trust is a unique transformational opportunity for you to rebuild your security architecture. In this course, we will focus on the subjects and resources in your zero trust architecture: what you can protect with zero trust and what you should protect.

Zero trust architecture (ZTA) design patterns
Course | 1 hour 15 minutes
In this course, you'll learn how to discern the differences between different patterns and gain an appreciation for when each should be used.

Zero trust policy
Course | 42 minutes
Here we will discuss types of policy with an example of a zero trust policy versus a legacy policy.
<table>
<thead>
<tr>
<th>Learning paths</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trust me ... decision &amp; trust algorithms</strong></td>
</tr>
<tr>
<td>Course</td>
</tr>
<tr>
<td>Here we will dissect the policy decision point into its constituent parts and discover how a policy decision point works by using trust algorithms.</td>
</tr>
<tr>
<td><strong>Threats to a zero trust architecture</strong></td>
</tr>
<tr>
<td>Course</td>
</tr>
<tr>
<td>Is a zero trust architecture resilient to cyberattack? What threats can it sustain? Take this course to find out.</td>
</tr>
<tr>
<td><strong>Migrating to a zero trust architecture (ZTA)</strong></td>
</tr>
<tr>
<td>Course</td>
</tr>
<tr>
<td>How do you start your zero trust roadmap? Here we learn how to start a zero trust architecture; how it can reside alongside your traditional security architecture for dual-running; and how to operationalize the ZTA. We also assess a frequently asked question: Can I remove my network-based firewall now that I have a zero trust architecture?</td>
</tr>
</tbody>
</table>
# IAPP CIPM

Make data privacy regulations work for your organization by understanding how to implement them in day-to-day operations. Learn to create a company vision, structure a data protection team, develop and implement system frameworks, communicate with stakeholders, measure performance and more.

## CIPM practice exam

**Practice Exam | 35 questions**

Prepare for your IAPP CIPM exam and test your knowledge.

## Developing a privacy program

**Course | 41 minutes**

An exploration of developing a privacy program: the dangers, the challenges and the methods.

**NICE Knowledge and Skill Statements:**

K0003, K0004, K0005, K0044, K0066, K0121, K0260, K0261, K0262, K0501, K0615, S0354, S0367, S0374

## Privacy governance

**Course | 37 minutes**

An exploration of privacy governance challenges and skills.

**NICE Knowledge and Skill Statements:**

K0003, K0004, K0005, K0044, K0066, K0101, K0121, K0260, K0261, K0262, K0411, K0504, K0615, S0027, S0354, S0367, S0374

## Privacy program frameworks

**Course | 38 minutes**

This course discusses existing legislation, standards and frameworks that can be utilized to build a roadmap for your privacy program.

**NICE Knowledge and Skill Statements:**

K0003, K0004, K0005, K0044, K0066, K0121, K0260, K0261, K0262, K0615, S0147, S0354, S0367, S0374

## Legal jurisdictions and global data flows

**Course | 52 minutes**

This course discusses existing legislation, standards and frameworks that can be utilized to build a roadmap for your privacy program.

**NICE Knowledge and Skill Statements:**

K0003, K0004, K0005, K0044, K0066, K0121, K0123, K0155, K0156, K0168, K0222, K0260, K0261, K0262, K0267, K0410, K0411, K0615, S0354, S0367, S0374

## Data assessments

**Course | 1 hour 2 minutes**

Exploring data assessments, data inventories, privacy risk assessments and more.

**NICE Knowledge and Skill Statements:**

K0003, K0004, K0005, K0006, K0044, K0066, K0121, K0165, K0260, K0261, K0262, K0501, K0615, S0080, S0189, S0271, S0354, S0360, S0367, S0374
Information security and protection of data

Course | 44 minutes
This course looks at the basics of information security, focusing on risk assessment to keep the level of technical and organizational controls appropriate to the organization.

NICE Knowledge and Skill Statements:
K0003, K0004, K0005, K0044, K0066, K0121, K0260, K0261, K0262, K0264, K0265, K0267, K0297, K0354, S0170, S0354, S0367, S0374

Privacy rights

Course | 53 minutes
This course looks at global privacy rights, using the EU GDPR as its focus.

NICE Knowledge and Skill Statements:
K0003, K0004, K0005, K0044, K0066, K0121, K0260, K0261, K0262, K0264, K0265, S0354, S0367, S0374

Managing a security breach

Course | 37 minutes
This course looks at what happens when security is breached, including the difference between an incident and a breach and steps to be taken in order to detect, assess, respond to and learn from security incidents.

NICE Knowledge and Skill Statements:
K0003, K0004, K0005, K0042, K0044, K0066, K0121, K0231, K0260, K0261, K0262, K0292, K0399, S0519, K0615, S0054, S0354, S0367, S0374

Continual improvement

Course | 43 minutes
A look at continual improvement: understanding performance, exploring metrics, audit methodologies and more.

NICE Knowledge and Skill Statements:
K0003, K0004, K0005, K0044, K0066, K0121, K0198, K0260, K0261, K0262, S0051, K0615
ISACA CIPT

This path explores the intersection of technology, data security, and policy. You’ll learn key concepts about privacy and compliance, as well as the frameworks and tech to support these. We’ll cover threats and violations, privacy by design, data management strategies, encryption and more. You’ll also get tips on passing the CIPT exam, as well as practice materials.

<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Table of contents</th>
<th>Boot camps</th>
<th>Self-paced training</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
</table>

### CIPT Practice Exam

Practice exam | 70 questions
---
Prepare for your IAPP Certified Information Privacy Technologist exam and test your domain knowledge.

### Privacy fundamentals

Course | 37 minutes
---
In this course, you’ll learn about the origins of modern privacy law and theory. What is anonymity? How do we define privacy harms? You’ll see how these relate to today’s privacy questions and dilemmas. You’ll also learn about commonly recognized frameworks such as the Fair Information Practice Principles, the OECD model for protecting privacy and data security and the phases of the data life cycle.

### Privacy in engineering

Course | 1 hour 24 minutes
---
In this course, you’ll cover a broad range of topics like risk management, the software development life cycle and requirements gathering. We’ll also go in-depth on systems architecture, modeling and documentation, design patterns and defining privacy harms from an engineering prospective. Finally, we’ll explore systems testing from all angles.

### Encryption

Course | 51 minutes
---
In this course, students will explore privacy and encryption fundamentals. We’ll start with a high-level overview, including many of the terms you’ll need to fully understand encryption concepts.

### Identity

Course | 32 minutes
---
This course discusses the concept of identity. There are many levels at which we can identify an individual, from completely identified to completely anonymous. We’ll cover these in depth and explain why these concepts are important to safeguarding data and privacy. We’ll also explore anonymization concepts and techniques. Finally, we’ll take an in-depth look at authentication concepts and practices, as well as some of the challenges identity presents in today’s privacy environment.

### Designing privacy interfaces

Course | 1 hour 6 minutes
---
This course is all about keeping the user and privacy in focus in our designs. We’ll explore some of the psychology behind how users make privacy-related decisions and why the privacy paradox sometimes prevents individuals from making the choices they really want to make.
### Surveillance & tracking

**Course | 1 hour 17 minutes**

This course gets into the ways in which users are tracked, and how they can protect themselves. We'll look at why companies, organizations and governments track and surveil users as well as the underlying internet technologies that make tracking users possible.

### Interference

**Course | 29 minutes**

In this course, we'll talk about the ways in which spam, behavior profiling, machine learning, cyberbullying and more can change the way people behave and the kinds of decisions they make. We'll also cover some best practices to reduce these harms.

### Cybersecurity principles

**Course | 29 minutes**

In this course, you'll learn about how cybersecurity principles can help to protect privacy. We'll discuss concepts like the CIA Triad, dealing with adversaries and attacks and malware, and principles like least privilege and implementing multiple layers of defense.

### Data governance

**Course | 25 minutes**

We'll talk in-depth about data governance, a few representative privacy laws and how compliance and technology intertwine. We'll also cover the principles of privacy by design, which help us put our users and their privacy needs front and center when we are creating and maintaining our apps and systems.
ISACA CISM

CERTIFICATION PATH

The Certified Information Security Manager (CISM) certification path is designed for individuals who oversee, design or assess an enterprise’s information security.

CISM Practice Exam

Practice Exam | 20 questions

Prepare for your CISM exam and test your knowledge.

Domain 1: Information Security Governance

Course | 2 hours 42 minutes

This course walks users through all the sections of domain 1 of the CISM exam. The topics covered range from designing a security strategy to gaining management support and putting that strategy into action.

NICE Knowledge and Skill Statements:
K0006, K0047, K0084, K0146, K0214, K0234, K0248, K0249, K0432, K0501, K0518, K0536, S0147, S0185, S0216, S0273, S0306

Domain 2: Information Risk Management

Course | 2 hours 43 minutes

The second course in the CISM learning path covers Domain 2. It has sections dedicated to risk identification as well as analysis or risk, how to treat it and the risk monitoring and reporting process.

NICE Knowledge and Skill Statements:
K0002, K0006, K0027, K0037, K0038, K0048, K0065, K0084, K0126, K0146, K0154, K0165, K0169, K0214, K0379, K0455, K0527, K0624, S0124, S0147, S0175, S0244

Domain 3: Information Security Program Development and Management

Course | 2 hours 43 minutes

This course covers Domain 3 of CISM and focuses on information security program development and management.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0043, K0047, K0072, K0090, K0121, K0146, K0150, K0257, K0270, K0287, K0432, K0501, K0518, S0185, S0209

Domain 4: Information Security Incident Management

Course | 2 hours 49 minutes

The final course of the CISM certification path focuses on Domain 4 and has sections dedicated to information security incident management.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0021, K0026, K0041, K0042, K0072, K0150, K0157, K0162, K0177, K0221, K0332, S0003, S0047, S0054, S0173, S0365
The Certified in Risk and Information Systems Control (CRISC) exam is a certification testing a student's ability to assess and evaluate risk, as well as risk management proficiency. This learning path will provide students with the knowledge and abilities necessary to pass the CRISC exam.

**CRISC Practice Exam**
Practice Exam | 74 questions
Prepare for your CRISC exam and test your knowledge.

**Domain 1: IT Risk Identification**
Course | 2 hours 52 minutes
This module walks users through all the sections of Domain 1 of the CRISC exam. There are seven learning tasks associated with this domain.

**NICE Knowledge and Skill Statements:**
K0002, K0048, K0126, K0149, K0154, K0169, K0195, K0379, K0455, K0506, K0527, K0624, S0304

**Domain 2: IT Risk Assessment**
Course | 2 hours 16 minutes
This module walks users through all the sections of Domain 2 of the CRISC exam. There are six learning tasks associated with this domain.

**NICE Knowledge and Skill Statements:**
K0002, K0048, K0126, K0149, K0154, K0169, K0195, K0379, K0455, K0506, K0527, K0624, S0034, S0080, S0171, S0304

**Domain 3: Risk Response and Mitigation**
Course | 1 hour 46 minutes
This module walks users through all the sections of Domain 3 of the CRISC exam. There are seven learning tasks associated with this domain.

**NICE Knowledge and Skill Statements:**
K0002, K0041, K0042, K0048, K0126, K0149, K0150, K0154, K0169, K0195, K0379, K0506, K0527, K0624, S0079, S0080, S0304

**Domain 4: Risk and Control Monitoring and Reporting**
Course | 2 hours 37 minutes
This module walks users through all the sections of Domain 4 of the CRISC exam. There are seven learning tasks associated with this domain.

**NICE Knowledge and Skill Statements:**
K0002, K0048, K0126, K0149, K0154, K0169, K0195, K0180, K0195, K0379, K0451, K0455, K0527, K0624, S0136, S0304
ISC2 Certified in Governance, Risk and Compliance (CGRC) (previously - CAP)

The Certified in Governance, Risk and Compliance (CGRC) certification path builds your expertise around the NIST Risk Management Framework (RMF). You'll learn best practices, policies and procedures used to authorize and maintain information systems.

**CERTIFICATION PATH**

**Skill Assessment**

Skill assessment | 20 questions
See how your CGRC skills stack up against other professionals in your field.

**CGRC Practice Exam**

Practice Exam | 125 questions
Prepare for your CGRC exam and test your domain knowledge.

**Introduction to CGRC**

Course | 2 minutes
Start off your exploration of CGRC, or Certified Authorization Professional, with this introductory course looking at the basics of your education path.

**Information Security Risk Management Program**

Course | 39 minutes
This course on risk management in a CGRC context covers security objectives, risk management programs, essential laws and documents, key roles (including federal entities) and more. Includes vocabulary and diagrams.

**Risk Management Program Processes**

Course | 9 minutes
In this course you'll explore the details of the risk management framework, including vocabulary, objectives and tasks.

**Regulatory and Legal Requirements**

Course | 40 minutes
Take a closer look at the regulatory and legal requirements connected to risk management, including federal laws, NIST documents and the Committee on National Security.
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categorization of Information Systems</td>
<td>21 minutes</td>
<td>K0003, K0004, K0048, K0053, K0081, K0199, K0260, K0579, S0078</td>
</tr>
<tr>
<td>Selection of Security Controls</td>
<td>9 minutes</td>
<td>K0002, K0004, K0048, K0065, K0612, S0007, S0031, S0034, S0097, S0147, S0152</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>17 minutes</td>
<td>K0002, K0004, K0005, K0006, K0007, K0013, K0040, K0048, K0070, K0161, K0162, K0165, K0177, K0336, K0344, K0579, S0078, S0167</td>
</tr>
<tr>
<td>Implementation of Security Controls</td>
<td>27 minutes</td>
<td>K0002, K0004, K0042, K0048, K0065, K0179, K0202, K0276, K0480, K0612, S0007, S0031, S0032, S0034, S0097, S0147, S0152</td>
</tr>
<tr>
<td>Assessment of Security Controls</td>
<td>11 minutes</td>
<td>K0002, K0004, K0005, K0013, K0048, K0065, K0342, K0579, K0612, S0031, S0034, S0051, S0137, S0147, S0152, S0167</td>
</tr>
<tr>
<td>Authorization of Information Systems</td>
<td>11 minutes</td>
<td>K0002, K0004, K0005, K0007, K0048, K0054, K0065, K0180, K0336, S0031, S0034, S0136, S0147, S0152, S0155</td>
</tr>
<tr>
<td>Continuous Monitoring</td>
<td>22 minutes</td>
<td>K0002, K0004, K0048, K0054, K0064, K0073, K0180, K0275, K0393, S0136, S0147, S0153, S0155</td>
</tr>
<tr>
<td>Preparing for the CGRC Exam</td>
<td>6 minutes</td>
<td>K0004, K0048</td>
</tr>
</tbody>
</table>
# ISC2 Certified Cloud Security Professional (CCSP)

The Certified Cloud Security Professional (CCSP) certification path teaches you the fundamentals of the cloud computing architecture framework and how to evaluate and implement appropriate controls around cloud services.

## Skill Assessment

Skill assessment | 20 questions

See how your CCSP skills stack up against other professionals in your field.

## CCSP Practice Exam

Practice Exam | 1,311 questions

Prepare for your CCSP exam and test your domain knowledge.

## Cybersecurity Basics

Course | 1 hour

Build a baseline of cybersecurity knowledge in this introductory course.

### NICE Knowledge and Skill Statements:

K0003, K0004, K0047, K0049, K0101, K0524, K0612

## Cloud Concepts, Architecture and Design

Course | 3 hours 38 minutes

Get an overview of cloud computing concepts, models (services & deployments) and principles. This course will build your knowledge of virtualization, treat modeling and design cloud requirements.

### NICE Knowledge and Skill Statements:

K0019, K0047, K0049, K0112, K0130, K0190, K0205, K0230, K0277, K0609, K0612

## Cloud Data Security

Course | 1 hour 29 minutes

Get an overview of data classification and categorization, data lifecycle stages, data retention and auditing, as well as an introduction to information and digital rights management.

### NICE Knowledge and Skill Statements:

K0004, K0007, K0025, K0038, K0065, K0158, K0195, K0287, K0377, K0622

## Cloud Platform and Infrastructure Security

Course | 1 hour 41 minutes

Build a baseline of knowledge around cloud security strategies, risks and responsibilities, storage and business continuity programs.

### NICE Knowledge and Skill Statements:

K0004, K0021, K0026, K0038, K0097, K0145, K0230, K0622
## Cloud Application Security

**Course | 38 minutes**

Explore the software development lifecycle, as well as the testing, architecture and auditing of cloud services.

### NICE Knowledge and Skill Statements:
- K0004, K0005, K0006, K0081, K0090, K0153, K0339, K0342, K0373, K0624

## Cloud Security Operations

**Course | 1 hour 22 minutes**

Learn the Uptime Institute requirements for achieving data center high availability through redundancy, capacity and maintenance monitoring, risk management, and change and configuration monitoring to achieve high availability, datacenter redundancy and standards.

### NICE Knowledge and Skill Statements:
- K0002, K0004, K0032, K0048, K0074, K0090, K0145, K0180, K0243

## Cloud Legal, Risk and Compliance Requirements

**Course | 55 minutes**

Build your knowledge of relevant jurisdictional laws, statues, regulations and frameworks, as well as the doctrine of proper law for the protection of data in cloud computing.

### NICE Knowledge and Skill Statements:
- K0003, K0004, K0005, K0006, K0158, K0524

## CCSP Exam Essentials

**Course | 17 minutes**

Review key knowledge areas to help focus your studies and prepare for the CCSP exam.
ISC2 CISSP

The Certified Information Systems Security Professional (CISSP) certification path teaches you the skills and best practices needed to create and execute enterprise-wide information security strategies.

Skill Assessment

Skill assessment | 20 questions
See how your CISSP skills stack up against other professionals in your field.

CISSP Practice Exam

Practice Exam | 2,170 questions
Prepare for your CISSP exam and test your domain knowledge.

Security Governance Principles

Course | 16 minutes
Explore security governance and how it relates to business processes and strategies in this brief overview course.

NICE Knowledge and Skill Statements:
K0004, K0006, K0047, K0146, K0261, K0295, K0511, K0579

Regulatory Compliance

Course | 30 minutes
Explore the compliance issues related to digital data, including privacy laws, regulations, intellectual property issues and more.

NICE Knowledge and Skill Statements:
K0003, K0004, K0006, K0157, K0196, K0260, K0261, K0262, K0410, K0524, K0615

Risk Management

Course | 49 minutes
Dive deep into risk management, including risk frameworks, assessments and modeling, as well as employee security awareness, vendor security and other issues.

NICE Knowledge and Skill Statements:
K0002, K0005, K0047, K0048, K0162, K0165, K0169, K0214, K0295, K0455, K0527

Security Policies

Course | 22 minutes
Explore security policies and control frameworks and how they help drive the overall security of an organization.

NICE Knowledge and Skill Statements:
K0004, K0006, K0157, K0169, K0215, K0242, K0243, K0264
### Asset Security

Course | 39 minutes

Learn how to secure sensitive data, including managing and classifying data, working with data at rest and in transit, and implementing data security controls.

NICE Knowledge and Skill Statements: K0049, K0065, K0083, K0195, K0287, K0377, K0622

### Cryptography Fundamentals

Course | 41 minutes

Explore the uses and challenges of cryptography. Learn about hashing, ciphers, digital signatures, types of cryptography and more.

NICE Knowledge and Skill Statements: K0004, K0018, K0190, K0295, K0305, K0308, K0403, K0427, K0622

### Public Key Infrastructure

Course | 21 minutes

Dig into the inner-workings of Public Key Infrastructure (PKI), including key components, certificates, key management and more.

NICE Knowledge and Skill Statements: K0004, K0018, K0056, K0190, K0285, K0403, K0427

### Secure Design Principles

Course | 39 minutes

Explore the principles behind secure system design, ranging from security models to certification and accreditation.

NICE Knowledge and Skill Statements: K0037, K0044, K0047, K0075, K0170, K0180, K0198, K0203, K0211, K0240, K0288, K0291, K0320, K0362, K0624

### System Protection Mechanisms

Course | 32 minutes

Learn about different system protection mechanisms and common issues such as Web-based vulnerabilities, architecture flaws and more.

NICE Knowledge and Skill Statements: K0004, K0070, K0077, K0090, K0109, K0199, K0209, K0271, K0322, K0392, K0493, K0624

### Physical Security

Course | 52 minutes

Don't forget about physical security! Explore how to keep your business secure starting with secure design and construction to physical intrusion detection and more.

NICE Knowledge and Skill Statements: K0065, K0075, K0165, K0244, S0023

### Data Center Security

Course | 21 minutes

Don't let an incident at your data center disrupt your organization. Explore ways to keep data centers secure from a variety of threats.

NICE Knowledge and Skill Statements: K0032, K0622

### Database Security

Course | 20 minutes

How do you keep a database secure? Revisit the key concepts behind database security in this brief course.

NICE Knowledge and Skill Statements: K0022, K0023, K0024, K0069, K0095, K0373, K0419, K0622

### Network Fundamentals

Course | 1 hour 20 minutes

Go in-depth into networking devices and technologies. Explore network types, protocols, models, attacks, security and more.

NICE Knowledge and Skill Statements: K0001, K0010, K0034, K0050, K0057, K0061, K0093, K0136, K0159, K0170, K0221, K0265, K0274, K0303, K0332, K0333, K0395, K0417, K0437, K0443, K0462, K0470, K0471, K0489, K0516, K0565, K0612, S0236
<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
<th>Description</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Network Design</td>
<td>26 mins</td>
<td>Explore key concepts behind secure network design, including tools to keep threats out and techniques to detect and deflect intruders that breach your defenses.</td>
<td>K0001, K0004, K0034, K0049, K0179, K0276, K0291, K0324, K0326, K0452, K0487, K0488, K0493, K0561, S0023, S0034</td>
</tr>
<tr>
<td>Distributed System &amp; Virtualized Networks</td>
<td>20 mins</td>
<td>Explore the use of distributed and virtualized systems as well as the security benefits and potential drawbacks involved in their use.</td>
<td>K0001, K0063, K0071, K0113, K0130, K0179, K0205, K0437, K0610</td>
</tr>
<tr>
<td>Access Control Fundamentals</td>
<td>1 hour 37 mins</td>
<td>Take a deep dive into one of the fundamental concepts of security: access control. Learn how to give the right people access to the right information in a secure way.</td>
<td>K0007, K0033, K0056, K0065, K0071, K0104, K0158, K0179, K0211, K0332, K0336, K0452, K0488, S0023, S0031</td>
</tr>
<tr>
<td>WAN &amp; Remote Access Security</td>
<td>33 mins</td>
<td>Learn about securing wide area networks (WAN) and remote access against different types of cyber threats in this five-video course.</td>
<td>K0001, K0005, K0070, K0071, K0104, K0113, K0138, K0190, K0269, K0274, K0362, K0395, K0417, K0427, K0438</td>
</tr>
<tr>
<td>Security Assessment</td>
<td>20 mins</td>
<td>Refresh your knowledge of cybercrime investigations with this overview course covering the investigation process and the discovery of digital evidence.</td>
<td>K0017, K0118, K0122, K0123, K0125, K0128, K0133, K0155, K0156, K0184, K0222, K0251, K0304, K0433</td>
</tr>
<tr>
<td>Preventative &amp; Detective Measures</td>
<td>39 mins</td>
<td>Explore ways to prevent cyber threats from impacting your organization, and learn how to quickly detect the threats that do slip through your defenses.</td>
<td>K0004, K0006, K0049, K0073, K0074, K0132, K0145, K0167, K0205, K0275, K0480, K0487, K0488, K0561</td>
</tr>
<tr>
<td>Business Continuity Planning</td>
<td>19 mins</td>
<td>Learn how to keep your business up and running. Explore the importance of continuity planning, incident response planning and impact analysis.</td>
<td>K0006, K0026, K0032, K0041, K0042, K0150, K0165, K0292</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>36 mins</td>
<td>Don’t let a lack of preparedness compound the effects of a disaster. Learn how to create and test a disaster recovery plan in this six-video course.</td>
<td>K0006, K0021, K0026, K0032, K0150, K0210, K0292, K0399, K0519, K0527</td>
</tr>
</tbody>
</table>
Secure Software Design

Course | 25 minutes

Explore the methods of creating secure software, including development and maturity models and the secure software development life cycle.

NICE Knowledge and Skill Statements:
K0004, K0039, K0047, K0081, K0153, K0198, K0200, K0258

Secure Software Development

Course | 43 minutes

Explore the ins and outs of secure software development as you progress through this nine-video course.

NICE Knowledge and Skill Statements:
K0039, K0070, K0153, K0276, K0373, K0396, K0480
ISC2 CISSP-ISSAP

The Information Systems Security Architecture Professional (CISSP-ISSAP) certification path teaches you how to provide risk-based guidance to senior management and develop, design and analyze security solutions that meet organizational goals.

Skill Assessment
Skill assessment | 20 questions
See how your CISSP-ISSAP skills stack up against other professionals in your field.

CISSP-ISSAP Practice Exam
Practice Exam | 125 questions
Prepare for your CISSP-ISSAP exam and test your domain knowledge.

Introduction to ISSAP
Course | 9 minutes
An overview of the CISSP-ISSAP credential and the certification exam.

Identity and Access Management Architecture
Course | 1 hour 23 minutes
Understand the lifecycle and the design of the identity management architecture.

NICE Knowledge and Skill Statements:
K0004, K0007, K0024, K0027, K0047, K0056, K0065, K0075, K0100, K0158, K0170, K0199, K0291, K0336, 50031, 50043, 50084

Security Architecture Modeling
Course | 41 minutes
Identify the correct approach for the organization’s security architecture.

NICE Knowledge and Skill Statements:
K0004, K0027, K0047, K0100, K0199, K0203, K0288, K0437

Architecture for Governance, Compliance and Risk Management
Course | 41 minutes
Discover the principles, processes and standards related to GRC (governance, risk management and compliance).

NICE Knowledge and Skill Statements:
K0002, K0004, K0006, K0027, K0047, K0048, K0100, K0101, K0202, K0260, K0261, K0262, K0267 K0455, K0527
<table>
<thead>
<tr>
<th>Security Operations Architecture</th>
<th>Infrastructure Security</th>
<th>Architect for Application Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Course</td>
<td>1 hour 30 minutes**</td>
<td>**Course</td>
</tr>
<tr>
<td>Know how to design and implement the appropriate architecture for security operations.</td>
<td>Get an overview of various protocols, controls and activities involved in designing infrastructure security.</td>
<td>Learn about common app-related threats and how to address them through the development lifecycle.</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**

Security Operations Architecture:

- K0004, K0021, K0026, K0027, K0046, K0047, K0093, K0100, K0242, K0299, K0324, K0417, K0432, K0440, K0481, K0531, S0032, S0145

Infrastructure Security:

- K0001, K0004, K0018, K0019, K0027, K0034, K0047, K0050, K0057, K0061, K0071, K0093, K0100, K0136, K0159, K0170, K0190, K0221, K0265, K0274, K0285, K0300, K0303, K0308, K0332, K0333, K0395, K0403, K0417, K0427, K0452, K0470, K0471, K0489, K0516, K0565, K0612, S0145

Architect for Application Security:

- K0004, K0005, K0009, K0070, K0081, K0082, K0186, K0373, K0396, K0624
ISC2 CISSP-ISSEP

**CERTIFICATION PATH**

The Information Systems Security Engineering Professional (CISSP-ISSEP) certification path teaches you how to design, construct and operate a network with a defined level of availability, integrity and confidentiality.

<table>
<thead>
<tr>
<th>Skill Assessment</th>
<th>CISSP-ISSEP Practice Exam</th>
<th>Introduction to ISSEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill assessment</td>
<td>20 questions</td>
<td>Practice Exam</td>
</tr>
<tr>
<td>See how your CISSP-ISSEP skills stack up against other professionals in your field.</td>
<td>Prepare for your CISSP-ISSEP exam and test your domain knowledge.</td>
<td>Get an overview of the Information Systems Security Engineering process and components.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Engineering Principles</th>
<th>Risk Management</th>
<th>System Resilience Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>22 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Review the security principles that security engineers need to know in order to implement systems.</td>
<td>Get a basic understanding or risk management in an organization.</td>
<td>Dive into defense-in-depth and other principles and methods of making your systems resilient.</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**

- Security Engineering Principles: K0004, K0005, K0006, K0044, K0157, K0158, K0267, K0287, K0568, K0584
- Risk Management: K0002, K0004, K0214, K0455, K0527
- System Resilience Principles: K0002, K0004, K0032, K0112, K0179, K0299, K0323, K0527, S0027, S0076
Vulnerability Management Principles
Course | 13 minutes
Know why it's important to manage vulnerabilities, and what the engineer's role is.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0013, K0040, K0106, K0147, K0157, K0187, K0339, K0373, K0392, K0624, S0036, S0078

Risk Management Process
Course | 37 minutes
Walk through the security risk management process and learn best practices.

NICE Knowledge and Skill Statements:
K0002, K0004, K0047, K0048, K0165, K0214, K0264, K0455, K0527

Operational Risk Management
Course | 30 minutes
Understand how today's complex business environment impacts operational risk and related controls.

NICE Knowledge and Skill Statements:
K0004, K0047, K0048, K0084, K0154, K0169, K0214, K0264, K0379, K0455, K0527

Stakeholder Requirements Definition
Course | 14 minutes
Review how different stakeholders impact security planning, design and implementation.

NICE Knowledge and Skill Statements:
K0004, K0169, K0376, K0379

Requirements Analysis
Course | 7 minutes
Discover the process for analyzing requirements before designing security systems.

NICE Knowledge and Skill Statements:
K0004, K0028, K0035, K0073, K0086, K0090, K0091, K0102, K0164, K0291, K0475, K0480

System Security Architecture and Design
Course | 12 minutes
Review the core components and processes of security architecture and design.

NICE Knowledge and Skill Statements:
K0004, K0044, K0047, K0075, K0087, K0170, K0180, K0198, K0199, K0203, K0211, K0240, K0267, K0288, K0291, S0023

Implementation, Integration and Deployment of System Modifications
Course | 5 minutes
Learn the basics of system implementation, integration and deployment.

NICE Knowledge and Skill Statements:
K0004, K0073, K0082, K0091, K0178, K0179, K0186, K0257, K0270, K0393, K0452, K0488, S0153

Verification and Validation of Systems or System Modifications
Course | 10 minutes
Go through the post-deployments steps of ensuring the system is adequately secure.

NICE Knowledge and Skill Statements:
K0004, K0028, K0091, S0110, S0282

Secure Operations
Course | 30 minutes
Understand the basics of maintaining a secure operations strategy.

NICE Knowledge and Skill Statements:
K0004, K0006, K0026, K0041, K0042, K0074, K0086, K0150, K0167, K0292, K0324, K0333, K0403, K0488
Secure Maintenance

Course | 13 minutes

Learn about the three main areas of secure maintenance and related strategies.

NICE Knowledge and Skill Statements:
K0004, K0035, K0074, K0103, K0167, K0294, K0419, S0027

Secure Disposal

Course | 8 minutes

Know how to handle a system at the end of its lifecycle and the key security considerations.

NICE Knowledge and Skill Statements:
K0004, K0090, K0270

Acquisition Process

Course | 15 minutes

Know what's involved in the systems acquisition phase and how to prepare for it.

NICE Knowledge and Skill Statements:
K0004, K0154, K0164, K0169, K0198, K0257, K0264, K0270, K0376, K0379

System Development Methodologies

Course | 3 minutes

Understand the advantages and disadvantages of different development methods.

NICE Knowledge and Skill Statements:
K0004, K0035, K0039, K0047, K0079, K0081, K0082, K0086, K0087, K0153, K0186, K0276

Technical Management Processes

Course | 32 minutes

Dive deep into the technical aspects of managing systems engineering.

NICE Knowledge and Skill Statements:
K0002, K0004, K0005, K0006, K0150, K0233, K0264, K0527, S0358
# CISSP-ISSEP (2021 Update)

The Information Systems Security Engineering Professional (ISSEP) certification path is a focused study in all aspects of system security engineering.

## CISSP-ISSEP Practice Exam

**Practice Exam | 125 questions**

Prepare for your CISSP-ISSEP exam and test your domain knowledge.

## Introduction to System Security Engineering

**Course | 1 hour 40 minutes**

A captivating look into the world of system and security engineering.

**NICE Knowledge and Skill Statements:**

K0004, K0005, K0045, K0067, K0076, K0081, K0082, K0102, K0153, K0280, K0321, S0052, S0140

## Domain 1: Systems Security Engineering Foundations

**Course | 1 hour 48 minutes**

This course covers systems security engineering and lays a foundation for both exam preparation and security engineering.

**NICE Knowledge and Skill Statements:**

K0004, K0005, K0006, K0045, K0067, K0076, K0081, K0082, K0092, K0102, K0153, K0280, K0321, K0435, K0436, K0560, S0052, S0140

## Domain 2: Risk Management

**Course | 1 hour 34 minutes**

Domain 2 focuses on the risk management practices necessary to protect the health of our organization.

**NICE Knowledge and Skill Statements:**

K0002, K0004, K0005, K0006, K0038, K0045, K0048, K0067, K0082, K0092, K0101, K0102, K0149, K0165, K0280, K0435, K0436, K0455, K0506, K0527, S0304

## Domain 3: Security Planning and Design

**Course | 1 hour 4 minutes**

Domain 3 introduces security planning and design, taking us from requirement to completed solutions.

**NICE Knowledge and Skill Statements:**

K0001, K0004, K0005, K0006, K0045, K0067, K0075, K0076, K0080, K0081, K0082, K0086, K0092, K0102, K0153, K0332, K0347, K0435, K0498, K0519, S0022, S0036, S0135, S0141, S0160

## Domain 4: Systems Implementation, Verification and Validation

**Course | 27 minutes**

Domain 4 looks at deploying, verifying and validating security controls within our enterprises.

**NICE Knowledge and Skill Statements:**

K0004, K0006, K0028, K0045, K0054, K0067, K0073, K0075, K0076, K0080, K0081, K0082, K0102, K0153, K0347, K0488, S0032, S0036, S0040, S0135, S0141, S0160, S0218, S0282
Domain 5: Secure Operations, Change Management and Disposal

Course | 1 hour 45 minutes

Domain 5 addresses the long-term management of our enterprise, from implementation to sunsetting of our systems.

NICE Knowledge and Skill Statements:
K0004, K0006, K0028, K0045, K0073, K0075, K0080, K0081, K0102, K0153, K0299, K0347, K0488, S0027, S0032, S0036, S0040, S0135, S0141, S0160, S0280, S0282
The Information System Security Management Professional (CISSP-ISSMP) certification path teaches you the necessary skills and knowledge to successfully manage an enterprise security program.

**ISSMP Practice Exam**

Practice Exam | 200 questions

Prepare for your ISSMP exam and test your domain knowledge.

**Leadership and Business Management**

Course | 2 hours 45 minutes

In this course, you'll look at how to align your security program with your organization's governance structure and define and implement your security strategies, maintain your security framework, define metrics and more.

**NICE Knowledge and Skill Statements:**
K0003, K0004, K0072, K0101, K0121, K0264, K0293, K0296, K0425, K0477, K0518, K0579, S0038, S0056

**Systems Life Cycle Management**

Course | 2 hours 37 minutes

Learn how to integrate security into the system development life cycle, integrate new business initiatives and emerging technologies, oversee a vulnerability management program and manage the security aspects of change management.

**Risk Management**

Course | 1 hour 22 minutes

In this course, you'll learn how to develop and manage a risk management program. You will also learn to conduct risk assessments and a Business Impact Analysis (BIA).

**NICE Knowledge and Skill Statements:**
K0002, K0004, K0048, K0084, K0149, K0154, K0165, K0169, K0214, K0263, K0264, K0267, K0379, K0455, K0527, S0171

**Threat Intelligence and Incident Management**

Course | 1 hour 6 minutes

Learn how to establish and maintain a threat intelligence program, conduct a baseline analysis and do threat modeling. Then you'll explore incident handling and investigations, the IR process, root cause analysis and more.

**NICE Knowledge and Skill Statements:**
K0004, K0021, K0026, K0041, K0042, K0146, K0150, K0231, K0267, K0292, K0317, K0343, K0381, K0399, K0519, K0543, K0586, S0032, S0054, S0080, S0175, S0365

**Contingency Management**

Course | 1 hour 43 minutes

In this course, you'll learn how to oversee the development of contingency plans. You'll address recovery strategy development and managing BCP and DRP plans, finally ending up with a discussion of how to manage the recovery process.

**NICE Knowledge and Skill Statements:**
K0004, K0021, K0026, K0032, K0041, K0042, K0046, K0150, K0157, K0210, K0292, K0353, K0399, K0519, K0584, S0032, S0054, S0186, S0365
Law, Ethics and Security Compliance Management

Course | 1 hour 54 minutes

We will discuss the ISC2 code of ethics, compliance issues with organization security policies and procedures, coordinating and assisting with auditors and the audit process, and managing exceptions to compliance.

NICE Knowledge and Skill Statements:
K0003, K0004, K0157, K0196, K0260, K0261, K0262, K0267, K0351, K0410, K0524, K0615
Blockchain Security

Skill Assessment

Skill assessment | 20 questions

See how your blockchain security skills stack up against other professionals in your field.

Blockchain Security Project

Project | 2 hours 11 minutes

Practice your blockchain security skills as your progress through five challenges.

Fundamentals of Blockchain Security

Course | 1 hour 6 minutes

This course introduces the fundamentals of blockchain security, from foundational concepts of blockchain and how the components of the blockchain are put together to how public-key cryptography and hash functions are used.

NICE Knowledge and Skill Statements:
K0018, K0019, K0059, K0190, K0403, K0427, K0431

Consensus Algorithm Security

Course | 1 hour 28 minutes

This course describes the underlying principles of consensus algorithms, how two of the primary consensus algorithms work under the hood and how they can be attacked.

NICE Knowledge and Skill Statements:
K0015, K0059, K0431

Blockchain in Action

Course | 1 hour 17 minutes

This course investigates how blocks are created in the blockchain (and how block creation can be attacked) as well as discussing attacks targeting blockchain nodes and the network that ties them together and enables communication.

NICE Knowledge and Skill Statements:
K0019, K0059, K0106, K0147, K0151, K0314, K0362, K0431, K0480, K0531

Smart Contract Security

Course | 1 hour 43 minutes

This course describes what a smart contract is and explores programming vulnerabilities that exist because a smart contract is a program, runs on a blockchain or is implemented on the Ethereum smart contract platform.

NICE Knowledge and Skill Statements:
K0059, K0070, K0431
Beyond the Basics of Blockchain

Course | 55 minutes

This course goes beyond blockchain-based distributed ledgers to discuss how the protocol can be replaced, expanded or improved to overcome some of the limitations of blockchain technology.

NICE Knowledge and Skill Statements:
K0018, K0059, K0427, K0431
Certified Security Awareness Practitioner (CSAP)

Learn the basics of running a successful training and awareness program that gets people’s attention and changes behavior.

<table>
<thead>
<tr>
<th>Training and Awareness Basics Overview</th>
<th>Security Basics</th>
<th>Introduction to Training and Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>5 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Begin at the beginning with this course introducing you to security training and awareness.</td>
<td>Take a look at some fundamental security basics for soft-skill-focused learners.</td>
<td>Take a look at what's going on in the world of training and awareness, including potential obstacles and concerns.</td>
</tr>
</tbody>
</table>

NICE Knowledge and Skill Statements: K0146

<table>
<thead>
<tr>
<th>Sales and Marketing Techniques for Training and Awareness</th>
<th>Creative</th>
<th>Program Execution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>38 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Delve into the role of sales and marketing in security awareness and training.</td>
<td>Explore possible concerns on the creative side of security programs.</td>
<td>Move from theory to practice with this course on executing a security program.</td>
</tr>
</tbody>
</table>

NICE Knowledge and Skill Statements: K0243, K0245

<table>
<thead>
<tr>
<th>NICE Knowledge and Skill Statements: K0252</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0252, K0243, K0245, K0252</td>
</tr>
</tbody>
</table>
Cloud Security Architecture

The Cloud Security Architecture skill path teaches you enterprise security architecture concepts related to the cloud, including cloud infrastructure, data and application security.

### Cloud Data Security

**Course** | 2 hours 35 minutes

Get to grips with cloud data security for aspiring cloud security professionals with this course covering storage types, the six phases of the data life cycle, data security technologies and more.

**NICE Knowledge and Skill Statements:**
K0004, K0007, K0025, K0038, K0065,

### Software Vulnerabilities and Security Controls

**Course** | 37 minutes

In this course, we take you through the fundamentals of software vulnerabilities and security controls.

**NICE Knowledge and Skill Statements:**
K0005, K0049, K0070, K0140, K0624

### Secure Storage Controls

**Course** | 29 minutes

Refresh your knowledge of secure storage controls with this course on storage types, protocols and management.

**NICE Knowledge and Skill Statements:**
K0021, K0038, K0097, K0622

### Securing Host Devices

**Course** | 20 minutes

Explore the challenges of securing host devices with this course on selecting host hardware and software, host hardening and protecting bootloaders.

**NICE Knowledge and Skill Statements:**
K0033, K0109, K0167, K0205, K0440

### Network Security Components

**Course** | 44 minutes

In this course, we help you explore the details of network security components: device types, component management and analyzing components and network configurations.

**NICE Knowledge and Skill Statements:**
K0007, K0011, K0033, K0071, K0145, K0170, K0179, K0296, K0324, K0373, K0487, K0488, K0491, K0561

### Secure Software Development

**Course** | 43 minutes

Explore the ins and outs of secure software development as you progress through this nine-video course.

**NICE Knowledge and Skill Statements:**
K0039, K0070, K0153, K0276, K0373, K0396, K0480
Secure Software Design
Course | 25 minutes
Explore the methods of creating secure software, including development and maturity models and the secure software development life cycle.

NICE Knowledge and Skill Statements:
K0004, K0039, K0047, K0081, K0082, K0153, K0198, K0200, K0258

Distributed System & Virtualized Networks
Course | 20 minutes
Explore the use of distributed and virtualized systems as well as the security benefits and potential drawbacks involved in their use.

NICE Knowledge and Skill Statements:
K0001, K0063, K0071, K0113, K0130, K0179, K0205, K0437, K0610

Cloud Application Security
Course | 2 hours 18 minutes
Cloud application security challenges are no match for this course covering common pitfalls, vulnerabilities, threat modeling, security devices, secure development and more.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0081, K0090, K0153, K0339, K0342, K0373, K0624

Cryptography Fundamentals
Course | 41 minutes
Explore the uses and challenges of cryptography. Learn about hashing, ciphers, digital signatures, types of cryptography and more.

NICE Knowledge and Skill Statements:
K0004, K0018, K0019, K0190, K0295, K0305, K0308, K0403, K0427, K0622

Cloud Platform and Infrastructure Security
Course | 2 hours 44 minutes
Review the fundamentals of cloud platform and infrastructure security with this course covering both physical and virtual security concerns and concepts.

NICE Knowledge and Skill Statements:
K0004, K0021, K0026, K0038, K0097, K0145, K0230, K0622

Operations
Course | 4 hours 27 minutes
Update your knowledge of the Operations domain in cloud security with this course covering logical design, secure configurations, host types, change management and more.

NICE Knowledge and Skill Statements:
K0002, K0004, K0032, K0048, K0074, K0090, K0145, K0180, K0243

Legal and Compliance
Course | 1 hour 57 minutes
Refresh your understanding of legal and compliance issues related to cloud security with this course. Covers key concepts, privacy laws, legal frameworks, country-specific regulations and more.

NICE Knowledge and Skill Statements:
K0003, K0004, K0005, K0006, K0158, K0524

Architectural Concepts & Design Requirements
Course | 4 hours 42 minutes
Brush up on your knowledge of architectural concepts and design requirements with this in-depth course. Review cloud service models, characteristics, deployment models, security and more.

NICE Knowledge and Skill Statements:
K0019, K0047, K0049, K0112, K0130, K0190, K0205, K0230, K0277, K0609, K0612

Data Center Security
Course | 21 minutes
Don't let an incident at your data center disrupt your organization. Explore ways to keep data centers secure from a variety of threats.

NICE Knowledge and Skill Statements:
K0032, K0622
<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Security</td>
<td>52 minutes</td>
<td>K0065, K0075, K0165, K0244, S0023</td>
</tr>
<tr>
<td>Secure Design Principles</td>
<td>39 minutes</td>
<td>K0037, K0044, K0047, K0075, K0170, K0180, K0198, K0203, K0211, K0240, K0288, K0291, K0320, K0362, K0624</td>
</tr>
</tbody>
</table>

Don't forget about physical security! Explore how to keep your business secure starting with secure design and construction to physical intrusion detection and more.

Explore the principles behind secure system design, ranging from security models to certification and accreditation.
# Cloud Security Management

The Cloud Security Management skill path teaches you important security issues related to cloud services, including legal and compliance issues as well as the security of cloud infrastructure, data and applications.

## Architectural Concepts & Design Requirements

Course | 4 hours 24 minutes

Brush up on your knowledge of architectural concepts and design requirements with this in-depth course. Review cloud service models, characteristics, deployment models, security and more.

**NICE Knowledge and Skill Statements:**
K0019, K0047, K0049, K0112, K0130, K0190, K0205, K0230, K0277, K0609, K0612

## Legal and Compliance

Course | 1 hour 57 minutes

Refresh your understanding of legal and compliance issues related to cloud security with this course. Covers key concepts, privacy laws, legal frameworks, country-specific regulations and more.

**NICE Knowledge and Skill Statements:**
K0003, K0004, K0005, K0006, K0158, K0524

## Operations

Course | 4 hours 27 minutes

Update your knowledge of the Operations domain in cloud security with this course covering logical design, secure configurations, host types, change management and more.

**NICE Knowledge and Skill Statements:**
K0002, K0004, K0032, K0048, K0074, K0090, K0145, K0180, K0243

## Cloud Platform and Infrastructure Security

Course | 2 hours 44 minutes

Review the fundamentals of cloud platform and infrastructure security with this course covering both physical and virtual security concerns and concepts.

**NICE Knowledge and Skill Statements:**
K0004, K0021, K0026, K0038, K0097, K0145, K0230, K0622

## Cloud Data Security

Course | 2 hours 35 minutes

Get to grips with cloud data security for aspiring cloud security professionals with this course covering storage types, the six phases of the data life cycle, data security technologies and more.

**NICE Knowledge and Skill Statements:**
K0004, K0007, K0025, K0038, K0065, K0158, K0195, K0287, K0377, K0622

## Cloud Application Security

Course | 2 hours 18 minutes

Cloud application security challenges are no match for this course covering common pitfalls, vulnerabilities, threat modeling, security devices, secure development and more.

**NICE Knowledge and Skill Statements:**
K0004, K0005, K0006, K0081, K0090, K0153, K0339, K0342, K0373, K0624
Cloud Service Provider (CSP) Security Features

In this learning path, students will learn about the areas they will be responsible for when choosing a service with a cloud provider and gain hands-on experience with the three major cloud providers: AWS, Azure and GCP.

Skill Assessment

Skill assessment | 20 questions
See how your CSP security skills stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

Cloud Security Provider (CSP) Roles and Responsibilities

Course | 37 minutes
An overview of the cloud service provider’s roles and responsibilities.

NICE Knowledge and Skill Statements:
K0194, K0230, K0233, K0579, S0073

AWS Security

Course | 1 hour 38 minutes
In this course, we review AWS-native security solutions. Students will have an opportunity for hands-on experience with a project in the console.

NICE Knowledge and Skill Statements:
K0007, K0018, K0021, K0026, K0032, K0038, K0044, K0056, K0065, K0070, K0170, K0179, K0187, K0194, K0210, K0230, K0403, K0579, K0622, K0624, S0073, S0077, S0097

Azure Security

Course | 1 hour 58 minutes
A review of Azure-native security solutions, followed by a console project.

NICE Knowledge and Skill Statements:
K0007, K0018, K0021, K0026, K0032, K0038, K0044, K0056, K0065, K0070, K0170, K0179, K0187, K0194, K0210, K0230, K0403, K0579, K0622, K0624, S0073, S0077, S0097

GCP Security

Course | 1 hour 26 minutes
In this course, we review GCP native security solutions and practice with a console project.

NICE Knowledge and Skill Statements:
K0007, K0018, K0021, K0026, K0032, K0038, K0044, K0056, K0065, K0070, K0170, K0179, K0187, K0194, K0210, K0230, K0403, K0579, K0622, K0624, S0073, S0077, S0097
CompTIA Advanced Security Practitioner (CASP+)

The CompTIA Advanced Security Practitioner (CASP+) certification path prepares your for CompTIA’s most advanced information security certification. You’ll learn the skills required to conceptualize, design and engineer secure solutions across complex enterprise environments.

**Skill Assessment**

Skill assessment | 20 questions

See how your CASP+ skills stack up against other professionals in your field.

**CASP+ Practice Exam**

Practice Exam | 134 questions

Prepare for your CASP+ exam and test your domain knowledge.

**Business and Industry Influences and Risks**

Course | 15 minutes

Brush up on your knowledge of business and industry influences and risks with this course on enterprise risk management (ERM) and business models.

**NICE Knowledge and Skill Statements:**

K0002, K0146, K0527

---

**Security & Privacy Policies and Procedures**

Course | 24 minutes

This course helps you refresh your knowledge of security and privacy policies and procedures.

**NICE Knowledge and Skill Statements:**

K0002, K0003, K0004, K0026, K0048, K0101, K0199, K0260, K0261, K0262, K0267, K0527

---

**Risk Mitigation Strategies and Controls**

Course | 26 minutes

Dive into risk mitigation strategies and controls with this course on risk scenarios, responses and more.

**NICE Knowledge and Skill Statements:**

K0002, K0004, K0048, K0148, K0165, K0169, K0194, K0267, K0527, K0556

---

**Risk Metric Scenarios**

Course | 12 minutes

This course on risk metric scenarios covers analyzing scenarios to secure enterprises and reviewing existing security.

**NICE Knowledge and Skill Statements:**

K0002, K0183, K0527
Network Security Components

Course | 44 minutes

In this course, we help you explore the details of network security components: device types, component management and analyzing components and network configurations.

NICE Knowledge and Skill Statements:
K0007, K0011, K0033, K0071, K0145, K0170, K0179, K0296, K0324, K0373, K0487, K0488, K0491, K0561

Securing Host Devices

Course | 20 minutes

Explore the challenges of securing host devices with this course on selecting host hardware and software, host hardening and protecting bootloaders.

NICE Knowledge and Skill Statements:
K0033, K0109, K0167, K0205, K0440

Secure Storage Controls

Course | 29 minutes

Refresh your knowledge of secure storage controls with this course on storage types, protocols and management.

NICE Knowledge and Skill Statements:
K0021, K0038, K0097, K0622

Software Vulnerabilities and Security Controls

Course | 37 minutes

In this course, we take you through the fundamentals of software vulnerabilities and security controls.

NICE Knowledge and Skill Statements:
K0005, K0049, K0070, K0140, K0624

Vulnerability Assessment Methods and Tools

Course | 21 minutes

This course helps you broaden your understanding of vulnerability assessment and tools, including tool lists and test types.

NICE Knowledge and Skill Statements:
K0005, K0006, K0013, K0106, K0177, K0301, K0342

Research, Development and Collaboration

Course | 33 minutes

In this course, we take you through the details of research, development and collaboration.

NICE Knowledge and Skill Statements:
K0059, K0065, K0081, K0147, K0151, K0309, K0431

Securing Communications and Collaboration Solutions

Course | 14 minutes

Secure your communications and collaboration solutions with this course covering BYOD, mobile device management and more.

NICE Knowledge and Skill Statements:
K0136, K0445, K0446

Implementing Cryptographic Techniques

Course | 30 minutes

Brush up on your understanding of implementing cryptographic techniques with this course covering cryptographic design, techniques and implementations.

NICE Knowledge and Skill Statements:
K0004, K0018, K0019, K0025, K0104, K0201, K0277, K0285, K0305, K0308, K0403, K0427, K0428

Integrating Authentication and Authorization Technologies

Course | 22 minutes

Review and update your knowledge of integrating authentication and authorization technologies with this course covering advanced identity management and more.

NICE Knowledge and Skill Statements:
K0004, K0007, K0056, K0065, K0092
<table>
<thead>
<tr>
<th>Incident Response and Recovery Procedures</th>
<th>Integrating Hosts, Storage, Networks and Applications</th>
<th>Integrating Cloud and Virtualization Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Course</td>
<td>16 minutes**</td>
<td>**Course</td>
</tr>
<tr>
<td>Prepare for possible trouble with this course on incident response and recovery procedures, including designing systems to facilitate incident response.</td>
<td>Put the pieces together with this course on integrating hosts, storage, networks and applications. Includes vocabulary and guidelines.</td>
<td>In this course, you'll get to grips with the challenges of integrating cloud and virtualization technologies. Includes vocabulary and guidelines.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>K0021, K0026, K0041, K0042, K0118, K0125, K0128, K0132, K0133, K0150, K0292</td>
<td>K0035, K0087, K0092, K0332, K0565, K0622</td>
<td>K0004, K0130, K0167, K0230, K0609, K0610</td>
</tr>
</tbody>
</table>
The Cybersecurity Administration skill path covers a variety of high-level tasks related to cybersecurity, including implementing identity and access management, understanding asset security, integrating enterprise security, performing assessments and more.

<table>
<thead>
<tr>
<th>Skill Path</th>
<th>Description</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Metric Scenarios</strong></td>
<td>Course on risk metric scenarios covering analyzing scenarios to secure enterprises and reviewing existing security.</td>
<td>12 minutes</td>
<td>K0002, K0183, K0527</td>
</tr>
<tr>
<td><strong>Vulnerability Assessment Methods and Tools</strong></td>
<td>Course helping you broaden your understanding of vulnerability assessment and tools, including tool lists and test types.</td>
<td>21 minutes</td>
<td>K0005, K0006, K0013, K0106, K0177, K0301, K0342</td>
</tr>
<tr>
<td><strong>Software Vulnerabilities and Security Controls</strong></td>
<td>Course taking you through the fundamentals of software vulnerabilities and security controls.</td>
<td>37 minutes</td>
<td>K0005, K0049, K0070, K0140, K0624</td>
</tr>
<tr>
<td><strong>Integrating Cloud and Virtualization Technologies</strong></td>
<td>Course getting you to grips with the challenges of integrating cloud and virtualization technologies. Includes vocabulary and guidelines.</td>
<td>33 minutes</td>
<td>K0004, K0130, K0167, K0230, K0609, K0610</td>
</tr>
<tr>
<td><strong>Integrating Hosts, Storage, Networks and Applications</strong></td>
<td>Course putting the pieces together with this course on integrating hosts, storage, networks and applications. Includes vocabulary and guidelines.</td>
<td>28 minutes</td>
<td>K0035, K0087, K0092, K0332, K0565, K0622</td>
</tr>
<tr>
<td><strong>Incident Response and Recovery Procedures</strong></td>
<td>Course preparing for possible trouble with this course on incident response and recovery procedures, including designing systems to facilitate incident response.</td>
<td>16 minutes</td>
<td>K0021, K0026, K0041, K0042, K0118, K0125, K0128, K0132, K0133, K0150, K0292</td>
</tr>
</tbody>
</table>
### Integrating Authentication and Authorization Technologies

**Course | 22 minutes**

Review and update your knowledge of integrating authentication and authorization technologies with this course covering advanced identity management and more.

**NICE Knowledge and Skill Statements:**
K0004, K0007, K0056, K0065, K0092

### Implementing Cryptographic Techniques

**Course | 30 minutes**

Brush up on your understanding of implementing cryptographic techniques with this course covering cryptographic design, techniques and implementations.

**NICE Knowledge and Skill Statements:**
K0004, K0018, K0019, K0025, K0104, K0201, K0277, K0285, K0305, K0308, K0403, K0427, K0428

### Securing Communications and Collaboration Solutions

**Course | 14 minutes**

Secure your communications and collaboration solutions with this course covering BYOD, mobile device management and more.

**NICE Knowledge and Skill Statements:**
K0136, K0445, K0446

### Asset Security

**Course | 39 minutes**

Learn how to secure sensitive data, including managing and classifying data, working with data at rest and in transit, and implementing data security controls.

**NICE Knowledge and Skill Statements:**
K0049, K0065, K0083, K0195, K0287, K0377, K0622

### Risk Mitigation Strategies and Controls

**Course | 26 minutes**

Dive into risk mitigation strategies and controls with this course on risk scenarios, responses and more.

**NICE Knowledge and Skill Statements:**
K0002, K0004, K0048, K0148, K0165, K0169, K0194, K0267, K0527, K0556

### Business and Industry Influences and Risks

**Course | 15 minutes**

Brush up on your knowledge of business and industry influences and risks with this course on enterprise risk management (ERM) and business models.

**NICE Knowledge and Skill Statements:**
K0002, K0146, K0527

### Security Assessment

**Course | 20 minutes**

Discover any weak spots in your cyber defense. Learn how to use security assessments to identify, analyze and report on an organization’s cyber risk.

**NICE Knowledge and Skill Statements:**
K0002, K0013, K0028, K0037, K0048, K0091, K0165, K0177, K0214, K0342

### Access Control Fundamentals

**Course | 1 hour 37 minutes**

Take a deep dive into one of the fundamental concepts of security: access control. Learn how to give the right people access to the right information in a secure way.

**NICE Knowledge and Skill Statements:**
K0007, K0033, K0056, K0065, K0071, K0104, K0158, K0179, K0211, K0332, K0336, K0452, K0488, S0023, S0031

### Secure Network Design

**Course | 26 minutes**

Explore key concepts behind secure network design, including tools to keep threats out and techniques to detect and deflect intruders that breach your defenses.

**NICE Knowledge and Skill Statements:**
K0001, K0004, K0034, K0049, K0179, K0276, K0291, K0324, K0326, K0452, K0487, K0488, K0493, K0561, S0023, S0034
**WAN & Remote Access Security**

Course | 33 minutes

Learn about securing wide area networks (WAN) and remote access against different types of cyber threats in this five-video course.

**NICE Knowledge and Skill Statements:**
K0001, K0005, K0070, K0071, K0104, K0113, K0138, K0190, K0265, K0274, K0362, K0395, K0417, K0427, K0438

---

**Network Fundamentals**

Course | 1 hour 20 minutes

Go in-depth into networking devices and technologies. Explore network types, protocols, models, attacks, security and more.

**NICE Knowledge and Skill Statements:**
K0001, K0034, K0050, K0057, K0061, K0093, K0136, K0159, K0170, K0221, K0265, K0274, K0303, K0332, K0333, K0395, K0417, K0437, K0452, K0470, K0471, K0489, K0516, K0565, K0612, S0236
Cybersecurity Audit Fundamentals

The Cybersecurity Audit Learning Path helps you get to grips with the controls implemented by the organization to reduce the risk to confidentiality, integrity and availability down to an acceptable level.

- **Skill Assessment**
  - Course | 20 questions
  - See how your cybersecurity audit fundamentals skills stack up against other professionals in your field.

- **Audit's Role in Cybersecurity**
  - Course | 33 minutes
  - Understand your role as an auditor in cybersecurity by understanding defense-in-depth and digital asset protection.
  - **NICE Knowledge and Skill Statements:**
    - K0004, K0005, K0006, K0043, K0126, K0200, K0270, K0412, S0085, S0192

- **Governance of Cybersecurity**
  - Course | 1 hour 23 minutes
  - Understand governance's role in cybersecurity by understanding how cybersecurity is framed, organized and managed.
  - **NICE Knowledge and Skill Statements:**
    - K0005, K0065, K0127, K0233, K0242, K0270, K0432, K0504, K0579, S0192

- **Cybersecurity Operations**
  - Course | 2 hours 24 minutes
  - Understand your role as an auditor in reviewing the cybersecurity controls used by the organization to protect the CIA of systems and data.
  - **NICE Knowledge and Skill Statements:**
    - K0005, K0006, K0018, K0019, K0021, K0026, K0032, K0042, K0074, K0151, K0201, K0202, K0292, K0308, K0317, K0362, K0427, K0480, K0612, S0089, S0167, S0206

- **Cybersecurity Technology Topics**
  - Course | 1 hour 24 minutes
  - Understand your role as an auditor in helping to define risk and controls related to specific information technologies and how they affect protection of assets.
  - **NICE Knowledge and Skill Statements:**
    - K0005, K0049, K0070, K0137, K0145, K0269, K0283, K0310, K0435, K0437, K0438, K0487, K0561, K0609, K0610, K0624, S0073, S0173
Cybersecurity Leadership and Management

This learning path will introduce you to cybersecurity leadership and management. Drawing on industry standards, frameworks and models, you will explore the key objective elements of cybersecurity leadership.

**Cybersecurity Leadership and Management Skill Assessment**

Practice Exam | 30 questions

See how your cybersecurity leadership and management skills stack up against other professionals in your field.

**Cybersecurity leadership - Information security governance (ISG) overview**

Course | 56 minutes

An introduction to the basic principles of cybersecurity leadership and management.

**NICE Knowledge and Skill Statements:**

K0005, K0072, K0121, K0248, K0477, K0506, K0518, S0018, S0216, S0273, S0309, S0323, S0359

**Cybersecurity senior management and information security governance (ISG)**

Course | 1 hour 16 minutes

Exploring the roles and responsibilities of senior management in information security.

**NICE Knowledge and Skill Statements:**

K0005, K0072, K0121, K0248, K0477, K0506, K0518, S0018, S0216, S0273, S0309, S0323, S0359

**Aligning information security to the business model**

Course | 1 hour 52 minutes

In this course, you’ll explore aligning information security to the business model.

**NICE Knowledge and Skill Statements:**

K0005, K0072, K0121, K0248, K0477, K0506, K0518, S0018, S0216, S0273, S0309, S0323, S0359

**Information communication reporting in the organization**

Course | 1 hour 23 minutes

In this course, learners will shift the focus from leadership to management and explore cybersecurity information reporting in the organization.

**NICE Knowledge and Skill Statements:**

K0005, K0072, K0121, K0248, K0477, K0506, S0018, S0216, S0273, S0309, S0323, S0359

**Actionable measured KPI and goals**

Course | 1 hour 21 minutes

In this course, the learner will explore key risk indicators and key performance indicators in cybersecurity.

**NICE Knowledge and Skill Statements:**

K0005, K0072, K0121, K0248, K0477, K0506, K0518, S0018, S0216, S0273, S0309, S0323, S0359
Cybersecurity responsibilities into information security programs

Course | 1 hour 33 minutes

For this final course, the learner will explore designing and incorporating cybersecurity within the organization's security programs.

NICE Knowledge and Skill Statements:
K0072, K0121, K0350, K0506, K0512, K0582, K0598
Cybersecurity Management

The Cybersecurity Management skill path teaches you governance and risk management related to cybersecurity. You’ll learn about developing and managing a security program, enterprise security operations, incident management, compliance and more.

Security & Privacy Policies and Procedures

Course | 24 minutes

This course helps you refresh your knowledge of security and privacy policies and procedures.

NICE Knowledge and Skill Statements:
K0002, K0003, K0004, K0026, K0048, K0101, K0199, K0260, K0261, K0262, K0267, K0527

IR, BC and DR Planning and Procedures

Course | 28 minutes

The fundamentals of incident response, business continuity and disaster recovery are explored in six videos.

NICE Knowledge and Skill Statements:
K0026, K0041, K0042, K0146, K0150, K0231, K0292, K0381, K0399

Effective Incident Management

Course | 25 minutes

Review effective incident management with eight videos on metrics, response procedures and more.

NICE Knowledge and Skill Statements:
K0042, K0150, K0292, K0381

Controls, Metrics and Monitoring

Course | 17 minutes

Take a closer look at what tools you have with this course on controls, metrics and monitoring for security managers.

NICE Knowledge and Skill Statements:
K0002, K0007, K0065, K0622

Security Program Activities

Course | 19 minutes

Explore security program activities with two videos on business case development, program development, documentation and more.

NICE Knowledge and Skill Statements:
K0002, K0006, K0065, K0121, K0154, K0165, K0230, K0263, K0264, K0317, K0381, K0579

Incident Response and Recovery Procedures

Course | 16 minutes

Prepare for possible trouble with this course on incident response and recovery procedures, including designing systems to facilitate incident response.

NICE Knowledge and Skill Statements:
K0021, K0026, K0041, K0042, K0118, K0125, K0128, K0132, K0133, K0150, K0292
<table>
<thead>
<tr>
<th>Table of contents</th>
<th>Boot camps</th>
<th>Self-paced training</th>
<th>Learning paths</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
</table>

## Securing Communications and Collaboration Solutions

**Course | 14 minutes**

Secure your communications and collaboration solutions with this course covering BYOD, mobile device management and more.

**NICE Knowledge and Skill Statements:**
K0136, K0445, K0446

## Security Program Architecture

**Course | 22 minutes**

Information security program architecture is reviewed and dissected in ten videos. Controls, objectives, program elements and more provide a strong foundation for an aspiring security manager.

**NICE Knowledge and Skill Statements:**
K0006, K0047, K0087, K0121

## Vulnerability Assessment Methods and Tools

**Course | 21 minutes**

This course helps you broaden your understanding of vulnerability assessment and tools, including tool lists and test types.

**NICE Knowledge and Skill Statements:**
K0005, K0006, K0013, K0106, K0177, K0301, K0342

## Monitoring and Communication

**Course | 6 minutes**

Enhance your risk management skills with three videos on risk monitoring and communication.

**NICE Knowledge and Skill Statements:**
K0002

## Software Vulnerabilities and Security Controls

**Course | 37 minutes**

In this course, we take you through the fundamentals of software vulnerabilities and security controls.

**NICE Knowledge and Skill Statements:**
K0005, K0049, K0070, K0140, K0624

## Asset Classification and Operational Considerations

**Course | 10 minutes**

Review asset classification and operational considerations in five videos, covering vocabulary, diagrams, key terms and important takeaways.

**NICE Knowledge and Skill Statements:**
K0021, K0090, K0154, K0195, K0211, K0267, K0270, K0287, K0291

## Risk Assessment

**Course | 17 minutes**

Refresh your knowledge of how bad things can get with this course on the four steps of risk assessment: Prepare, Conduct the Assessment, Report and Communicate and Maintain.

**NICE Knowledge and Skill Statements:**
K0002, K0006, K0149, K0165, K0263

## Risk Metric Scenarios

**Course | 12 minutes**

This course on risk metric scenarios covers analyzing scenarios to secure enterprises and reviewing existing security.

**NICE Knowledge and Skill Statements:**
K0002, K0183, K0527

## Risk Mitigation Strategies and Controls

**Course | 26 minutes**

Dive into risk mitigation strategies and controls with this course on risk scenarios, responses and more.

**NICE Knowledge and Skill Statements:**
K0002, K0004, K0048, K0148, K0165, K0169, K0194, K0267, K0527, K0556

---

Security architecture, engineering and management

Use code “learnskills” to get 30 days for $1  
GET STARTED
<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Learning paths</th>
<th>Learning paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Planning</td>
<td>Business and Industry Influences and Risks</td>
<td>Strategy and Implementation</td>
</tr>
<tr>
<td>Course</td>
<td>40 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Review business continuity planning and the challenges of disaster recovery with two videos on business impact analysis, auditing business continuity and more.</td>
<td>Brush up on your knowledge of business and industry influences and risks with this course on enterprise risk management (ERM) and business models.</td>
<td>Take a fresh look at risk management strategy and implementation. Includes vocabulary, phases and tips for effective information risk management.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements: K0006, K0026, K0032, K0041, K0042, K0150, K0165, K0292</td>
<td>NICE Knowledge and Skill Statements: K0002, K0146, K0527</td>
<td>NICE Knowledge and Skill Statements: K0002, K0006, K0165, K0263, K0527</td>
</tr>
<tr>
<td>Implementation Action Plan</td>
<td>IS Resources and Constraints</td>
<td>Information Security Strategy</td>
</tr>
<tr>
<td>Course</td>
<td>11 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Two videos help you review action plan types, action plan implementation strategies and information security program objectives.</td>
<td>Information security resources and constraints are examined in this two-video course covering personnel, organizational structure and more.</td>
<td>Five videos take you through the core tenets of information security strategy, including strategy elements and metrics.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements: K0054, K0121, K0198, K0258, K0501</td>
<td>NICE Knowledge and Skill Statements: K0002, K0007, K0065, K0072, K0199, K0200, K0496, K0501, K0527</td>
<td>NICE Knowledge and Skill Statements: K0002, K0101, K0146, K0293, K0432</td>
</tr>
<tr>
<td>IS Roles and Responsibilities</td>
<td>Introduction to IS Governance</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>Course</td>
<td>6 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Refresh your knowledge of information security roles and responsibilities with three videos on key roles and responsibilities, risk management and associated topics.</td>
<td>Three videos provide an introduction to information security governance, including the use of governance and why it is important for an organization.</td>
<td>Don't let a lack of preparedness compound the effects of a disaster. Learn how to create and test a disaster recovery plan in this six-video course.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements: K0579</td>
<td>NICE Knowledge and Skill Statements: K0101</td>
<td>NICE Knowledge and Skill Statements: K0006, K0021, K0026, K0032, K0150, K0210, K0292, K0399, K0519, K0527</td>
</tr>
<tr>
<td>Learning paths</td>
<td>Labs</td>
<td>Projects</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>Preventative &amp; Detective Measures</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Course</strong></td>
<td>39 minutes</td>
<td></td>
</tr>
<tr>
<td>Explore ways to prevent cyber threats from impacting your organization, and learn how to quickly detect the threats that do slip through your defenses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0004, K0006, K0049, K0073, K0074, K0132, K0145, K0167, K0205, K0275, K0480, K0487, K0488, K0561</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Crime Investigations</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Course</strong></td>
<td>32 minutes</td>
<td></td>
</tr>
<tr>
<td>Refresh your knowledge of cybercrime investigations with this overview course covering the investigation process and the discovery of digital evidence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0017, K0118, K0122, K0123, K0125, K0128, K0133, K0155, K0156, K0184, K0222, K0251, K0384, K0433</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control Fundamentals</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Course</strong></td>
<td>1 hour 37 minutes</td>
<td></td>
</tr>
<tr>
<td>Take a deep dive into one of the fundamental concepts of security: access control. Learn how to give the right people access to the right information in a secure way.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0007, K0033, K0056, K0065, K0071, K0104, K0158, K0179, K0211, K0332, K0336, K0452, K0488, S0023, S0031</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Course</strong></td>
<td>39 minutes</td>
<td></td>
</tr>
<tr>
<td>Learn how to secure sensitive data, including managing and classifying data, working with data at rest and in transit, and implementing data security controls.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0049, K0065, K0083, K0195, K0287, K0377, K0622</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Policies</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Course</strong></td>
<td>22 minutes</td>
<td></td>
</tr>
<tr>
<td>Explore security policies and control frameworks and how they help drive the overall security of an organization.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0004, K0006, K0157, K0169, K0215, K0242, K0243, K0264</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Course</strong></td>
<td>49 minutes</td>
<td></td>
</tr>
<tr>
<td>Dive deep into risk management, including risk frameworks, assessments and modeling, as well as employee security awareness, vendor security and other issues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0002, K0005, K0047, K0048, K0162, K0165, K0169, K0214, K0295, K0455, K0527</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enterprise Security Risk Management

The Enterprise Security Risk Management skill path covers essential enterprise risk topics, including risk identification and assessment, implementing security controls, regulatory compliance, strategy and culture, and more.

### Key Risk Indicators and Key Performance Indicators

**Course** | 49 minutes
---
Learn key risk indicators, key performance indicators, plus monitoring and reporting tools and techniques.

**NICE Knowledge and Skill Statements:**
K0002, K0054, K0145, K0527

---

### Monitoring and Communication

**Course** | 6 minutes
---
Enhance your risk management skills with three videos on risk monitoring and communication.

**NICE Knowledge and Skill Statements:**
K0002

---

### Asset Classification and Operational Considerations

**Course** | 10 minutes
---
Review asset classification and operational considerations in five videos, covering vocabulary, diagrams, key terms and important takeaways.

**NICE Knowledge and Skill Statements:**
K0021, K0090, K0154, K0195, K0211, K0267, K0270, K0287, K0291

---

### Risk Assessment

**Course** | 17 minutes
---
Two videos take you through risk assessment methodologies, vocabulary and examples.

**NICE Knowledge and Skill Statements:**
K0002, K0006, K0149, K0165, K0263

---

### Risk Metric Scenarios

**Course** | 12 minutes
---
This course on risk metric scenarios covers analyzing scenarios to secure enterprises and reviewing existing security.

**NICE Knowledge and Skill Statements:**
K0002, K0183, K0527

---

### Access Control Fundamentals

**Course** | 1 hour 37 minutes
---
Take a deep dive into one of the fundamental concepts of security: access control. Learn how to give the right people access to the right information in a secure way.

**NICE Knowledge and Skill Statements:**
K0007, K0033, K0056, K0065, K0071, K0104, K0158, K0179, K0211, K0332, K0336, K0452, K0488, S0023, S0031
Security Policies

Course | 22 minutes

Explore security policies and control frameworks and how they help drive the overall security of an organization.

NICE Knowledge and Skill Statements:
K0004, K0006, K0157, K0169, K0215, K0242, K0243, K0264

Risk Management

Course | 49 minutes

Dive deep into risk management, including risk frameworks, assessments and modeling, as well as employee security awareness, vendor security and other issues.

NICE Knowledge and Skill Statements:
K0002, K0005, K0047, K0048, K0162, K0165, K0169, K0214, K0295, K0455, K0527

Regulatory Compliance

Course | 30 minutes

Explore the compliance issues related to digital data, including privacy laws, regulations, intellectual property issues and more.

NICE Knowledge and Skill Statements:
K0003, K0004, K0006, K0157, K0196, K0260, K0261, K0262, K0410, K0524, K0615

Security Governance Principles

Course | 16 minutes

Explore security governance and how it relates to business processes and strategies in this brief overview course.

NICE Knowledge and Skill Statements:
K0004, K0006, K0047, K0146, K0261, K0295, K0511, K0579

Risk Mitigation Strategies and Controls

Course | 26 minutes

Dive into risk mitigation strategies and controls with this course on risk scenarios, responses and more.

NICE Knowledge and Skill Statements:
K0002, K0004, K0048, K0148, K0165, K0169

Risk Identification Frameworks and Methods

Course | 39 minutes

Review best practices for IT risk management, including the steps that risk managers need to go through.

NICE Knowledge and Skill Statements:
K0002, K0048, K0165

Control Design and Implementation

Course | 1 hour 4 minutes

Understand the major types of risk controls and their interdependencies.

NICE Knowledge and Skill Statements:
K0002, K0018, K0019, K0048, K0073, K0075, K0201, K0291, K0427, K0488, S0036

Risk Response Options

Course | 43 minutes

Alignment with business objectives is one of the drivers of risk management.

NICE Knowledge and Skill Statements:
K0002, K0005, K0101

Risk-Based Decision Making

Course | 52 minutes

Learn about different business-related and IT management aspects that factor into risk assessment.

NICE Knowledge and Skill Statements:
K0002, K0005, K0021, K0026, K0059, K0072, K0121, K0147, K0165, K0169, K0199, K0335, K0431, K0455
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk and Control Analysis</strong></td>
<td>1 hour 15 min</td>
<td>K0013, K0165, K0342</td>
</tr>
<tr>
<td><strong>Risk Assessment Techniques</strong></td>
<td>33 min</td>
<td>K0002, K0165</td>
</tr>
<tr>
<td><strong>IT Security Risk Concepts</strong></td>
<td>1 hour 45 min</td>
<td>K0002, K0004, K0005, K0007, K0065, K0070, K0106, K0151, K0267, K0342, K0527</td>
</tr>
<tr>
<td><strong>Impact of Compliance</strong></td>
<td>28 min</td>
<td>K0003, K0066, K0168, K0260, K0261, K0262, K0267, K0410, K0615</td>
</tr>
<tr>
<td><strong>IT Risk Strategy</strong></td>
<td>31 min</td>
<td>K0002, K0003, K0101, K0293, S0038</td>
</tr>
<tr>
<td><strong>Risk Culture and Communication</strong></td>
<td>27 min</td>
<td>K0002, K0527, S0070</td>
</tr>
</tbody>
</table>

Know how to use controls, along with incident management, to determine the state of current risk.

Learn how to assess the potential impacts of the various IT risks.

Understand the security risks concepts and principles that impact IT risk practitioners' jobs.

Refresh your awareness about the regulatory and statutory privacy and security requirements and their impact on risk.

Dive deeper into the importance of an IT strategy and how it should align with business goals, objectives and values.

Risk culture, appetite and communication of risk are important in understanding how risk relates to the organization's values, goals and objectives.
Certified SCADA Security Architect (CSSA)

The Certified SCADA Security Architect (CSSA) certification path covers everything from field-based attacks to automated vulnerability assessments for SCADA networks. You'll learn how to defend against both internal and external attackers to provide holistic security for critical industrial automation systems.

Skill Assessment
Skill assessment | 20 questions
See how your CCSA skills stack up against other professionals in your field.

CSSA Practice Exam
Practice Exam | 75 questions
Prepare for your CCSA exam and test your domain knowledge.

SCADA Cyber Range
Cyber range | 15 labs
Gain practical experience and build real-world Supervisory Control and Data Acquisition (SCADA) skills through 15 hands-on labs in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:
S0046, S0051, S0057, S0067, S0081, S0120, S0156, S0158, S0221

Introduction to SCADA Security
Course | 19 minutes
Get an introduction to SCADA security, including ICS types, ICS components, process control and safety systems, and strengths and weaknesses.

NICE Knowledge and Skill Statements:
K0005, K0137, K0170, K0437

ICS Protocols
Course | 1 hour 7 minutes
Explore common Industrial Control System (ICS) protocols and their security features as you progress through this 15-video course.

NICE Knowledge and Skill Statements:
K0005, K0137, K0170, K0417, K0437

SCADA Security Frameworks
Course | 1 hour 7 minutes
This course will begin your reintroduction to SCADA security frameworks, covering common threats to SCADA, relevant security standards and bodies, developing SCADA security policies and more.

NICE Knowledge and Skill Statements:
K0005, K0006, K0065, K0137, K0177, K0267, K0437, K0612
<table>
<thead>
<tr>
<th>Learning path</th>
<th>Course Time</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SCADA Security Assessment</strong></td>
<td>44 minutes</td>
<td>K0002, K0013, K0040, K0165, K0290, K0342, K0437</td>
</tr>
<tr>
<td><strong>SCADA Device Identification and Analysis</strong></td>
<td>43 minutes</td>
<td>K0004, K0137, K0170, K0177, K0274, K0342, K0437, K0536, K0565</td>
</tr>
<tr>
<td><strong>SCADA Vulnerabilities</strong></td>
<td>26 minutes</td>
<td>K0005, K0060, K0071, K0077, K0137, K0170, K0177, K0342, K0437, K0536, K0565</td>
</tr>
<tr>
<td><strong>Pentesting SCADA Services and Protocols</strong></td>
<td>24 minutes</td>
<td>K0005, K0060, K0137, K0170, K0177, K0342, K0437, K0536, K0565</td>
</tr>
<tr>
<td><strong>SCADA Access Controls</strong></td>
<td>31 minutes</td>
<td>K0007, K0033, K0056, K0065, K0137, K0170, K0437</td>
</tr>
<tr>
<td><strong>Remote Access and Field Site Security</strong></td>
<td>36 minutes</td>
<td>K0071, K0104, K0137, K0190, K0427, K0437, K0561</td>
</tr>
<tr>
<td><strong>SCADA Network Security</strong></td>
<td>39 minutes</td>
<td>K0033, K0049, K0137, K0145, K0179, K0437, K0561, K0565</td>
</tr>
<tr>
<td><strong>SCADA Intrusion Detection and Incident Response</strong></td>
<td>61 minutes</td>
<td>K0004, K0041, K0042, K0046, K0137, K0324, K0437</td>
</tr>
<tr>
<td><strong>SCADA Preventative Controls</strong></td>
<td>47 minutes</td>
<td>K0033, K0049, K0074, K0162, K0205, K0324, K0437, K0480</td>
</tr>
</tbody>
</table>
ICS/SCADA Security Best Practices

Course | 26 minutes

Learn about the three aspects of SCADA security best practices: prevention, detection and correction.

NICE Knowledge and Skill Statements:
K0004K0005, K0073, K0437, K0527

CSSA Exam Overview

Course | 4 minutes

This course will give you an overview of the Certified SCADA Security Architect (CSSA) exam and what to expect.

NICE Knowledge and Skill Statements:
NONE
In this learning path, you will explore the details of the IAPP CIPP/E subject matter and learn more about privacy law, the rights of individuals and the common body of knowledge.

**CIPP/E Practice Exam**

Practice Exam | 35 questions
Prepare for your CISA exam and test your domain knowledge.

**Origins and Historical Context of Data Protection Law**

Course | 36 minutes
A discussion of privacy versus data protection and different approaches around the world.

**European Union Institutions**

Course | 42 minutes
A discussion on the differences between the Council of Europe and the EU.

**EU Legislative Framework**

Course | 35 minutes
The timeline of data protection law and the extent of GDPR application.

**Data Protection Concepts and Scope**

Course | 44 minutes
A discussion on types of personal data and further definitions of roles assigned by the GDPR.

**Data Processing Principles**

Course | 39 minutes
A discussion of the application of the privacy principles and their role in data protection law.
<table>
<thead>
<tr>
<th>Security architecture, engineering and management</th>
</tr>
</thead>
</table>

### Lawful Processing Criteria

Course | 43 minutes
A discussion on how to process data with lawful reasoning.

**NICE Knowledge and Skill Statements:**
K0003, K0004, K0044, K0222, K0260, K0261, K0262, K0504, K0524

### Transparency and Data Subject's Rights

Course | 55 minutes
A discussion on the rights of the data subjects under the GDPR.

**NICE Knowledge and Skill Statements:**
K0003, K0004, K0044, K0260, K0261, K0262, S0147

### Obligations of Controllers and Processors

Course | 51 minutes
A discussion of controllers and processor obligations under the GDPR.

**NICE Knowledge and Skill Statements:**
K0003, K0004, K0044, K0260, K0261, K0262, S0147

### Security and Data Breaches

Course | 37 minutes
Exploring security and data breaches, and what the law requires.

**NICE Knowledge and Skill Statements:**
K0003, K0004, K0005, K0044, K0168, K0222, K0260, K0261, K0262, S0147

### International Data Transfer

Course | 45 minutes
Exploring international data transfer and its challenges.

**NICE Knowledge and Skill Statements:**
K0003, K0004, K0044, K0168, K0222, K0260, K0261, K0262, K0411

### Powers of the Regulator

Course | 26 minutes
A discussion on the roles of the regulators and their enforcement powers.

**NICE Knowledge and Skill Statements:**
K0003, K0004, K0044, K0260, K0261, K0262, K0411

### Application of the Law

Course | 38 minutes
The GDPR and its interactions with different laws.

**NICE Knowledge and Skill Statements:**
K0003, K0004, K0044, K0168, K0222, K0260, K0261, K0262, K0411
ICS/SCADA Security Analyst

The ICS/SCADA Security Analyst skill path provides you with the knowledge needed to defend the systems that control critical infrastructure. You'll learn about assessing the security of industrial control and SCADA systems and protecting them from cyber threats.

ICS/SCADA Pentesting CTF: Lights Out

Cyber range | 1 lab

You are the whitehat. You've become aware of a plot to launch a proof-of-concept cyber-attack against a large sports stadium in which the attackers will take over the facility's power management system and turn out the lights during a Sunday night sporting event.

NICE Knowledge and Skill Statements: S0051, S0078, S0081

SCADA Security Frameworks

Course | 1 hour 6 minutes

This course will begin your reintroduction to SCADA security frameworks, covering common threats to SCADA, relevant security standards and bodies, developing SCADA security policies and more.

NICE Knowledge and Skill Statements: K0005, K0006, K0065, K0137, K0177, K0267, K0437, K0612

SCADA Security Assessment

Course | 44 minutes

Review your understanding of SCADA security assessment with this course covering SCADA security objectives, security assessment programs and more.

NICE Knowledge and Skill Statements: K0002, K0013, K0040, K0165, K0290, K0342, K0437

SCADA Device Identification and Analysis

Course | 43 minutes

Make sure you know what you need to know with this course on SCADA device identification and analysis.

NICE Knowledge and Skill Statements: K0004, K0137, K0170, K0177, K0274, K0342, K0437, K0536, K0565

SCADA Vulnerabilities

Course | 26 minutes

Explore SCADA vulnerabilities with this course covering common vulnerabilities, vulnerability scanning, server OS testing and more.

NICE Knowledge and Skill Statements: K0005, K0060, K0071, K0077, K0137, K0177, K0267, K0437, K0536, K0565

Pentesting SCADA Services and Protocols

Course | 24 minutes

Review what it takes to attack standard services, server OS, ICS protocols and more with this course on pentesting SCADA services and protocols.

NICE Knowledge and Skill Statements: K0005, K0060, K0137, K0170, K0177, K0342, K0437, K0536, K0565
SCADA Access Controls

Course | 31 minutes

In this course, you'll look at the importance of SCADA access controls. Review physical safety, access control models and more.

NICE Knowledge and Skill Statements:
K0007, K0033, K0056, K0065, K0170, K0437

Remote Access and Field Site Security

Course | 36 minutes

Re-familiarize yourself with the challenges of remote access and field site security through this course on remote access technologies, field site firewalls and more.

NICE Knowledge and Skill Statements:
K0071, K0104, K0137, K0190, K0427, K0437, K0561

SCADA Network Security

Course | 39 minutes

In this course, you'll refresh your knowledge of SCADA network security through secure network design, firewalls and logical security zones.

NICE Knowledge and Skill Statements:
K0033, K0049, K0137, K0145, K0179, K0437, K0561, K0565

SCADA Intrusion Detection and Incident Response

Course | 61 minutes

Get to grips with what you need to know for SCADA intrusion detection and incident response.

NICE Knowledge and Skill Statements:
K0004, K0041, K0042, K0046, K0137, K0324, K0437

SCADA Preventative Controls

Course | 46 minutes

Brush up on what you need to prevent or mitigate disasters with this course on SCADA preventative controls.

NICE Knowledge and Skill Statements:
K0033, K0049, K0074, K0162, K0205, K0324, K0437, K0480
Implementing Controls for HIPAA Compliance

This path will help students and professionals understand how to maintain the confidentiality, integrity and availability of PHI and ePHI. You'll get to grips with protecting ePHI from unauthorized use and disclosure, and the importance of helping employees stay compliant with the rules.

### Skill Assessment

**Skill assessment | 20 questions**

See how your HIPAA compliance skills stack up against other professionals in your field.

### Privacy and Security in Health Care and Public Health

**Course | 25 minutes**

This course explores the nature and purpose of HIPAA. Beginning with why HIPAA is important, explore the advantages of HIPAA implementation and the importance of its role.

**NICE Knowledge and Skill Statements:**

K0003, K0004, K0044, K0260, K0262

### HIPAA Data Privacy and Data Regulation

**Course | 1 hour 26 minutes**

In this course, we explore helpful suggestions on how HIPAA businesses should comply not only to HIPAA regulations but also to be more familiar with the state laws within their jurisdiction.

**NICE Knowledge and Skill Statements:**

K0003, K0044, K0222, K0262

### How to Conduct Assessments

**Course | 1 hour 9 minutes**

In this course, you'll dig deeper into the how and why of assessments, as well as different assessment types. You'll learn how assessments are important to understand where you're at within the HIPAA compliance meter.

**NICE Knowledge and Skill Statements:**

K0003, K0044, K0066, K0222, K0262

### Key Principles of Security – NIST Standards

**Course | 53 minutes**

In this course, you'll dive deeper into the details of NIST. Explore what NIST is, its families and security controls, and look at an introductory resource guide for implementing the HIPAA security rule.

**NICE Knowledge and Skill Statements:**

K0003, K0025, K0044, K0195, K0222, K0260, K0262, S0374

### HIPAA Training and Awareness

**Course | 26 minutes**

HIPAA requires covered entities to conduct training. But do you know what areas to cover? How often you must conduct your training? This course will help you get your HIPAA training off the ground and maintain it.

**NICE Knowledge and Skill Statements:**

K0003, K0243, K0245, K0262, K0512
Health Care Data Breaches

Course | 29 minutes

This course will help you understand the main differences between an incident and a breach. You'll take a look at why breaches and incidents are important, and why the difference between them matters.

NICE Knowledge and Skill Statements:
K0003, K0044, K0260, K0262, K0287

HIPAA Compliance Checklist

Course | 26 minutes

Now that we have learned HIPAA and understand the importance of implementing HIPAA controls, where do we start? Take a look at building a culture of compliance, data hygiene and the importance of mobile device security.

NICE Knowledge and Skill Statements:
K0003, K0044, K0222, K0260, K0262
Introduction to Applied Cryptography and Cryptanalysis

This learning path introduces cryptography, its applications, and methods for decrypting and deobfuscating data. The fundamentals of cryptography are introduced as well as common applications of cryptography. The path also introduces weak algorithms used by malware, how to identify them and methods for deobfuscating the data.

Skill Assessment
Skill assessment | 20 questions
See how your applied cryptography and cryptanalysis skills stack up against other professionals in your field.

Cryptography and Cryptanalysis Project
Project | 2 hours 10 minutes
Practice your cryptography skills by solving challenges.

NICE Knowledge and Skill Statements:
S0089, S0199, S0221, S0258

Introduction to Cryptography
Course | 25 minutes
This course defines the basic vocabulary and concepts of cryptography.

NICE Knowledge and Skill Statements:
K0308, K0412, K0427

Fundamentals of Cryptography
Course | 20 minutes
This course describes mathematics and structures commonly used in cryptography.

NICE Knowledge and Skill Statements:
K0005, K0018, K0019, K0308, K0403, K0412, K0427

Symmetric Cryptography
Course | 45 minutes
This course provides an introduction to symmetric encryption algorithms.

NICE Knowledge and Skill Statements:
K0427, K0018, K0019, K0201, K0403

Asymmetric Cryptography
Course | 36 minutes
This course provides an introduction to asymmetric encryption algorithms.

NICE Knowledge and Skill Statements:
K0005, K0018, K0019, K0403, K0427
<table>
<thead>
<tr>
<th>Topic</th>
<th>Course Time</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Functions</td>
<td>17 minutes</td>
<td>K0018, K0427, S0089, S0298</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI)</td>
<td>18 minutes</td>
<td>K0004, K0019, K0056, K0427</td>
</tr>
<tr>
<td>SSL and TLS</td>
<td>26 minutes</td>
<td>K0005, K0018, K0308, K0427, K0603</td>
</tr>
<tr>
<td>Virtual Private Networks (VPNs)</td>
<td>18 minutes</td>
<td>K0004, K0005, K0071, K0104, K0427, K0428, S0059</td>
</tr>
<tr>
<td>Secure Credential Management</td>
<td>26 minutes</td>
<td>K0005, K0007, K0158, K0336, K0427</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>10 minutes</td>
<td>K0005, K0622</td>
</tr>
<tr>
<td>Blockchain Technology</td>
<td>25 minutes</td>
<td>K0038, K0059, K0622</td>
</tr>
<tr>
<td>Introduction to Cryptanalysis</td>
<td>36 minutes</td>
<td>K0305, K0403, K0427</td>
</tr>
<tr>
<td>Applied Cryptanalysis</td>
<td>25 minutes</td>
<td>K0005, K0305, K0403, K0427</td>
</tr>
</tbody>
</table>
ISACA Certified Information Systems Auditor (CISA)

The Certified Information Systems Auditor (CISA) certification path builds your knowledge of auditing information systems. You'll learn the tools and guidelines involved in the IT auditing process as well as concepts such as business continuity, enterprise IT governance, common security controls and more.

<table>
<thead>
<tr>
<th>Certification Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Assessment</td>
<td>See how your CISA skills stack up against other professionals in your field.</td>
</tr>
<tr>
<td>CISA Practice Exam</td>
<td>Prepare for your CISA exam and test your domain knowledge.</td>
</tr>
<tr>
<td>CISA Introduction</td>
<td>Introduce yourself to CISA with this course introduction covering study plans, CISA stats and details, and more.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Learning Paths</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS Audit Functions</td>
<td>Explore the functions of an information security audit with this course looking at auditor practices, IS audit purposes and more.</td>
</tr>
<tr>
<td>Business Process Applications and Controls</td>
<td>Explore the Business Process section and the controls you'll need to understand during your CISA study.</td>
</tr>
<tr>
<td>Types of Controls and Risk Assessments</td>
<td>Explore the types of controls and risk assessments in four parts, beginning with Control Objectives and Control Measures.</td>
</tr>
</tbody>
</table>

---

**NICE Knowledge and Skill Statements:**

- **IS Audit Functions:** K0003, K0004, K0044, K0047, K0264
- **Business Process Applications and Controls:** K0003, K0004, K0005, K0044, K0047, K0146, K0263, K0264, S0085
- **Types of Controls and Risk Assessments:** K0002, K0004, K0005, K0044, K0047, K0065, K0264, S0034, S0085, S0147, S0171
Continuous Auditing
Course | 39 minutes
In this course, you'll look at the five parts of the Audit Project Management section, as well as sampling, audit report objectives and more.

NICE Knowledge and Skill Statements:
K0002, K0005, K0047, K0121, K0432, S0085

Governance and Management of IT
Course | 39 minutes
Dig deep into the details of governance and management of IT.

NICE Knowledge and Skill Statements:
K0002, K0027, K0044, K0146, K0154, K0198, K0429, K0591, K0504, S0085

IT Organizational Structure
Course | 32 minutes
Explore IT organizational structure and the critical associated concepts.

NICE Knowledge and Skill Statements:
K0002, K0004, K0027, K0044, K0047, K0267, K0429, K0598, S0085

IT Management
Course | 39 minutes
In this course, you'll review the details of IT management and more.

NICE Knowledge and Skill Statements:
K0004, K0027, K0044, K0053, K0101, K0154, K0198, K0257, K0265, K0267, K0270, K0429, S0085

Information Systems Acquisition
Course | 32 minutes
Take a closer look at the first part of the Information Systems Acquisition and Development subdomain.

NICE Knowledge and Skill Statements:
K0090, K0101, K0121, K0154, K0257, K0270, S0085, S0273

Business Cases and Development
Course | 1 hour 4 minutes
Take some time to explore the second part of Information Systems Acquisition and Development.

NICE Knowledge and Skill Statements:
K0004, K0044, K0080, K0081, K0121, K0140, K0183, K0267, K0429, K0622, S0085, S0273

Information Systems Implementation
Course | 42 minutes
Wrap up Domain 3 of CISA with this course covering Control Identification and Design and Information Systems Implementation.

NICE Knowledge and Skill Statements:
K0004, K0044, K0074, K0091, K0178, K0267, K0275, K0290, K0531, K0622, S0085, S0273

Information Systems Operations
Course | 1 hour 18 minutes
Dive into Part A of CISA Domain 4 in this course covering Common Technology Components and more.

NICE Knowledge and Skill Statements:
K0002, K0074, K0109, K0275, K0317, K0361, K0419, K0589, K0622, S0085, S0273

Business Resilience
Course | 23 minutes

NICE Knowledge and Skill Statements:
K0021, K0026, K0032, K0210, S0027, S0085, S0273
### Business Continuity

**Course | 40 minutes**

Wrap up Part B of Domain 4 with this course on business continuity.

**NICE Knowledge and Skill Statements:**
K0021, K0026, K0210, S0027, S0032, S0085, S0273

### Asset Security Frameworks, Standards and Guidelines

**Course | 41 minutes**

In this course, you'll start on CISA Domain 5 by covering Information Asset Security and Control topics.

**NICE Knowledge and Skill Statements:**
K0005, K0007, K0261, K0262, K0263, K0622, S0085

### Identity and Access Management

**Course | 1 hour 6 minutes**

Continue with Domain 5, Part A of CISA in this course covering identification and authentication topics.

**NICE Knowledge and Skill Statements:**
K0004, K0007, K0056, K0065, S0085

### Network Infrastructure Security

**Course | 52 minutes**

Network infrastructure security has no secrets in this three-video course. Covers structure, auditing and more.

**NICE Knowledge and Skill Statements:**
K0004, K0005, K0010, K0044, K0061, K0108, K0113, K0221, K0262, K0417, K0556, K0560, K0561, K0600, S0085, S0192

### Asset Security

**Course | 51 minutes**

Wrap up part A of CISA Domain 5 with this course covering asset security topics.

**NICE Knowledge and Skill Statements:**
K0004, K0005, K0018, K0019, K0044, K0065, K0113, K0136, K0150, K0190, K0195, K0230, K0287, K0322, K0427, K0609, K0622, S0085

### Security Event Management

**Course | 42 minutes**

Explore Part B of CISA Domain 5 with this course on security event management.

**NICE Knowledge and Skill Statements:**
K0003, K0005, K0042, K0118, K0145, K0150, K0215, K0243, K0245, K0290, K0324, K0474, K0503, K0548, K0603, S0085, S0273
ISACA Certified Information Security Manager (CISM)

The Certified Information Security Manager (CISM) certification path is designed for individuals that oversee, design or assess an enterprise’s information security. You’ll learn about information security governance, risk management, program development and incident management.

---

**Skill Assessment**

Skill assessment | 20 questions

See how your CISM skills stack up against other professionals in your field.

---

**CISM Practice Exam**

Practice Exam | 931 questions

Prepare for your CISM exam and test your domain knowledge.

---

**Introduction to IS Governance**

Course | 11 minutes

Three videos provide an introduction to information security governance, including the use of governance and why it is important for an organization.

NICE Knowledge and Skill Statements: K0101

---

**IS Roles and Responsibilities**

Course | 6 minutes

Refresh your knowledge of information security roles and responsibilities with three videos on key roles and responsibilities, risk management and associated topics.

NICE Knowledge and Skill Statements: K0579

---

**Information Security Strategy**

Course | 21 minutes

Five videos take you through the core tenets of information security strategy, including strategy elements and metrics.

NICE Knowledge and Skill Statements: K0002, K0101, K0146, K0293, K0432

---

**IS Resources and Constraints**

Course | 12 minutes

Information security resources and constraints are examined in this two-video course covering personnel, organizational structure and more.

NICE Knowledge and Skill Statements: K0002, K0007, K0065, K0072, K0199, K0200, K0496, K0501, K0527
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation Action Plan</td>
<td>11 minutes</td>
<td>K0054, K0121, K0198, K0258, K0501</td>
</tr>
<tr>
<td>Strategy and Implementation</td>
<td>17 minutes</td>
<td>K0002, K0006, K0165, K0263, K0527</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>17 minutes</td>
<td>K0002, K0006, K0149, K0165, K0263</td>
</tr>
<tr>
<td>Asset Classification and Operational Considerations</td>
<td>10 minutes</td>
<td>K0021, K0090, K0154, K0195, K0211, K0267, K0270, K0287, K0291</td>
</tr>
<tr>
<td>Monitoring and Communication</td>
<td>6 minutes</td>
<td>K0002</td>
</tr>
<tr>
<td>Security Program Architecture</td>
<td>22 minutes</td>
<td>K0006, K0047, K0087, K0121</td>
</tr>
<tr>
<td>Security Program Activities</td>
<td>19 minutes</td>
<td>K0002, K0006, K0065, K0121, K0154, K0165, K0230, K0263, K0264, K0317, K0381, K0579</td>
</tr>
<tr>
<td>Controls, Metrics and Monitoring</td>
<td>17 minutes</td>
<td>K0002, K0007, K0065, K0622</td>
</tr>
<tr>
<td>Effective Incident Management</td>
<td>25 minutes</td>
<td>K0042, K0150, K0292, K0381</td>
</tr>
</tbody>
</table>

Two videos help you review action plan types, action plan implementation strategies and information security program objectives.

Take a fresh look at risk management strategy and implementation. Includes vocabulary, phases and tips for effective information risk management.

Two videos take you through risk assessment methodologies, vocabulary and examples.

Enhance your risk management skills with three videos on risk monitoring and communication.

Information security program architecture is reviewed and dissected in ten videos. Controls, objectives, program elements and more provide a strong foundation for an aspiring security manager.

Explore security program activities with two videos on business case development, program development, documentation and more.

Take a closer look at what tools you have with this course on controls, metrics and monitoring for security managers.

Review effective incident management with eight videos on metrics, response procedures and more.
IR, BC and DR Planning and Procedures

Course | 28 minutes

The fundamentals of incident response, business continuity and disaster recovery are explored in six videos.

NICE Knowledge and Skill Statements:
K0026, K0041, K0042, K0146, K0150, K0231, K0292, K0381, K0399
ISACA Certified in Risk and Information Systems Control

The Certified in Risk and Information Systems Control (CRISC) certification path teaches you how to design, implement, monitor and maintain risk-based, efficient and effective IS controls.

**CERTIFICATION PATH**

- **Skill Assessment**
  - Skill assessment | 20 questions
  - See how your CRISC skills stack up against other professionals in your field.

- **CRISC Practice Exam**
  - Practice Exam | 156 questions
  - Prepare for your CRISC exam and test your domain knowledge.

- **Risk Identification Overview**
  - Course | 59 minutes
  - Understand what you’ll need to prepare for the ISACA CRISC certification exam, and learn what to expect on the exam.
  - NICE Knowledge and Skill Statements: NONE

- **Risk Identification Frameworks and Methods**
  - Course | 39 minutes
  - Review best practices for IT risk management, including the steps that risk managers need to go through.
  - NICE Knowledge and Skill Statements: K0002, K0048, K0165

- **Risk Culture and Communication**
  - Course | 27 minutes
  - Risk culture, appetite and communication of risk are important in understanding how risk relates to the organization’s values, goals and objectives.
  - NICE Knowledge and Skill Statements: K0002, K0527, S0070

- **IT Risk Strategy**
  - Course | 31 minutes
  - Dive deeper into the importance of an IT strategy and how it should align with business goals, objectives and values.
  - NICE Knowledge and Skill Statements: K0002, K0003, K0101, K0293, S0038
<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
<th>Description</th>
<th>NICE Knowledge and Skill Statements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact of Compliance</td>
<td>28 minutes</td>
<td>Refresh your awareness about the regulatory and statutory privacy and security requirements and their impact on risk.</td>
<td>K0003, K0066, K0168, K0260, K0261, K0262, K0267, K0410, K0615</td>
</tr>
<tr>
<td>IT Security Risk Concepts</td>
<td>1 hour 45 minutes</td>
<td>Understand the security risks concepts and principles that impact IT risk practitioners' jobs.</td>
<td>K0002, K0004, K0005, K0007, K0065, K0070, K0106, K0151, K0267, K0342, K0527</td>
</tr>
<tr>
<td>Risk Assessment Overview</td>
<td>37 minutes</td>
<td>Get an overview of the IT risk assessment aspects that risk practitioners need to know.</td>
<td>K0165</td>
</tr>
<tr>
<td>Risk Assessment Techniques</td>
<td>33 minutes</td>
<td>Learn how to assess the potential impacts of the various IT risks.</td>
<td>K0002, K0165</td>
</tr>
<tr>
<td>Risk and Control Analysis</td>
<td>1 hour 15 minutes</td>
<td>Know how to use controls, along with incident management, to determine the state of current risk.</td>
<td>K0013, K0165, K0342</td>
</tr>
<tr>
<td>Risk-Based Decision Making</td>
<td>52 minutes</td>
<td>Learn about different business-related and IT management aspects that factor into risk assessment.</td>
<td>K0002, K0005, K0021, K0026, K0059, K0072, K0121, K0147, K0165, K0169, K0199, K0335, K0431, K0455</td>
</tr>
<tr>
<td>Risk Response and Mitigation Overview</td>
<td>18 minutes</td>
<td>See the learning objectives for CRISC Domain 3, Risk Response and Mitigation.</td>
<td>K0002</td>
</tr>
<tr>
<td>Risk Response Options</td>
<td>43 minutes</td>
<td>Alignment with business objectives is one of the drivers of risk management.</td>
<td>K0002, K0005, K0101</td>
</tr>
<tr>
<td>Control Design and Implementation</td>
<td>1 hour 4 minutes</td>
<td>Understand the major types of risk controls and their interdependencies.</td>
<td>K0002, K0018, K0019, K0048, K0073, K0075, K0201, K0291, K0427, K0488, S0036</td>
</tr>
</tbody>
</table>
Risk and Control Monitoring and Reporting Overview

Course | 15 minutes

Gain the knowledge you need for monitoring and reporting risks.

NICE Knowledge and Skill Statements:
K0002

Key Risk Indicators and Key Performance Indicators

Course | 49 minutes

Learn key risk indicators, key performance indicators, plus monitoring and reporting tools and techniques.

NICE Knowledge and Skill Statements:
K0002, K0054, K0145, K0527
ITIL 4 Foundation

The ITIL® 4 Foundations certification path teaches you best practices for aligning IT services with business goals. You’ll learn about the ITIL framework, the four dimensions of service management, best practices for implementing ITIL and more.

Skill Assessment
Skill assessment | 20 questions
See how your ITIL 4 Foundation skills stack up against other professionals in your field.

ITIL 4 Foundation Practice Exam
Practice Exam | 80 questions
Prepare for your ITIL 4 Foundation exam and test your domain knowledge.

ITIL 4 Foundation Introduction
Course | 15 minutes
Learn about the role of the ITIL framework in managing IT service in the era of the 4th industrial revolution.

Service Management
Course | 1 hour 1 minute
Understand the service management definitions and concepts that apply to ITIL as well as other frameworks.

NICE Knowledge and Skill Statements:
K0200, K0291, K0293, S0005, S0122

Four Dimensions of Service Management
Course | 39 minutes
Take a closer look at how the model based on the four dimensions of IT service management applies within ITIL.

NICE Knowledge and Skill Statements:
K0200, K0291, K0293, S0005, S0122

Service Value System
Course | 10 minutes
Get an overview of the service value system and how the organization's systems and components work together to enable value co-creation.

NICE Knowledge and Skill Statements:
K0200, K0291, K0293, S0005, S0122
<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
<tbody>
<tr>
<td>NICE mapping</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security architecture, engineering and management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Guiding Principles**

Course | 43 minutes
Discover the seven guiding principles organizations should consider while adapting ITIL guidance to their needs.

**NICE Knowledge and Skill Statements:**
K0200, K0291, K0293, S0005, S0122

---

**Service Value Chain**

Course | 41 minutes
Get a breakdown of the different activities in the service value chain and how they interconnect.

**NICE Knowledge and Skill Statements:**
K0004, K0200, K0291, K0293, S0005, S0122, S0296

---

**Continual Improvement**

Course | 23 minutes
Learn about the continual improvement model, its purpose and its place within the service value chain and the service value system.

**NICE Knowledge and Skill Statements:**
K0200, K0291, K0293, S0005, S0122

---

**Categories of Practices**

Course | 37 minutes
Become aware of the 34 practices that support value chain activities within the ITIL framework.

**NICE Knowledge and Skill Statements:**
K0200, K0291, K0293, S0005, S0122

---

**Service Management Practices**

Course | 1 hour
Dive into the ITIL service management practices category, which includes 17 practices developed over 20-30 years.

**NICE Knowledge and Skill Statements:**
K0200, K0291, K0293, S0005, S0122

---

**Technical Management Practices**

Course | 3 minutes
Review the three ITIL technical management practices that have been adapted from technology management domains.

**NICE Knowledge and Skill Statements:**
K0200, K0291, K0293, S0005, S0122

---

**ITIL 4 Foundation Conclusion**

Course | 10 minutes
Wrap up your knowledge of ITIL foundations by putting together everything you've learned.

**NICE Knowledge and Skill Statements:**
K0200
JNCIA-Junos

CERTIFICATION PATH

This learning path covers all exam topics for the Juniper JN0-103 exam required for the JNCIA-Junos certification. This is the recently updated exam, superseding the JN0-102.

Skill Assessment
Skill assessment | 20 questions
See how your JNCIA-Junos skills stack up against other professionals in your field.

CASP+ Practice Exam
Practice Exam | 65 questions
Prepare for your JNCIA-Junos exam and test your domain knowledge.

Junos OS Fundamentals
Course | 27 minutes
Refresh your knowledge of Juniper Networks software and device architecture with this course.

User Interfaces
Course | 1 hour 43 minutes
Go from command-line zero to hero! In this course, we’ll be covering the user interfaces and configuration concepts.

Configuration Basics
Course | 1 hour 53 minutes
Just pulled your router out of the box? Use what you learn in this course to get it into production right away.

Operational Monitoring and Maintenance
Course | 1 hour 20 minutes
Learn how to perform NetOps functions on Juniper devices and get your feet wet in troubleshooting and maintenance.

NICE Knowledge and Skill Statements:
K0060, K0061, K0255

NICE Knowledge and Skill Statements:
K0011, K0061, K0073, K0255, K0275, K0296, K0393, K0452, K0516, S0084, S0158, S0207

NICE Knowledge and Skill Statements:
K0061, K0103, K0294, K0516, S0041, S0142, S0151, S0158
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Fundamentals</td>
<td>1 hour 51 minutes</td>
<td>K001, K0011, K0061, K0221, K0255, K0296, K0395, K0471, K0516, K0565, S0041</td>
</tr>
<tr>
<td>Routing Policy and Firewall Filters</td>
<td>1 hour 20 minutes</td>
<td>K0004, K0005, K0049, K0061, K0255, K0395, K0487, K0516, K0561, K0565, S0076, S0084, S0170, S0207</td>
</tr>
</tbody>
</table>
NIST Cybersecurity Framework

Build a basic understanding of NIST cybersecurity fundamentals, including using the RMF process and identifying, assessing and responding to risk. Additionally, you will learn how to use the framework to assess an organization's cybersecurity risk and the steps to implement or improve a cybersecurity program.

**Skill Assessment**

Skill assessment | 20 questions

See how your NIST Cybersecurity Framework skills stack up against other professionals in your field.

**NIST Cybersecurity Framework Project**

Project | 2 hours 13 minutes

Apply your NIST Cybersecurity Framework knowledge with this practical exercise.

**NIST Cybersecurity Basics**

Course | 43 minutes

This course helps you build a baseline of cybersecurity knowledge.

**Cybersecurity Framework Components**

Course | 24 minutes

This course breaks down the Cybersecurity Framework components into understandable language.

**Risk Management**

Course | 36 minutes

This course describes the Risk Management Framework (RMF), as well as guidelines for applying the RMF to information systems and organizations.

**Cybersecurity Framework Core Functions**

Course | 1 hour 1 minute

This course describes the five Framework Core Functions and includes descriptions of categories, subcategories and informative references.
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybersecurity Framework Self-Assessments</strong></td>
<td>12 minutes</td>
<td>K0044, K0165, S0147</td>
</tr>
<tr>
<td><strong>The 7-Step Cybersecurity Framework Process</strong></td>
<td>8 minutes</td>
<td>K0044, K0264, S0147</td>
</tr>
<tr>
<td><strong>NIST Cybersecurity Framework Summary &amp; Tips</strong></td>
<td>11 minutes</td>
<td>K0044</td>
</tr>
</tbody>
</table>

This course describes the new section on Self-Assessing Cybersecurity Risk and explains how the Framework can be used by organizations to understand and assess their cybersecurity risk.

This course illustrates the steps an organization could use to create a new cybersecurity program or improve an existing program.

Review the NIST Cybersecurity Framework path with this summary and some tips.
This learning path explains the Risk Management Framework (RMF) and its processes and provides guidance for applying the RMF to information systems and organizations.

**Skill Assessment**

Skill assessment | 10 questions

See how your DoD RMF skills stack up against other professionals in your field.

**NIST DoD RMF Project**

Project | 2 hours 17 minutes

Practice your DoD RMF knowledge with this project.

**Legal and Regulatory Organizations**

Course | 32 minutes

This course introduces regulatory organizations which have an impact on the development and execution of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

**Laws, Policies and Regulations**

Course | 13 minutes

In this course, we discuss some of the laws, policies and regulations which mandate the implementation of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

**Integrated Organization Wide Risk Management**

Course | 52 minutes

In this course, we describe the basic concepts associated with managing information system-related security and privacy risk in organizations.

**Risk Management Framework Phases**

Course | 2 hours

In this course, we discuss the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) steps.
Risk Management Framework Review

Course | 5 minutes

This is a recap of the RMF course.

NICE Knowledge and Skill Statements:
K0002, K0048
# PMI Project Management Professional (PMP)

The Project Management Professional (PMP) certification path covers the best practices and principles of project management and prepares you to pass the Project Management Institute's PMP exam. You'll learn how to initiate, plan, execute, monitor and close a project.

## PMP Practice Exam

- **Practice Exam | 1,433 questions**
  - Prepare for your PMP exam and test your domain knowledge.

## PMP Introduction

- **Course | 14 minutes**
  - Introductory course for the PMP education pathway.
  
  **NICE Knowledge and Skill Statements:**
  - K0121

## Project Management Overview

- **Course | 1 hour 40 minutes**
  - Get ready to dive into project management with five videos on projects and project planning.
  
  **NICE Knowledge and Skill Statements:**
  - K0072, K0121, K0249, K0579

## Initiating

- **Course | 30 minutes**
  - Start off right with three videos on the Initiating process group, covering the Develop Project Charter and Identify Stakeholders processes.
  
  **NICE Knowledge and Skill Statements:**
  - K0072, K0084, K0121, K0249, K0579

## Planning I

- **Course | 59 minutes**
  - Six videos begin your dive into the Planning process group, focusing on processes such as Collect Requirements, Define Scope and Plan Scope Management.
  
  **NICE Knowledge and Skill Statements:**
  - K0072, K0084, K0121, K0249, K0506, K0512, K0579

## Planning II

- **Course | 1 hour 26 minutes**
  - The second part of the Planning process group covers the Schedule Management knowledge area, including defining and sequencing activities and schedule development.
  
  **NICE Knowledge and Skill Statements:**
  - K0072, K0084, K0121, K0249, K0506, K0512, K0579
<table>
<thead>
<tr>
<th>Planning III</th>
<th>Planning IV</th>
<th>Executing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>1 hour 16 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>This seven-video course continues our in-depth examination of the Planning process group, including cost estimation, determining budgets and planning communications management.</td>
<td>The final course covering the Planning process group takes you through planning risk management and stakeholder engagement, procurement management and more.</td>
<td>Refresh your knowledge of the Executing process with this course on directing and managing project work, acquiring resources, developing teams and more.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>K0072, K0084, K0121, K0249, K0506, K0512, K0579</td>
<td>K0002, K0072, K0084, K0121, K0233, K0249, K0270, K0376, K0379, K0506, K0512, K0579</td>
<td>K0072, K0084, K0121, K0249, K0506, K0579</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitoring and Controlling</th>
<th>Closing</th>
<th>Preparing for PMP Exam</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>1 hour 38 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Thirteen videos take you through the details of the Monitoring and Controlling process group, including controlling quality, costs, schedule and resources.</td>
<td>Wrap up your project right with this brief course on the Closing process group.</td>
<td>Prepare to become a certified project manager with three videos on ethics, exam preparation and the exam application process.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>K0072, K0084, K0121, K0249, K0506, K0512, K0579</td>
<td>K0072, K0084, K0121, K0249, K0506, K0512, K0579</td>
<td>NONE</td>
</tr>
</tbody>
</table>
The Project Management Professional learning path explores the Project Management Institute’s project management practices.

**PMP Practice Exam (2021)**

Practice Exam | 135 questions
---
Prepare for your PMP exam and test your domain knowledge.

**Creating a high-performing team**

Course | 2 hours 20 minutes
---
In this course, you will explore the importance of creating a high-performing team and the means to do it.

**Starting the project**

Course | 4 hours 14 minutes
---
In this course, students will explore the project start process, including choosing appropriate methodology and planning scope.

**Doing the work**

Course | 1 hour 57 minutes
---
Time to get to work! In this course, you’ll see the beginning of project work and the Process domain.

**Keeping the team on track**

Course | 2 hours 5 minutes
---
In this course, you’ll work to keep the team on track as they execute the project. Explore managing conflict, stakeholder collaboration and promoting team performance.

**Keeping the business in mind**

Course | 1 hour 17 minutes
---
In this course, you’ll explore how internal and external business environments can influence the work of a project.
Security Architecture

The Security Architecture Learning Path enables security practitioners to develop security architectures that are resilient against cyberthreats while enabling and supporting the goals of the business.

---

Skill Assessment

Skill assessment | 20 questions

See how your Threat Modeling skills stack up against other professionals in your field.

---

Security Architecture – The Essentials

Course | 44 minutes

Get an introduction to the essential elements of security architecture and why it is such an important discipline.

NICE Knowledge and Skill Statements:
K0004, K0027, K0047, K0109, K0179, K0199, K0255, K0291, K0293

---

Enterprise Architecture Frameworks

Course | 53 minutes

Learn about aligning business systems with information systems to achieve business goals and enable the business.

NICE Knowledge and Skill Statements:
K0047, K0199

---

Security Architecture Development Process

Course | 37 minutes

In this course, we will introduce a seven-step, business- and risk-driven process to develop security architectures.

NICE Knowledge and Skill Statements:
K0005, K0044, K0165, K0211, K0287, S0367

---

Threat Modeling

Course | 55 minutes

In this course, we examine four popular threat modeling methodologies: Microsoft STRIDE, the Process for Attack Simulation and Threat Analysis, the Operationally Critical Threat Assessment and Vulnerability Evaluation, and Trike.

NICE Knowledge and Skill Statements:
K0177, K0469, K0475, K0612, S0229

---

Designing for security

Course | 38 minutes

In this course, we will introduce students to security design patterns and reference security architectures as reusable solutions to solve reoccurring information security problems.

NICE Knowledge and Skill Statements:
K0075, K0170, K0291, K0297, S0022, S0036, S0122, S0141
Case Study

Course | 55 minutes

Learn to develop a security architecture that enables a remote workforce while maintaining or increasing the security posture of the organization.

NICE Knowledge and Skill Statements:
K0199, K0291, K0474, S0023, S0122

Summary and Conclusion

Course | 14 minutes

In this course, we will summarize everything we've covered in the learning path and provide final words of wisdom for anyone interested in starting or continuing a career as a security architect.

NICE Knowledge and Skill Statements:
K0047
## Security Engineering

The Security Engineering skill path teaches you concepts related to security architecture and engineering, including technical integration of enterprise security, security design and implementation, secure maintenance and disposal, and more.

<table>
<thead>
<tr>
<th>Skill Path</th>
<th>Course Duration</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secure Design Principles</strong></td>
<td>39 minutes</td>
<td>K0037, K0044, K0047, K0075, K0170, K0180, K0198, K0203, K0211, K0240, K0288, K0291, K0320, K0362, K0624</td>
</tr>
</tbody>
</table>

Explore the principles behind secure system design, ranging from security models to certification and accreditation.

| **Secure Network Design** | 26 minutes | K0001, K0004, K0034, K0049, K0179, K0276, K0291, K0324, K0326, K0452, K0487, K0488, K0493, K0561, S0023, S0034 |

Explore key concepts behind secure network design, including tools to keep threats out and techniques to detect and deflect intruders that breach your defenses.

| **Distributed System & Virtualized Networks** | 20 minutes | K0001, K0063, K0071, K0113, K0130, K0179, K0205, K0437, K0610 |

Explore the use of distributed and virtualized systems as well as the security benefits and potential drawbacks involved in their use.

| **WAN & Remote Access Security** | 33 minutes | K0001, K0005, K0070, K0071, K0104, K0113, K0138, K0190, K0269, K0274, K0362, K0395, K0417, K0427, K0438 |

Learn about securing wide area networks (WAN) and remote access against different types of cyber threats in this five-video course.

| **System Protection Mechanisms** | 32 minutes | K0004, K0070, K0077, K0090, K0109, K0199, K0209, K0271, K0302, K0392, K0493, K0624 |

Learn about different system protection mechanisms and common issues such as Web-based vulnerabilities, architecture flaws and more.

| **Physical Security** | 52 minutes | K0065, K0075, K0165, K0244, S0023 |

Don't forget about physical security! Explore how to keep your business secure starting with secure design and construction to physical intrusion detection and more.
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Duration</th>
<th>Content Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Center Security</strong></td>
<td>21 minutes</td>
<td>Don't let an incident at your data center disrupt your organization. Explore ways to keep data centers secure from a variety of threats.</td>
</tr>
<tr>
<td><strong>Secure Software Development</strong></td>
<td>43 minutes</td>
<td>Explore the ins and outs of secure software development as you progress through this nine-video course.</td>
</tr>
<tr>
<td><strong>Disaster Recovery</strong></td>
<td>36 minutes</td>
<td>Don't let a lack of preparedness compound the effects of a disaster. Learn how to create and test a disaster recovery plan in this six-video course.</td>
</tr>
<tr>
<td><strong>Business Continuity Planning</strong></td>
<td>19 minutes</td>
<td>Learn how to keep your business up and running. Explore the importance of continuity planning, incident response planning and impact analysis.</td>
</tr>
<tr>
<td><strong>Network Security Components</strong></td>
<td>44 minutes</td>
<td>In this course, we help you explore the details of network security components: device types, component management and analyzing components and network configurations.</td>
</tr>
<tr>
<td><strong>Securing Host Devices</strong></td>
<td>20 minutes</td>
<td>Explore the challenges of securing host devices with this course on selecting host hardware and software, host hardening and protecting bootloaders.</td>
</tr>
<tr>
<td><strong>Secure Storage Controls</strong></td>
<td>29 minutes</td>
<td>Refresh your knowledge of secure storage controls with this course on storage types, protocols and management.</td>
</tr>
<tr>
<td><strong>Software Vulnerabilities and Security Controls</strong></td>
<td>37 minutes</td>
<td>In this course, we take you through the fundamentals of software vulnerabilities and security controls.</td>
</tr>
<tr>
<td><strong>Security Engineering Principles</strong></td>
<td>22 minutes</td>
<td>Review the security principles that security engineers need to know in order to implement systems.</td>
</tr>
<tr>
<td>Learning paths</td>
<td>Labs</td>
<td>Projects</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
<td>----------</td>
</tr>
</tbody>
</table>

### Risk Management
- **Course | 7 minutes**
- Get a basic understanding or risk management in an organization.

**NICE Knowledge and Skill Statements:**
K0002, K0004, K0214, K0455, K0527

### System Resilience Principles
- **Course | 10 minutes**
- Dive into defense-in-depth and other principles and methods of making your systems resilient.

**NICE Knowledge and Skill Statements:**
K0002, K0004, K0032, K0112, K0179, K0299, K0323, K0527, S0027, S0076

### Vulnerability Management Principles
- **Course | 13 minutes**
- Know why it’s important to manage vulnerabilities, and what the engineer’s role is.

**NICE Knowledge and Skill Statements:**
K0004, K0005, K0013, K0040, K0070, K0106, K0147, K0157, K0187, K0339, K0373, K0392, K0624, S0036, S0078

### Risk Management Process
- **Course | 37 minutes**
- Walk through the security risk management process and learn best practices.

**NICE Knowledge and Skill Statements:**
K0002, K0004, K0047, K0048, K0165, K0214, K0264, K0455, K0527

### Operational Risk Management
- **Course | 30 minutes**
- Understand how today’s complex business environment impacts operational risk and related controls.

**NICE Knowledge and Skill Statements:**
K0004, K0047, K0048, K0084, K0154, K0169, K0214, K0264, K0379, K0455, K0527

### Stakeholder Requirements Definition
- **Course | 14 minutes**
- Review how different stakeholders impact security planning, design and implementation.

**NICE Knowledge and Skill Statements:**
K0004, K0169, K0376, K0379

### Requirements Analysis
- **Course | 7 minutes**
- Discover the process for analyzing requirements before designing security systems.

**NICE Knowledge and Skill Statements:**
K0004, K0028, K0035, K0073, K0086, K0090, K0091, K0102, K0164, K0291, K0475, K0480

### System Security Architecture and Design
- **Course | 12 minutes**
- Review the core components and processes of security architecture and design.

**NICE Knowledge and Skill Statements:**
K0004, K0044, K0047, K0075, K0087, K0170, K0180, K0198, K0199, K0203, K0211, K0240, K0267, K0288, K0291, S0023

### Implementation, Integration and Deployment of System Modifications
- **Course | 5 minutes**
- Learn the basics of system implementation, integration and deployment.

**NICE Knowledge and Skill Statements:**
K0004, K0073, K0082, K0091, K0178, K0179, K0186, K0257, K0270, K0393, K0452, K0488, S0153

---

**Use code “learnskills” to get 30 days for $1**

[GET STARTED]
Verification and Validation of Systems or System Modifications

Course | 10 minutes

Go through the post-deployments steps of ensuring the system is adequately secure.

NICE Knowledge and Skill Statements:
K0004, K0028, K0091, S0110, S0282

Secure Operations

Course | 30 minutes

Understand the basics of maintaining a secure operations strategy.

NICE Knowledge and Skill Statements:
K0004, K0006, K0026, K0041, K0042, K0074, K0086, K0150, K0167, K0292, K0324, K0333, K0403, K0488

Secure Maintenance

Course | 13 minutes

Learn about the three main areas of secure maintenance and related strategies.

NICE Knowledge and Skill Statements:
K0004, K0035, K0074, K0103, K0167, K0294, K0419, S0027

Secure Disposal

Course | 8 minutes

Know how to handle a system at the end of its lifecycle and the key security considerations.

NICE Knowledge and Skill Statements:
K0004, K0090, K0270

Acquisition Process

Course | 15 minutes

Know what's involved in the systems acquisition phase and how to prepare for it.

NICE Knowledge and Skill Statements:
K0004, K0154, K0164, K0169, K0198, K0257, K0264, K0270, K0376, K0379

System Development Methodologies

Course | 3 minutes

Understand the advantages and disadvantages of different development methods.

NICE Knowledge and Skill Statements:
K0004, K0035, K0039, K0047, K0079, K0081, K0082, K0086, K0087, K0153, K0186, K0276

Technical Management Processes

Course | 32 minutes

Dive deep into the technical aspects of managing systems engineering.

NICE Knowledge and Skill Statements:
K0002, K0004, K0005, K0006, K0150, K0233, K0264, K0527, S0358
SIEM Architecture and Process

This learning path introduces you to what SIEM is and how it operates. Next we dive in to learn about the challenges faced with modern distributed enterprise architectures and the reason why time to detection is outrageously long and completely unmanageable without a technology like SIEM.

Skill Assessment
Skill assessment | 20 questions
See how your SIEM skills stack up against other professionals in your field.

SIEM Architecture and Process Project
Project | 1 hour 13 minutes
Test your understanding of SIEM architecture and process in this project consisting of 5 challenges.
NICE Knowledge and Skill Statements:
S0173

What is SIEM
Course | 1 hour 6 minutes
In this course we will introduce what SIEM is, the problems it is designed to help address, and various vendors in the SIEM space. We will also begin setting up our SIEM environment.
NICE Knowledge and Skill Statements:
K0145, S0038, S0173

Architecture
Course | 1 hour 26 minutes
In this course we will discuss the high level components that SIEM utilizes to help store, process and provide structure around our data. We will also overview the SIEM UI we previously installed.
NICE Knowledge and Skill Statements:
K0109, K0145, K0199, K0255, S0173

Data Collection
Course | 55 minutes
In this course we will discuss various methodologies to ingest data into the SIEM. We will also be configuring our systems to ship our first logs into the SIEM.
NICE Knowledge and Skill Statements:
K0131, K0132, K0145, K0448, S0173

Data Processing
Course | 53 minutes
In this course, we discuss various data formats and data structures. We review various methods to organize our data and make the data meaningful. We also use sample log data to view how the system structures various data formats.
NICE Knowledge and Skill Statements:
K0017, K0038, K0145, S0106, S0173, S0252, S0334
<table>
<thead>
<tr>
<th>Learning paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Enrichment</td>
</tr>
<tr>
<td>Course</td>
</tr>
<tr>
<td>In this course we discuss the purpose behind data enrichment and how we map data from various sources to provide contextual information in the SIEM. We also review a real-world example using event data to enrich a malware event.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td>K0145, S0038, S0123, S0173, S0217</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Indexing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
</tr>
<tr>
<td>In this course we briefly touch on various capabilities to store and manage data. This course is designed to give you ideas behind scalability and resiliency and what these capabilities mean when it comes to managing your data.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td>K0145, S0173</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Using Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
</tr>
<tr>
<td>In this course we introduce Use Cases which are a framework designed to take a detection based capability from concept to reality. We then proceed to follow the process for an example Use Case Detection.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td>K0054, K0145, K0299, K0481, S0027, S0173</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIEM Wrap-Up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
</tr>
<tr>
<td>In this course we discuss the key concepts and key takeaways from each of the courses to help solidify your foundational understanding of SIEM.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td>K0145, S0173</td>
</tr>
</tbody>
</table>
Training and Awareness Basics

Go “beyond compliance” to learn about sales and marketing techniques that can take a training and awareness program to the next level: engagement and behavior change. You’ll also learn security basics for soft-skilled professionals new to the security field, as well as how to leverage brain chemistry to be more effective.

<table>
<thead>
<tr>
<th>Training and Awareness Basics Overview</th>
<th>Security Basics</th>
<th>Introduction to Training and Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>5 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Begin at the beginning with this course introducing you to security training and awareness.</td>
<td>Take a look at some fundamental security basics for soft-skill-focused learners.</td>
<td>Take a look at what’s going on in the world of training and awareness, including potential obstacles and concerns.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td>K0146</td>
<td>K0003, K0004, K0005, K0007, K0104, K0145, K0162, K0412, K0480, K0487</td>
<td>K0252, K0313</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sales and Marketing Techniques for Training and Awareness</th>
<th>Creative</th>
<th>Program Execution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>38 minutes</td>
<td>Course</td>
</tr>
<tr>
<td>Delve into the role of sales and marketing in security awareness and training.</td>
<td>Explore possible concerns on the creative side of security programs.</td>
<td>Move from theory to practice with this course on executing a security program.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td>K0243, K0245</td>
<td>K0252</td>
<td>K0243, K0245, K0252</td>
</tr>
</tbody>
</table>
Vulnerability Assessment

The vulnerability assessment learning path guides you through a holistic security assessment approach, where you will develop a well-structured framework for analyzing the security of a system. You will acquire the skills to perform custom vulnerability assessment for any computer system, application or network infrastructure.

Skill Assessment

Skill assessment | 20 questions
See how your vulnerability assessment skills stack up against other professionals in your field.

Vulnerability Assessment Project

Project | 1 hours 14 minutes
Test your vulnerability assessment skills as your progress through seven challenges leveraging free-to-use security tools and services.

NICE Knowledge and Skill Statements:
S0001, S0137, S0174

Vulnerability Management in a Nutshell

Course | 30 minutes
This course covers the basics of vulnerability assessment, including definitions, scope, policy and process.

NICE Knowledge and Skill Statements:
K0006, K0314

Vulnerability Discovery

Course | 1 hour 47 minutes
This course guides you through five different type of security tools for discovering vulnerabilities in various environments.

NICE Knowledge and Skill Statements:
K0013, K0272, K0290, K0339

Vulnerability Classification

Course | 39 minutes
This course covers three main topics: false positives, standardized vulnerabilities, and weakness classification systems and threat-based vulnerability/weakness classification.

NICE Knowledge and Skill Statements:
K0005, K0040, K0402, K0612

Prioritization and Risk Assessment

Course | 1 hour 11 minutes
This course covers how to classify and prioritize vulnerabilities based on real-world criticality measures and how to define the true risk of the vulnerabilities for a specific environment.

NICE Knowledge and Skill Statements:
K0002, K0013, K0054, K0149, K0165, K0344, K0402, K0469, K0475, S0219
<table>
<thead>
<tr>
<th>Vulnerability Assessment Documentation and Maintenance</th>
<th>Remediation and Mitigation</th>
<th>Key Security Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Course</strong></td>
<td>43 minutes</td>
<td><strong>Course</strong></td>
</tr>
<tr>
<td>This course covers how to create comprehensive, clear and easy-to-understand vulnerability assessment documentation, and how to go about keeping the vulnerability findings and scoring current.</td>
<td>In this course, we will cover a wide range of topics about the vulnerability remediation and mitigation process, including the most common remediations and mitigations and strategies for deployment of security measures.</td>
<td>This course covers the top most effective security controls to reduce the overall risk of systems and networks. Recommendation of such controls is a perfect add-on for any vulnerability assessment.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0013, K0054, K0165</td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K002, K0205, K0275, K0440, K0527, K0531</td>
<td><strong>NICE Knowledge and Skill Statements:</strong> K0033, K0049, K0065, K0145, K0324, K0440, K0523, K0561</td>
</tr>
</tbody>
</table>
Secure coding and DevSecOps training helps programmers, developers and security professionals recognize and mitigate vulnerabilities. It covers a variety of common mistakes, how those mistakes can be exploited by cybercriminals, and what can be done to correct them throughout the development life cycle.

CertNexus Certified IoT Security Practitioner

Securing Internet of Things (IoT) systems can be a complicated process. Explore the challenges and complexities of IoT.

CertNexus Certified IoT Security Practitioner Practice Exam

Prepare for your Internet of Things Security Practitioner exam.

Managing IoT Risks

Course | 32 minutes
In this course, you will identify threats to cybersecurity and privacy throughout an IoT system and apply the principles of Security by Design to plan and design a secure IoT system.

NICE Knowledge and Skill Statements:
K0002, K0004, K0322, K0379, K0455, K0471, K0527, S0357

Securing cloud and web interfaces

Course | 1 hour 17 minutes
In this course, you will explore multiple threats and vulnerabilities that affect IoT systems in the web and the cloud.

NICE Knowledge and Skill Statements:
K0004, K0005, K0135, K0160, K0194, K0283, K0349, K0444, K0603, S0073, S0357

Securing data

Course | 1 hour 31 minutes
In this course, you will learn the details of protecting and securing data from unauthorized access.

NICE Knowledge and Skill Statements:
K0004, K0018, K0019, K0104, K0190, K0285, K0308, K0427, K0561, S0089, S0138, S0298

Controlling access to IoT resources

Course | 1 hour 1 minute
In this course, you will explore identifying relevant strategies and implementing security features to control access to IoT resources.

NICE Knowledge and Skill Statements:
K0004, K0007, K0044, K0056, K0065, K0180, K0487, K0561, S0031, S0136, S0171, S0367

Securing IoT networks

Course | 1 hour 19 minutes
In this course, you will explore the complexities of protecting IoT networks.

NICE Knowledge and Skill Statements:
K0004, K0160, K0180, K0322, K0471, K0487, K0561, S0136
Ensuring privacy

Course | 50 minutes

In this course, you will learn more about taking precautions and disposing of sensitive data in IoT systems.

NICE Knowledge and Skill Statements:
K0003, K0004, K0038, K0044, S0367

Managing software and firmware risks

Course | 59 minutes

In this course, you will explore the details of managing software and firmware risks in IoT.

NICE Knowledge and Skill Statements:
K0004, K0079, K0081, K0082, K0152, K0153, K0178, K0186, K0246, K0509, S0034, S0076, S0172

Promoting physical security

Course | 17 minutes

Explore the details of protecting local memory and storage, and protecting devices from shell access over a physical port connection.

NICE Knowledge and Skill Statements:
K0065, K0075, K0165, K0244, S0023
CertNexus CyberSec First Responder

This learning path is designed to assist students in preparing for the CertNexus CyberSec First Responder (Exam CFR-310) certification examination. It provides a comprehensive methodology for individuals responsible for defending the cybersecurity of their organization.

CertNexus CyberSec First Responder Practice Exam

Practice Exam | 41 questions

Prepare for your CertNexus CyberSec First Responder exam.

CyberSec First Responder Introduction

Course | 4 minutes

This course provides a brief overview of CertNexus CyberSec First Responder certification objectives.

Assessing Information Security Risk

Course | 1 hour, 44 minutes

This course teaches how to identify the strategic value of risk management in the context of information assurance, assess risks that affect the organization, translate risk assessment into specific strategies for mitigation, and integrate documentation into risk management.

NICE Knowledge and Skill Statements:

Analyzing the Threat Landscape

Course | 34 minutes

This course teaches how to compare, contrast, and categorize cybersecurity threats and threat profiles and perform ongoing threat landscape research to prepare for incidents.

NICE Knowledge and Skill Statements:
K0004, K0165, K0177, K0233, K0362, K0455, K0469, K0474, K0475, K0480, K0543, K0603, K0607, K0612, S0228, S0229, S0256, S0258, S0340

Analyzing Reconnaissance Threats to Computing and Network Environments

Course | 34 minutes

This course teaches how to implement threat modeling tools and tactics and assess the impacts of reconnaissance and social engineering.

NICE Knowledge and Skill Statements:
K0004, K0058, K0165, K0177, K0334, K0362, K0474, K0475, K0480, K0603, K0612, S0046, S0056, S0156, S0228, S0229, S0256, S0258, S0340

Analyzing Attacks on Computing and Network Environments

Course | 1 hour, 7 minutes

This course teaches how to assess the impact of various attacks, including system hacking attacks, threats to web apps and services, malware, hijacking and impersonation attacks, denial of service incidents, and threats to mobile and cloud infrastructures.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0009, K0058, K0070, K0119, K0165, K0177, K0334, K0362, K0474, K0475, K0480, K0603, K0612, K0624, S0056, S0228, S0229, S0256, S0258, S0340

Secure coding and DevSecOps

Use code “learnskills” to get 30 days for $1
<table>
<thead>
<tr>
<th>Learning paths</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secure coding and DevSecOps</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CertNexus Cyber Secure Coder

Cyber Secure Coder is the ideal learning path for application developers, testers and architects who have previously not had to consider including security in their project. Even students who are new to programming can benefit by instilling security into their thought process before creating their first application.

### CertNexus Cyber Secure Coder Practice Exam

**Practice Exam | 22 questions**

Prepare for your Cyber Secure Coder exam and test your domain knowledge.

### Identifying the Need for Security in Your Software Projects

**Course | 1 hour 59 minutes**

The first step in tackling the problem of software security is to understand the challenges you're up against.

**NICE Knowledge and Skill Statements:**

K0001, K0003, K0005, K0006, K0028, K0044, K0068, K0080, K0082, K0084, K0139, K0178, K0261, K0624

### Handling Vulnerabilities

**Course | 2 hours 3 minutes**

Before you focus on specific vulnerabilities and tactics for dealing with them, there are some general strategies that you can employ to prevent vulnerabilities from creeping into your software.

**NICE Knowledge and Skill Statements:**

K0004, K0044, K0079, K0081, K0084, K0178, S0367

### Designing for Security

**Course | 1 hour 4 minutes**

The process you use to design your software should reflect what is important to you, your customers and other project stakeholders.

**NICE Knowledge and Skill Statements:**

K0005, K0006, K0178, K0624

### Developing Secure Code

**Course | 2 hours 30 minutes**

In this course, you will follow best practices for secure coding, prevent defects that lead to security vulnerabilities common to various platforms, and prevent defects that lead to privacy vulnerabilities.

**NICE Knowledge and Skill Statements:**

K0039, K0044, K0070, K0105, K0140, K0178, K0260, K0624, S0367

### Implementing Common Protections

**Course | 3 hours 10 minutes**

In this course, you will limit access using login and user roles, protect data in transit and at rest, implement error handling and logging, protect sensitive data and functions, and protect database access.

**NICE Knowledge and Skill Statements:**

K0039, K0044, K0079, K0178, K0260, K0262, S0014, S0022, S0031, S0034, S0138, S0149
Testing Software Security

Course | 32 minutes

In this course, you will follow an appropriate approach to security testing based on business and technical criteria, use code analysis to find security problems and use automated testing tools to find security problems.

NICE Knowledge and Skill Statements:
K0153, K0178, S0135, S0174

Maintaining Security in Deployed Software

Course | 38 minutes

In this course, you will monitor and log applications to support security, maintain security after deployment, and analyze code for suspicious or unauthorized changes.

NICE Knowledge and Skill Statements:
S0090
Gain the advantages of running applications in Docker while maintaining a solid security posture with this Container Security Learning Path.

### Skill Assessment

**Skill assessment | 20 questions**

See how your container security skills stack up against other professionals in your field.

**NICE Knowledge and Skill Statements:**

### Container Security Project

**Project | 1 hour 11 minutes**

Test your understanding of container security with this project. You will review images to reduce risk, make docker images follow best practices, and scan images for vulnerable software.

**NICE Knowledge and Skill Statements:**

### Introduction and Overview of Containers

**Course | 55 minutes**

Gain an understanding of the role containers and Docker have in modernizing IT with this overview of container fundamentals.

**NICE Knowledge and Skill Statements:**

### Docker Security

**Course | 4 hours 46 minutes**

Containers are gaining popularity and prominence in IT. This course provides methods to use Docker securely.

**NICE Knowledge and Skill Statements:**

### Kubernetes Security

**Course | 5 hours 57 minutes**

Kubernetes won the container orchestration race. Learn how it works and how to deploy containers and keep your cluster secure.

**NICE Knowledge and Skill Statements:**
Developing in Splunk

In this path, you will learn to create effective visualizations for different stakeholders with the Splunk Web Framework, utilize tokens and event handlers, explore SDKs, interact with REST APIs and build a test lab for log analysis and incident response.

Developing in Splunk skill assessment

Skill assessment | 20 questions
See how your Splunk skills stack up against other professionals in your field.

Getting Started With Splunk

Course | 27 minutes
Understand the way of setting up Splunk on cloud and locally with this course, and choose the right platform for you.

NICE Knowledge and Skill Statements:
K0004, K0089, K0147, K0161, K0162, K0167, K0224, K0344, K0452, K0488, K0536, S0121, S0149

Introduction to Splunk

Course | 1 hour 52 minutes
Learn the features, components, types and more about Splunk through this course.

NICE Knowledge and Skill Statements:
K0004, K0089, K0147, K0161, K0162, K0167, K0224, K0344, K0452, K0488, K0536, S0121, S0149

Building Splunk Apps

Course | 50 minutes
What are Splunk apps and how do we create them? This will be the main topic of this course. We'll also learn to integrate data inputs and how to maintain Splunk apps.

NICE Knowledge and Skill Statements:
K0004, K0089, K0147, K0161, K0162, K0167, K0224, K0452, K0488, K0536, S0121, S0149

Developing with Splunk’s REST API

Course | 4 hours 9 minutes
What is Splunk's REST API? What about SDK and KV-Store? We will explore all of these topics in this course. We'll also look at the HTTP Event Collector(HEC).

NICE Knowledge and Skill Statements:
K0004, K0089, K0147, K0161, K0162, K0167, K0224, K0452, K0488, K0536, S0121, S0149
DevSecOps

You will learn techniques used by leading organization to increase innovation and speed up delivery while remaining secure.

DevSecOps Skill Assessment

Skill assessment | 20 questions
See how your DevSecOps security skills stack up against other professionals in your field.

DevSecOps project

Project | 2 hours 27 minutes
Put what you’ve learned about DevSecOps to the test with this project.

DevSecOps overview

Course | 50 minutes
An introduction to DevSecOps topics, including security models, definitions and the software development life cycle (SDLC).

Source control management

Course | 38 minutes
This course explores source control management, GitHub, repositories and more.

Secure CI/CD pipeline

Course | 42 minutes
This course starts with an introduction to threat modeling, using Microsoft Threat Modeling Tool to identify potential threats at the design phase of the software development life cycle.

SCA in CI/CD pipeline

Course | 47 minutes
A look at software composition analysis in the CI/CD pipeline.
SAST in CI/CD pipeline

Course | 53 minutes

In this course, you’ll explore static application security testing (SAST) in the CI/CD pipeline.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0068, K0070, K0140, K0186, K0531, K0559, K0624, S0031, S0034, S0060, S0172, S0174, S0341

DAST in CI/CD pipeline

Course | 49 minutes

Explore the details of dynamic application security testing (DAST) in the CI/CD pipeline.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0068, K0070, K0140, K0531, K0559, K0624, S0031, S0034, S0060, S0172, S0174, S0341

Container security

Course | 50 minutes

A look at container security with an introduction to Docker and Kubernetes.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0068, K0070, K0130, K0140, K0186, K0531, K0559, K0610, K0624, S0029, S0031, S0034, S0060, S0073, S0172, S0341
Secure coding and DevSecOps

Use code “learnskills” to get 30 days for $1  GET STARTED

JavaScript Security

In this learning path, we will go through diverse JavaScript-related attacks and learn how to build safer JavaScript applications. Most of this learning path will cover front-end JavaScript; however, we will also consider Node.js in certain parts of the learning paths.

Skill Assessment

Skill assessment | 20 questions

See how your JavaScript security skills stack up against other professionals in your field.

JavaScript Security Project

Project | 2 hours 19 minutes

In the first four challenges, you will find vulnerabilities and exploit them. In the next five challenges, you will fix the vulnerabilities.

NICE Knowledge and Skill Statements:
K0004, K0016, K0068, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213

Cyber Range

Cyber range | 30 minutes

This lab covers multiple secure coding errors commonly found in JavaScript, including DOM rewrites and the use of the eval() statement.

Secure JavaScript Programming overview

Course | 53 minutes

In this course, we will cover some base concepts of JavaScript and its runtime environments.

NICE Knowledge and Skill Statements:
K0004, K0016, K0068, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213

Authentication

Course | 49 minutes

We will cover the case of cookies and non-cookies-based front-end authentication. We will also cover best practices in term of front-end identity management.

NICE Knowledge and Skill Statements:
K0004, K0007, K0016, K0068, K0140, K0236, K0325, K0336, K0372, K0396, K0398, K0487, K0561, S0060, S0172, S0213

XSS and JavaScript remote code executions

Course | 1 hour 33 minutes

This course explores cross-site scripting (XSS) in JavaScript.

NICE Knowledge and Skill Statements:
K0004, K0016, K0068, K0070, K0140, K0236, K0325, K0336, K0372, K0396, K0398, S0060, S0172, S0213
<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CSRF and browser security</strong></td>
<td>37 minutes</td>
</tr>
<tr>
<td>An exploration of cross-site request forgery, or CSRF.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
</tr>
<tr>
<td>K0004, K0016, K0061, K0068, K0070, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regular expressions</strong></td>
<td>34 minutes</td>
</tr>
<tr>
<td>Regular expressions are one of the most powerful, yet dangerous parts of JavaScript. In this course, we will dig into them to understand what risks they can bring and how to mitigate them.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
</tr>
<tr>
<td>K0004, K0016, K0023, K0068, K0070, K0140, K0236, K0325, K0372, K0396, K0398, S0013, S0037, S0060, S0172, S0213, S0285</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prototype pollution</strong></td>
<td>34 minutes</td>
</tr>
<tr>
<td>In this course, we will go through real-life examples of such attacks and learn how to protect against them.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
</tr>
<tr>
<td>K0004, K0005, K0016, K0068, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ecosystem modules (npm) and supply chain</strong></td>
<td>1 hour 13 minutes</td>
</tr>
<tr>
<td>In this course, we will see everything we need to know to find and assess packages. We will even see what to do if one of the packages we use is flagged as vulnerable.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
</tr>
<tr>
<td>K0004, K0016, K0068, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213, S0213</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Serverless JavaScript</strong></td>
<td>1 hour 5 minutes</td>
</tr>
<tr>
<td>In this course, we will review the security best practices of a safe serverless project.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
</tr>
<tr>
<td>K0004, K0016, K0068, K0077, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0143, S0153, S0172, S0213</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web developer desktop security</strong></td>
<td>10 minutes</td>
</tr>
<tr>
<td>Building web applications can open some parts of your own workstation to attacks. In this short course, we will go through a few “gotchas” anyone building web applications should know about.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
</tr>
<tr>
<td>K0004, K0016, K0068, K0105, K0140, K0236, K0325, K0349, K0372, K0396, K0398, K0444, K0624, S0060, S0172, S0213</td>
<td></td>
</tr>
</tbody>
</table>
Secure Coding Fundamentals

This path helps you understand software vulnerabilities and how to recognize them in code, demonstrates how they are exploited by attackers (including real-world case studies of vulnerable applications in production), and describes ways by which the vulnerabilities can be mitigated.

**Skill Assessment**

Skill assessment | 20 questions

See how your secure coding skills stack up against other professionals in your field.

**Python Code Security Cyber Range**

Cyber range | 10 labs

Gain practical experience and develop your secure Python coding skills through 10 hands-on labs in the Python Code Security Cyber Range.

NICE Knowledge and Skill Statements:

S0051, S0060, S0172, S0174, S0266

**Secure Coding Fundamentals Project**

Project | 2 hours 8 minutes

Practice your secure coding skills by solving challenges.

NICE Knowledge and Skill Statements:

S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266

**Introduction to Secure Coding Fundamentals**

Course | 6 minutes

This course introduces the need for secure coding and the tools used in this learning path.

NICE Knowledge and Skill Statements:

K0009, K0140

**Buffer Overflows**

Course | 50 minutes

This course introduces the buffer overflow vulnerability, its exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140

**Integer Overflows and Underflows**

Course | 53 minutes

This course introduces integer overflow and underflow vulnerabilities, their exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140
## Race Conditions

Course | 48 minutes
This course introduces race conditions, their exploitation and possible mitigations.

**NICE Knowledge and Skill Statements:**
K0009, K0016, K0063, K0070, K0140

## Format String Vulnerabilities

Course | 32 minutes
This course introduces format string vulnerabilities, their exploitation and possible mitigations.

**NICE Knowledge and Skill Statements:**
K0009, K0016, K0070, K0140

## Command Injection

Course | 39 minutes
This course introduces command injection vulnerabilities, their exploitation and possible mitigations.

**NICE Knowledge and Skill Statements:**
K0009, K0016, K0070, K0140, K0372

## Least Privilege

Course | 33 minutes
This course introduces the principle of least privilege and its importance in secure coding.

**NICE Knowledge and Skill Statements:**
K0009, K0016, K0070, K0140, K0167

## Credential Management

Course | 1 hour
This course describes how poor credential management can make an application vulnerable to attack, how it can be exploited and how to manage credentials properly.

**NICE Knowledge and Skill Statements:**
K0009, K0016, K0070, K0140, K0336, K0362

## Cryptography

Course | 40 minutes
This course discusses how the poor use of cryptography can leave an application vulnerable to attack and how it can be exploited, as well as potential mitigations.

**NICE Knowledge and Skill Statements:**
K0009, K0016, K0070, K0190, K0362

## SQL Injection

Course | 43 minutes
This course introduces SQL injection vulnerabilities, their exploitation and possible mitigations.

**NICE Knowledge and Skill Statements:**
K0009, K0016, K0024, K0069, K0070, K0140

## Cross-Site Scripting

Course | 31 minutes
This course introduces cross-site scripting vulnerabilities, their exploitation and possible mitigations.

**NICE Knowledge and Skill Statements:**
K0009, K0016, K0070, K0140

## Cross-Site Request Forgery

Course | 23 minutes
This course introduces cross-site request forgery vulnerabilities, their exploitation and possible mitigations.

**NICE Knowledge and Skill Statements:**
K0009, K0016, K0070, K0140
Poor HTTP Usage

Course | 43 minutes
This course describes how poor use of HTTP and HTML can be exploited, as well as possible mitigations.

NICE Knowledge and Skill Statements:
K0009, K0016, K0070, K0140, K0398

Error Handling

Course | 27 minutes
This course describes how poor error handling can be exploited and possible mitigations for this problem.

NICE Knowledge and Skill Statements:
K0009, K0016, K0070, K0140
Secure SDLC

The Secure SDLC learning path is a step-by-step approach to integrate the security controls into your software or system development life cycle. You will learn how to use each phase to develop or establish both proactive and reactive security controls across your organization.

Skill Assessment

Skill assessment | 20 questions
See how your secure SDLC skills stack up against other professionals in your field.

Secure SDLC Project

Project | 2 hours 27 minutes
Practice your secure SDLC skills by solving challenges.

NICE Knowledge and Skill Statements:
S0174

Introduction to SDLC

Course | 23 minutes
In this course, you'll be introduced to Secure SDLC, a framework to establish system development by integrating security.

NICE Knowledge and Skill Statements:
K0005, K0039, K0165

Security Awareness Training

Course | 1 hour 1 minute
Security awareness training is an education process that teaches employees and users about cybersecurity, IT best practices and even regulatory compliance.

NICE Knowledge and Skill Statements:
K0005, K0039, K0243

Secure Requirements

Course | 35 minutes
Secure requirements are security features required by system users or a quality the system must have to increase the user's trust.

NICE Knowledge and Skill Statements:
K0039, K0044, K0263, K0624

Secure Design

Course | 2 hours
Secure design applies to individual features that can correspond to their respective secure requirements.

NICE Knowledge and Skill Statements:
K0087, K0165, K0297
<table>
<thead>
<tr>
<th>Secure Build</th>
<th>Secure Deploy</th>
<th>Secure Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>38 minutes</td>
<td>Secure deploy is for the purpose of formalizing and automating the deployment process in a secure way.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>K0039, K0153</td>
<td>Secure validation is testing with a hacker's perspective to check whether the security controls are in place.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure Response</th>
<th>Collaborative Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>34 minutes</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>K0039, K0042</td>
</tr>
</tbody>
</table>

Use code “learnskills” to get 30 days for $1
Software Security Testing

This pathway will help you master industry standards and enable you to carry out professional assessments to secure technologies, as well as communicate risks to high-level executives, management and technical staff.

Skill Assessment

Skill assessment | 20 questions
See how your software security testing skills stack up against other professionals in your field.

Software security testing project

Project | 2 hours 18 minutes
Test your knowledge of software security testing with this project.

Introduction to Software Security Testing

Course | 22 minutes
Environment setup is an essential process for becoming professional software security testers. This course will set up Kali Linux, a Debian-derived Linux distribution designed for digital forensics and penetration testing.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0290, K0609, K0610, K0624, S0014, S0078, S0174

Important software security testing terminology

Course | 21 minutes
It is vitally important to learn and adopt critical terminology and vocabulary. This course will highlight some essential concepts that you need to know in software security testing.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0009, K0059, K0070, K0090, K0147, K0290, K0412, K0415, K0436, K0609, K0610, K0624, S0014, S0078, S0174

Methodologies and standards

Course | 14 minutes
In this course, we will explore essential testing methodologies and standards that software security testers use regularly.

NICE Knowledge and Skill Statements:
K0001, K0004, K0005, K0006, K0009, K0054, K0059, K0070, K0075, K0087, K0090, K0147, K0154, K0260, K0261, K0262, K0290, K0377, K0624, S0014, S0078, S0174

Software testing as a process

Course | 29 minutes
Continuous learning and improvement are essential to staying relevant. Software security testing is similar to chess: easy to learn but hard to master. In this course, we will explore software testing as a process.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0009, K0043, K0070, K0075, K0087, K0090, K0147, K0290, K0624, S0014, S0078, S0174
<table>
<thead>
<tr>
<th>Title</th>
<th>Course Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The HTTP protocol</td>
<td>46 minutes</td>
<td>HTTP (HyperText Transfer Protocol) is the underlying protocol of the web. This course will explore the foundations of the HTTP protocol and the importance to software security.</td>
</tr>
<tr>
<td>Introduction to encoding</td>
<td>16 minutes</td>
<td>In this course, we will learn how to identify different encoding algorithms and decode them.</td>
</tr>
<tr>
<td>Configuration and management testing</td>
<td>20 minutes</td>
<td>In this course, we will learn about configuration and management testing.</td>
</tr>
<tr>
<td>Identity management testing</td>
<td>14 minutes</td>
<td>This course will explore identity and access management as one of the most critical provisions for IT departments.</td>
</tr>
<tr>
<td>Authorization testing</td>
<td>22 minutes</td>
<td>Testing for authorization means understanding how the authorization process works and using that information to circumvent the authorization mechanism. In this course, we will learn about authorization and various vulnerabilities in the implementation.</td>
</tr>
<tr>
<td>Session management testing</td>
<td>29 minutes</td>
<td>In this course, we will explore some of the misconfigurations and vulnerabilities in session management.</td>
</tr>
<tr>
<td>Input validation testing</td>
<td>39 minutes</td>
<td>In this course, we will explore data validation vulnerabilities and mitigation.</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**
- **The HTTP protocol:** K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0140, K0147, K0290, K0624, S0014, S0078, S0095, S0174
- **Introduction to encoding:**
  - K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0140, K0147, K0290, K0624, S0014, S0078, S0095, S0174
- **Configuration and management testing:**
  - K0004, K0005, K0006, K0009, K0059, K0070, K0073, K0075, K0090, K0275, K0290, K0624, S0014, S0078, S0153, S0174
- **Identity management testing:**
  - K0004, K0005, K0006, K0007, K0009, K0056, K0059, K0065, K0070, K0075, K0090, K0158, K0290, K0624, S0014, S0031, S0078, S0174
- **Authorization testing:**
  - K0004, K0005, K0006, K0009, K0059, K0061, K0070, K0075, K0090, K0147, K0290, K0315, K0408, K0624, S0014, S0078, S0174
- **Session management testing:**
  - K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0290, K0336, K0487, K0624, S0014, S0078, S0174
- **Input validation testing:**
  - K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0290, K0624, S0014, S0019, S0078, S0174
Client-side testing

Course | 32 minutes

Client-side testing refers to any type of testing that occurs in the user's browser. This course will explore testing mechanisms for client-side vulnerabilities and ways to mitigate and reduce impact.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0290, K0624, S0014, S0078, S0174

Client-side testing reports

Course | 39 minutes

This course will help you learn crucial components of a software security testing report.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0403, S0014, S0078, S0174

Error handling

Course | 12 minutes

In this course, we will explore error handling vulnerabilities and mitigation.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0290, K0624, S0014, S0078, S0174

Cryptography

Course | 14 minutes

Cryptography appears to be closely linked to modern electronic communication. This course will teach you about cryptography and weak cryptographic algorithms that should be avoided while developing software.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0009, K0018, K0019, K0044, K0059, K0070, K0075, K0090, K0147, K0290, K0308, K0624, S0014, S0073

Business logic testing

Course | 14 minutes

Testing for business logic flaws in a multi-functional dynamic application requires thinking in unconventional ways. This course will teach you about the importance of business logic testing while helping you to think creatively.

NICE Knowledge and Skill Statements:
K0004, K0005, K0006, K0009, K0059, K0068, K0070, K0075, K0090, K0146, K0147, K0403, S0014, S0078, S0174, S0354
Writing Secure Code for Android

This learning path teaches you how to incorporate security in Android application development for mobile devices. You will learn about Kotlin, best practices for addressing the most common security mistakes Android app developers make and learn to implement security into your app development.

Skill Assessment

Skill assessment | 20 questions
See how your secure coding in Android skills stack up against other professionals in your field.

Introduction to secure coding in Android

Course | 3 hours 6 minutes
Start your learning by understanding why secure coding is essential in mobile app development.

NICE Knowledge and Skill Statements:
K0014, K0016, K0068, K0372, K0624, S0060, S0257, S0266

Input validation

Course | 8 hours 11 minutes
Now that you understand the need for mobile app security, you should learn how to implement the most fundamental security mechanism of all: input validation.

NICE Knowledge and Skill Statements:
K0014, K0016, K0068, K0140, K0236, K0372, K0624, S0019, S0060, S0257, S0266

Memory corruption

Course | 46 minutes
You have learned the many ways to sanitize input in your app. It's time to turn your attention to mitigating another major application security risk: memory corruption.

NICE Knowledge and Skill Statements:
K0014, K0068, K0070, K0114, K0140, K0236, K0372, K0624, S0019, S0060, S0257, S0266

Encryption in Android

Course | 2 hours 31 minutes
You know about the most pressing security risks your app faces and how to address those risks. You can now learn how to use the one control that protects data better than any other: encryption.

NICE Knowledge and Skill Statements:
K0014, K0016, K0018, K0019, K0068, K0140, K0190, K0236, K0308, K0372, K0427, S0019, S0060, S0257, S0266

Protecting data

Course | 5 hours 12 minutes
Now that you have a good understanding of encryption, you can build on that foundation by learning additional ways to protect user data.

NICE Knowledge and Skill Statements:
K0005, K0014, K0016, K0068, K0095, K0140, K0168, K0224, K0236, K0372, K0419, K0624, S0019, S0060, S0257, S0266
Access control in Android

Course | 3 hours 12 minutes

You have learned many ways to protect data. You can now expand your security efforts by controlling access to the device and the app.

NICE Knowledge and Skill Statements:
K0005, K0007, K0014, K0016, K0033, K0056, K0068, K0070, K0095, K0372, K0488, S0007, S0019, S0031, S0060, S0097, S0257, S0266

Protecting software and system integrity

Course | 2 hours 32 minutes

You have gained a solid foundation for implementing the most common security controls in Android app development. You can now finish up your skill set by learning how to maintain application and device integrity.

NICE Knowledge and Skill Statements:
K0005, K0007, K0014, K0016, K0044, K0068, K0091, K0152, K0211, K0229, K0372, S0006, S0007, S0034, S0060, S0076, S0149, S0257, S0266, S0367
Writing Secure Code in C++

This learning path is intended for people who already know the C and C++ languages and want to improve their ability to write secure code.

Skill Assessment

Skill assessment | 20 questions
See how your secure C++ coding skills stack up against other professionals in your field.

Writing Secure Code in C++ Project

Project | 2 hours 48 minutes
Practice your secure C++ coding skills by solving challenges.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

C++ Code Security Cyber Range

Cyber range | 10 labs
Gain practical experience and develop your secure C++ coding skills through 10 hands-on labs in the C++ Code Security Cyber Range.

NICE Knowledge and Skill Statements:
S0060, S0172, S0174, S0266

Secure C/C++

Course | 13 minutes
This course is the introduction to the learning path. It presents the teacher, the tools and the content of the courses and explains why secure C/C++ is important.

NICE Knowledge and Skill Statements:
K0009, K0016, K0068, K0070

C/C++ Particularities

Course | 2 hours 44 minutes
This course covers all of the C/C++ particularities a programmer needs to know to create secure programs using these languages.

NICE Knowledge and Skill Statements:
K0009, K0016, K0068, K0070, K0372, K0396

Interacting with the World

Course | 2 hours 15 minutes
This course describes many ways a program can interact with the world.

NICE Knowledge and Skill Statements:
K0009, K0016, K0068, K0140, K0396
<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Handling</td>
<td>43 minutes</td>
<td>This course describes what to do and what not to do when an error occurs.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>K0009, K0016, K0068, K0140, K0229, K0396</td>
<td></td>
</tr>
<tr>
<td>Random Number Generation</td>
<td>21 minutes</td>
<td>This course explains why good random number generation is important when developing software. It also shows how the functions, the C library provides for that, are flawed. And then, it describes better way to generate random numbers.</td>
</tr>
<tr>
<td>SETUID Bit</td>
<td>29 minutes</td>
<td>Some programs have “superpowers,” and programming them requires special attention.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>K0009, K0016, K0068, K0140, K0396</td>
<td></td>
</tr>
<tr>
<td>Driver Development</td>
<td>43 minutes</td>
<td>Device drivers, as operating systems, are written in C. When applications interact directly with them, they become the kernel's last line of defense.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>K0009, K0016, K0068, K0140, K0396, K0608</td>
<td></td>
</tr>
</tbody>
</table>
# Writing Secure Code in iOS

This learning path teaches you how to incorporate security in iOS application development for mobile devices. Focused mostly on Swift, Apple's new programming language, you will learn best practices for addressing the most common security mistakes iOS app developers make.

## Skill Assessment

<table>
<thead>
<tr>
<th>Skill Assessment</th>
<th>20 questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill assessment</td>
<td>See how your secure iOS coding skills stack up against other professionals in your field.</td>
</tr>
</tbody>
</table>

## Penetration Testing Cyber Range

<table>
<thead>
<tr>
<th>Penetration Testing Cyber Range</th>
<th>7 hours 26 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber range</td>
<td>This cyber range helps you develop your knowledge of penetration testing and ethical hacking by practicing on cloud-hosted virtual machines.</td>
</tr>
</tbody>
</table>

## Purple Team Web Application Security Project

<table>
<thead>
<tr>
<th>Purple Team Web Application Security Project</th>
<th>2 hours 34 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project</td>
<td>This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application.</td>
</tr>
</tbody>
</table>

## Introduction to Secure Coding

<table>
<thead>
<tr>
<th>Introduction to Secure Coding</th>
<th>3 hours 48 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>Start your learning by understanding why secure coding is essential in mobile app development.</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**

- K0004, K0039, K0068, K0070, K0079, K0080, K0082, K0139, K0140, K0269, K0559, K0624, S0060, S0172

## Input Validation

<table>
<thead>
<tr>
<th>Input Validation</th>
<th>5 hours 22 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>Now that you understand the need for mobile app security, you should learn how to implement the most fundamental security mechanism of all: input validation.</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**

- K0004, K0039, K0059, K0068, K0070, K0080, K0082, K0140, K0624, S0019, S0060, S0172

## Memory Corruption

<table>
<thead>
<tr>
<th>Memory Corruption</th>
<th>45 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>You have learned the many ways to sanitize input in your app. It is time now to turn your attention to mitigating another major application security risk: memory corruption.</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**

- K0039, K0059, K0068, K0070, K0079, K0080, K0082, K0114, K0140, K0624, S0060, S0172
Encrypting data and protecting system integrity

Course | 3 hours 2 minutes

You know about the most pressing security risks your app faces and how to address those risks. You can now learn how to use the one control that protects data better than any other: encryption.

NICE Knowledge and Skill Statements:
K0018, K0019, K0039, K0068, K0070, K0080, K0082, K0140, K0190, K0308, K0403, K0427, S0060, S0172, S0298

Protecting Data

Course | 2 hours 20 minutes

Now that you have a good understanding of encryption, you can build on that foundation by learning additional ways to protect user data.

NICE Knowledge and Skill Statements:
K0005, K0039, K0068, K0070, K0079, K0080, K0082, K0104, K0392, K0438, K0559, K0560, K0624, S0060, S0172

Access Control

Course | 1 hour 6 minutes

You have learned many ways to protect data. You can now expand your security efforts by controlling access to the device and the app.

NICE Knowledge and Skill Statements:
K0004, K0005, K0007, K0039, K0065, K0068, K0070, K0079, K0080, K0082, K0140, K0336, S0031, S0060, S0172

Protecting software and system integrity

Course | 1 hour 49 minutes

You have gained a solid foundation for implementing the most common security controls in iOS app development. You can now finish up your skill set by learning how to maintain application and device integrity.

NICE Knowledge and Skill Statements:
K0004, K0005, K0039, K0044, K0068, K0070, K0079, K0080, K0082, K0140, K0229, K0295, S0006, S0060, S0149, S0172
Writing Secure Code in ASP.NET

This skill path will enable you as a professional to execute secure coding practices, identify vulnerabilities in the code, remediate identified weaknesses, design with security in mind and build effective security controls to protect against breaches and malicious hackers.

**ASPNET skill assessment**

Skill assessment | 20 questions

See how your secure secure coding skills stack up against other professionals in your field.

**.NET project**

Project | 2 hours 22 minutes

Test your knowledge of ASP.NET security with this project.

**Getting started with .NET core**

Course | 45 minutes

In this course, you'll get to grips with the fundamentals of ASP.NET Core.

**.NET core vulnerabilities**

Course | 1 hour 55 minutes

Without in-depth knowledge of what causes a vulnerability, it is almost impossible to deliver on the customers' expectations. This course addresses .NET Core vulnerabilities.

**.NET core vulnerabilities mitigation**

Course | 2 hours 24 minutes

Mitigation of vulnerabilities is a critical statement in the fight against cybercriminals. This course explores vulnerability mitigation.

**Cryptography in .NET**

Course | 59 minutes

This course will explore cryptographic operations in .NET Core that help developers code systems that protect confidentiality, integrity, non-repudiation and authenticity.
Writing Secure Code in Java

Explore the ins and outs of writing secure coding in Java with these courses covering authentication, injection attacks, website security and more.

Skill Assessment
Skill assessment | 20 questions
See how your secure Java coding skills stack up against other professionals in your field.

Writing Secure Code in Java Project
Project | 2 hours 24 minutes
Build your Java project, then mitigate the vulnerabilities by adding validation to the inputs. You will also implement spring security on an application.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

Introduction to Java
Course | 51 minutes
Take a deep dive into input validation, how to validate various input types and how to safeguard against malicious inputs that would be used for injection attacks.

NICE Knowledge and Skill Statements:
K0009, K0016, K0068, K0070, K0140

Injection Attacks
Course | 32 minutes
This course provides a demonstration of several SQL injection attacks and the special characters required to make them possible.

NICE Knowledge and Skill Statements:
K0009, K0016, K0068, K0070, K0140

Authentication
Course | 29 minutes
In this course, you'll review all the components required to secure a system.

NICE Knowledge and Skill Statements:
K0009, K0016, K0068, K0070, K0140, K0336

Sensitive Data
Course | 27 minutes
This course discusses sensitive data, non-sensitive data and personally identifiable information and provides examples of each.

NICE Knowledge and Skill Statements:
K0003, K0260, K0261, K0262, K0615
<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
<th>NICE Knowledge and Skill Statements:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input Output</strong></td>
<td>49 minutes</td>
<td>K0001, K0009, K0070, K0140</td>
<td>This course reviews inputs and outputs to your system and how to move data in and out of your system securely.</td>
</tr>
<tr>
<td><strong>Website Security</strong></td>
<td>1 hour 34 minutes</td>
<td>K0070, K0140, K0349, K0398</td>
<td>This course is a deep dive into redirects and forwards and the vulnerabilities associated with each.</td>
</tr>
<tr>
<td><strong>Malware</strong></td>
<td>21 minutes</td>
<td>K0153, K0480</td>
<td>This course discusses malware related to Java development and how to mitigate the risks, and go over formalized code reviews.</td>
</tr>
</tbody>
</table>
Writing Secure Code in Node.js

In this learning path, you will learn how to attack and protect Node.js applications.

Skill Assessment

Skill assessment | 20 questions

See how your secure node.js coding skills stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

Writing Secure Code in Node.js Project

Project | 2 hours 15 minutes

There are seven challenges spread across three Node.js projects. Part 1 focuses on MongoDB injections and how to prevent them. Part 2 exploits event loop blocking. Part 3 is the one you need if you want to attack and fix a GraphQL API.

NICE Knowledge and Skill Statements:

Refresher on Node.js

Course | 30 minutes

This course will cover the basics of Node.js architecture.

NICE Knowledge and Skill Statements:

Protecting databases

Course | 46 minutes

This course will focus on protecting database access.

NICE Knowledge and Skill Statements:

Node.js denial-of-service

Course | 1 hour 17 minutes

This course will focus on different ways of obtaining denial-of-service in Node.js and how to prevent them.

NICE Knowledge and Skill Statements:

Authentication and authorization

Course | 47 minutes

A look at authentication and authorization in Node.js.

NICE Knowledge and Skill Statements:
Prototype pollution

Course | 33 minutes
Exploring prototype pollution in Node.js.

NICE Knowledge and Skill Statements:
K0016, K0068, K0070, K0140, K0372, K0624

Unsafe strings

Course | 1 hour 3 minutes
Confronting the challenge of unsafe strings in Node.js.

NICE Knowledge and Skill Statements:
K0009, K0070, K0140

Error handling and asynchronous debugging monitoring

Course | 46 minutes
A look at the challenges of error handling in an asynchronous environment.

NICE Knowledge and Skill Statements:
K0016, K0068, K0079, K0140, K0186, K0372, K0396, S0014, S0149

Ecosystem modules (npm) and supply chain

Course | 55 minutes
An introduction to the challenges of npm modules.

NICE Knowledge and Skill Statements:
K0016, K0068, K0140, K0152, K0164, K0372

GraphQL security

Course | 44 minutes
This course explores mitigating the risks of GraphQL.

NICE Knowledge and Skill Statements:
K0016, K0068, K0140, K0332, K0372

Unsafe strings

Course | 1 hour 3 minutes
Confronting the challenge of unsafe strings in Node.js.

NICE Knowledge and Skill Statements:
K0009, K0070, K0140

Error handling and asynchronous debugging monitoring

Course | 46 minutes
A look at the challenges of error handling in an asynchronous environment.

NICE Knowledge and Skill Statements:
K0016, K0068, K0079, K0140, K0186, K0372, K0396, S0014, S0149

Ecosystem modules (npm) and supply chain

Course | 55 minutes
An introduction to the challenges of npm modules.

NICE Knowledge and Skill Statements:
K0016, K0068, K0140, K0152, K0164, K0372

GraphQL security

Course | 44 minutes
This course explores mitigating the risks of GraphQL.

NICE Knowledge and Skill Statements:
K0016, K0068, K0140, K0332, K0372
## Writing Secure Code in PHP

The Writing Secure Code in PHP Learning Path provides you with a foundation of secure programming techniques implemented in PHP. By the end of the learning path, you will be equipped to design and build secure and modern PHP applications.

### Skill Assessment

**Skill assessment | 20 questions**

See how your secure PHP coding skills stack up against other professionals in your field.

### Writing Secure Code in PHP Project

**Project | 2 hours 15 minutes**

Use your secure PHP coding skills to uncover issues in a simple application, such as cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, insecure secrets, lack of input sanitation and lack of proper error handling.

**NICE Knowledge and Skill Statements:**

S0060, S0172, S0239, S0266

### Operating Environment

**Course | 36 minutes**

This course takes a close look at the operating environment that your code runs in. This includes the version of PHP being used, third-party libraries and browser security such as HTTPS.

**NICE Knowledge and Skill Statements:**

K0009, K0016, K0070, K0140, K0603

### Cryptography Weaknesses

**Course | 1 hour 24 minutes**

This course provides a look at weaknesses in common cryptographic logic, including the better options that we have available to us. Also includes an overview of correctly handling our secret information.

**NICE Knowledge and Skill Statements:**

K0007, K0009, K0016, K0018, K0019, K0070, K0140, K0190, K0336, K0403

### Code-Data Separation

**Course | 1 hour 2 minutes**

This course covers the separation of our code and data to prevent some of the most common types of attacks. These include SQL injection, XSS, CSRF, data leaks and source disclosure.

**NICE Knowledge and Skill Statements:**

K0009, K0016, K0070, K0140, K0624

### Application Logic

**Course | 1 hour 13 minutes**

In this course, you'll explore common types of application logic that are often sources of security vulnerabilities. These affect every part of your application and include things such as sessions, cookies, file uploads and error handling.

**NICE Knowledge and Skill Statements:**

K0007, K0009, K0016, K0068, K0070, K0140
<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APIs</strong></td>
<td>25 minutes</td>
</tr>
<tr>
<td><strong>Development Process</strong></td>
<td>1 hour 11 minutes</td>
</tr>
<tr>
<td><strong>Infrastructure</strong></td>
<td>1 hour 6 minutes</td>
</tr>
</tbody>
</table>

### APIs

APIs are an important part of modern web applications and require careful planning to ensure security. This course looks at how we secure APIs during authentication as well as responses.

NICE Knowledge and Skill Statements:
K0007, K0009, K0016, K0068, K0070, K0140, K0624

### Development Process

This course takes a look at our entire development process to ensure security at every point. This includes the tools we use and the places our code lives, as well as how we develop our code.

NICE Knowledge and Skill Statements:
K0009, K0016, K0068, K0070, K0140, K0153, K0178

### Infrastructure

A look at the infrastructure beneath our code, including how to set it up and secure it. This includes traditional architectures as well as modern architectures.

NICE Knowledge and Skill Statements:
K0032, K0178, K0205, K0286
Labs

Cyber ranges in Infosec Skills are cloud-hosted on virtual machines to provide the most realistic learning environment possible. With 100+ labs covering a variety of topics, you can build your cybersecurity skills through relevant, practical training — and go into your next project or job role with confidence.

C++ Code Security Cyber Range

This cyber range helps you develop your knowledge in finding and remediating vulnerabilities in C++ code. You’ll build and reinforce your skills as you progress through labs covering a wide range of C++ code security topics.

C++ – Introduction to cppcheck

Lab | 14 steps

cppcheck is a static code analysis tool for C++ code that tests for a wide number of potential vulnerabilities and other errors. This lab demonstrates some of the basic functionality and use of cppcheck.

NICE Knowledge and Skill Statements:
S0174

C++ – Control Flow Analysis in C++

Lab | 11 steps

A variety of different errors can affect the execution flow of code and its eventual result. This lab demonstrates the use of a control flow analysis tool for tracking the flow of C++ code and identifying these errors.

NICE Knowledge and Skill Statements:
S0174

C++ – Buffer Overflows

Lab | 14 steps

Buffer overflows are one of the simplest and most common programming errors in C++ code. This lab demonstrates several ways that a buffer overflow vulnerability can be introduced into code, how they can be exploited, and how to correct them.

NICE Knowledge and Skill Statements:
S0174

C++ – Integer Overflows and Underflows

Lab | 13 steps

Integer overflow and underflow vulnerabilities are created by unsafe typecasting between different integer variable types. This lab demonstrates code containing these vulnerabilities and how the vulnerabilities can be exploited.

NICE Knowledge and Skill Statements:
S0174

C++ – Format String Vulnerabilities

Lab | 13 steps

Format string specifiers are useful for building strings using variables of other types. However, if they are misused, they can have unexpected results or open up a program to exploitation.

NICE Knowledge and Skill Statements:
S0174

C++ – XPath Injection

Lab | 15 steps

XPath makes it possible to programmatically access data stored within an XML document. This lab demonstrates how poorly-designed XPath queries can be exploited and corrected.

NICE Knowledge and Skill Statements:
S0174

Use code “learnskills” to get 30 days for $1 GET STARTED
C++ – Type Management

Lab | 15 steps

C++ has a number of different variable types and ways of using them. This lab explores some of the ways that types and functions can be misused.

NICE Knowledge and Skill Statements:
S0174

C++ – Pointer Management

Lab | 14 steps

C++ pointers contain memory addresses and are used as a reference to arrays and other object types. This lab demonstrates some of the common mistakes made using pointers in C++.

NICE Knowledge and Skill Statements:
S0174

C++ – Sensitive Data Disclosure

Lab | 13 steps

Applications are frequently designed to process and protect sensitive information. This lab explores some of the ways that logical or implementation errors can unintentionally expose this data.

NICE Knowledge and Skill Statements:
S0174

C++ – Poor Error Handling

Lab | 15 steps

A variety of different factors can cause low-level functions and other code to fail. This lab demonstrates some ways in which errors in error handling can make code execution unpredictable or exploitable.

NICE Knowledge and Skill Statements:
S0174
Command Line Basics Cyber Range

This cyber range introduces the most common Linux and Windows command-line tools and utilities. From basic navigation commands to port scanning and modifying file permissions, the labs in this cyber range help you practice some of the fundamental system and network administration tasks using Command-Line Interface (CLI).

**Navigation**

- Lab | 26 steps
  
  This lab goes through some of the basic commands for listing and navigating between files and directories on Linux and Windows systems.

  NICE Knowledge and Skill Statements: S0267

**Text Control**

- Lab | 13 steps
  
  Learn the basics of text control and searching for specific strings of text.

  NICE Knowledge and Skill Statements: S0267

**User Accounts and Privileges**

- Lab | 33 steps
  
  This lab focuses on creating and assigning users to groups as well as changing the privileges of said users and groups.

  NICE Knowledge and Skill Statements: S0158, S0267

**File and Directory Permissions**

- Lab | 18 steps
  
  This lab consists of editing permissions for files and directories and seeing how these permissions affect specific users.

  NICE Knowledge and Skill Statements: S0267

**Basic Networking Utilities**

- Lab | 14 steps
  
  This lab introduces the most popular command-line tools for testing and troubleshooting network connections, including ping, netstat, traceroute, tcpdump and others.

  NICE Knowledge and Skill Statements: S0046, S0241, S0267, S0294

**Port Scanning**

- Lab | 15 steps
  
  This lab walks through some of the most basic port scans that every system administrator should know.

  NICE Knowledge and Skill Statements: S0081, S0267
Introduction to PowerShell

Lab | 12 steps

In this lab we will demonstrate the uses of PowerShell as well as the functionality as a command line tool.

NICE Knowledge and Skill Statements:
S0158, S0267

File Transfer Protocol (FTP)

Lab | 20 steps

This lab uses an FTP server to demonstrate some of the utilities of the FTP protocol as well as some of the weaknesses.

NICE Knowledge and Skill Statements:
S0158, S0267

Remote Access (telnet vs. SSH)

Lab | 11 steps

This lab compares two commonly used methods of remote access — telnet and Secure Shell (SSH). You will go through steps of connecting to a remote host using both methods and try capturing login credentials.

NICE Knowledge and Skill Statements:
S0267
Computer Forensics Cyber Range

HANDS-ON TRAINING

Build and reinforce your skills as you progress through labs covering key computer forensics topics, including creating and examining forensic images, performing memory forensics to identify malware activity, data carving and more. You will practice working with popular forensics tools, such as Volatility and Foremost.

Command Line Basics for Forensics

Lab | 13 steps

Practice basic Linux commands and some of the most useful native Linux tools for computer forensic investigations.

NICE Knowledge and Skill Statements: S0267

Recovering data

Lab | 11 steps

In this lab, you will practice different methods of recovering data and finding out useful information straight from the command line.

NICE Knowledge and Skill Statements: S0051, S0267

Hash Databases

Lab | 7 steps

DFIR uses hashing and it is used as a way of verifying the authenticity and structure of a file, normally with MD5 or SHA-1 checksums. We will use sha1deep and sha1sum to show how this works.

NICE Knowledge and Skill Statements: S0071, S0267

File Carving

Lab | 13 steps

Practice carving different file types using foremost and scalpel.

NICE Knowledge and Skill Statements: S0071, S0267

Network Forensics and Volatility

Lab | 9 steps

Use Volatility to find malware network activity from an infected Windows 7 memory dump.

NICE Knowledge and Skill Statements: S0071, S0091, S0267

Memory Forensics with Volatility

Lab | 15 steps

Practice using Volatility to discover evidence on a Windows memory dump.

NICE Knowledge and Skill Statements: S0062, S0071, S0091, S0267
ICS/SCADA Pentesting CTF: Lights Out

HANDS-ON TRAINING

You've become aware of a plot to launch a cyber-attack against a large sports stadium. Attackers plan to take over the facility's power management system and turn out the lights during a Sunday night sporting event. Your mission is to convince local authorities and stadium management the threat is real before time runs out.

Capture the Flag: Lights Out

Lab | 10 steps

Put on your white hat and try to prevent a major disaster from happening by solving 10 ICS/SCADA pentesting challenges.

NICE Knowledge and Skill Statements:
S0051, S0078, S0081
Linux Cyber Range

HANDS-ON TRAINING

Build your skills as you progress through labs covering a wide range of Linux topics, including basic commands, file and directory operations and attributes, permissions, job scheduling and much more. You'll also learn about managing SELinux, packages, extended file systems, firewalls, and units and control groups.

### Basic Commands

**Lab | 15 steps**

Learn basic Linux commands and gain hands-on experience as you practice in the Linux Cyber Range.

*NICE Knowledge and Skill Statements:*

S0267

### VI Editor and Help

**Lab | 14 steps**

Learn about the visual editor as you practice in the Linux Cyber Range.

*NICE Knowledge and Skill Statements:*

S0067, S0158, S0267

### Compressing and Archiving Tools

**Lab | 18 steps**

Explore compressing and archiving tools, such as gzip, gunzip, bzip2, bunzip2 and tar, as you practice in the Linux Cyber Range.

*NICE Knowledge and Skill Statements:*

S0067, S0158, S0267

### Login History and System Information

**Lab | 17 steps**

Learn about login user and group info, history info and system info as you practice in the Linux Cyber Range.

*NICE Knowledge and Skill Statements:*

S0067, S0267

### File Path and File Types

**Lab | 12 steps**

Learn about file paths and types as you practice in the Linux Cyber Range.

*NICE Knowledge and Skill Statements:*

S0067, S0158, S0267

### File and Directory Operations

**Lab | 19 steps**

Learn about file and directory operations as you practice in the Linux Cyber Range.

*NICE Knowledge and Skill Statements:*

S0067, S0158, S0267
**File and Directory Control Attributes**

Lab | 20 steps

Learn about file and directory control attributes as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

**File and Directory Permissions**

Lab | 18 steps

Learn about file and directory permissions as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

**Special Permissions**

Lab | 16 steps

Learn about special permissions as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

**Bash Shell**

Lab | 18 steps

Learn about Bash Shell as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

**Regular Expressions and Metacharacters**

Lab | 19 steps

Learn about regular expressions and metacharacters as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0267

**Network Information and NTP**

Lab | 10 steps

Learn about Network Time Protocol (NTP) as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

**Managing User and Group Accounts**

Lab | 36 steps

Learn about managing user and group accounts, including creating, deleting and passwords, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

**Creating and Managing Partitions**

Lab | 25 steps

Learn about creating and managing partitions as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

**Defining a NAT Virtual Network**

Lab | 7 steps

Learn about defining a Network Address Translation (NAT) virtual network as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0007, S0067, S0158, S0267
<table>
<thead>
<tr>
<th>Labs</th>
<th>Working with Processes</th>
<th>Job Scheduling</th>
<th>Creating Storage Pools and Volumes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab</td>
<td>13 steps</td>
<td>Lab</td>
<td>12 steps</td>
</tr>
<tr>
<td>Learn about working with processes, such as nice/renice, ps and kill, as you practice in the Linux Cyber Range.</td>
<td>Learn about job scheduling as you practice in the Linux Cyber Range.</td>
<td>Learn about creating storage pools and volumes as you practice in the Linux Cyber Range.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
</tr>
<tr>
<td>S0067, S0158, S0267</td>
<td>S0067, S0158, S0267</td>
<td>S0067, S0158, S0267</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labs</th>
<th>Working with Logical Volume Manager</th>
<th>Understanding and Managing SELinux</th>
<th>TCP Wrappers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab</td>
<td>31 steps</td>
<td>Lab</td>
<td>21 steps</td>
</tr>
<tr>
<td>Learn about the Logical Volume Manager (LVM) as you practice in the Linux Cyber Range.</td>
<td>Gain insight into managing SELinux as you practice in the Linux Cyber Range.</td>
<td>Explore TCP wrappers as you practice in the Linux Cyber Range.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
</tr>
<tr>
<td>S0067, S0158, S0267</td>
<td>S0007, S0067, S0158, S0267</td>
<td>S0067, S0158, S0267</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labs</th>
<th>Managing Packages with Yum</th>
<th>Managing Packages with RPM</th>
<th>Understanding Linux Kernel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab</td>
<td>18 steps</td>
<td>Lab</td>
<td>22 steps</td>
</tr>
<tr>
<td>Learn about managing packages with Yum as you practice in the Linux Cyber Range.</td>
<td>Learn about managing packages with RPM as you practice in the Linux Cyber Range.</td>
<td>Learn about Linux kernel as you practice in the Linux Cyber Range.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
</tr>
<tr>
<td>S0067, S0158, S0267</td>
<td>S0067, S0158, S0267</td>
<td>S0067, S0158, S0267</td>
<td></td>
</tr>
</tbody>
</table>
Creating and Managing Extended File Systems

Lab | 33 steps

Learn about creating and managing extended file systems as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

Managing Firewall

Lab | 33 steps

Learn about managing firewalls, including iptables and firewalld, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0084, S0158, S0267

Managing Units and Control Groups

Lab | 29 steps

Learn about managing units and control groups, including systemctl, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

Working with XFS and VFAT File Systems

Lab | 25 steps

Learn about working with XFS and VFAT (Virtual File Allocation Table) file systems as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

System Logging

Lab | 17 steps

Learn about system logging, including syslog, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

Using Swap

Lab | 11 steps

Learn about using swap as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

Access Control Lists

Lab | 15 steps

Learn about access control lists (ACL), including file and directory ACLs, and default ACLs, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:
S0007, S0067, S0158, S0267
MITRE ATT&CK® Reconnaissance

HANDS-ON TRAINING

This cyber range will help you learn the reconnaissance tactics outlined in the MITRE ATT&CK framework. Reconnaissance is the act of gathering information about a system or target before an attack.

**Building a Target Profile**

Lab | 15 steps

This lab entails a series of Mitre ATT&CK techniques and sub-techniques with the aim of creating a detailed profile, which includes organization, infrastructure, and human resource mapping.

**Website Enumeration**

Lab | 18 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how website enumeration can discover resources and underlying technology that the webserver is using.

**Extracting Information from Routers and Access Points**

Lab | 18 steps

This lab entails a series of Mitre ATT&CK techniques and sub-techniques to learn how routers and access points can be targeted and enumerated.

**Forwarding Host Traffic to the Router**

Lab | 18 steps

Routers are networking devices that perform the traffic directing functions between computer networks. If adversaries gain access to these devices, an entirely internal network structure is compromised. Different attack vectors exist for exploiting these devices, allowing adversaries to gain higher access by port forwarding between machines.

**Mapping DNS Information**

Lab | 19 steps

This lab entails a series of Mitre ATT&CK techniques and sub-techniques with the aim of showcasing the possibility of intertwinement between them.

**Planning a Spearphishing Attack**

Lab | 10 steps

This lab entails a series of Mitre ATT&CK techniques and sub-techniques to identify and bypass security mechanisms to extract server information and plan a spearphishing attack.
Scanning Techniques

Lab | 13 steps

This lab will focus on teaching students to map the network structure by probing the active hosts via network traffic. The lab covers scenarios of false-positive results, packet crafting, and stealthy scanning.
MITRE ATT&CK® Resource Development

This cyber range will help you learn the resource development tactics outlined in the MITRE ATT&CK framework. Resource development involves techniques of creating, buying, stealing, or compromising resources to carry out an attack.

### HANDS-ON TRAINING

<table>
<thead>
<tr>
<th>Lab</th>
<th>Title</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building Custom Tools</td>
<td>Lab</td>
<td>15</td>
</tr>
<tr>
<td>Compromising Accounts</td>
<td>Lab</td>
<td>18</td>
</tr>
<tr>
<td>Drive-by Scenarios</td>
<td>Lab</td>
<td>20</td>
</tr>
<tr>
<td>Establishing Accounts</td>
<td>Lab</td>
<td>22</td>
</tr>
<tr>
<td>Malicious APK</td>
<td>Lab</td>
<td>20</td>
</tr>
<tr>
<td>Malicious Linux Packages</td>
<td>Lab</td>
<td>20</td>
</tr>
</tbody>
</table>

- **Building Custom Tools**
  Understanding how tools are built allow a user to modify those tools to their needs or create new tools for the task at hand. This lab teaches the user to re-create the functionality of known tools such as Nmap and Netcat as well as tools that can be used for enumeration and vulnerability scanning.

- **Compromising Accounts**
  In some cases, the compromise of computer accounts can be caused by simple information leakage or profiling techniques, which give attackers the possibility to break in.

- **Drive-by Scenarios**
  This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show several drive-by attack scenarios and learn how to identify them.

- **Establishing Accounts**
  This lab incorporates a series of Mitre ATT&CK techniques and sub techniques to identify and access website resources that could contain information of value. That information will be used to compromise accounts and establish access to target servers.

- **Malicious APK**
  Android Package (APK) is the Android application package file format. This package is used by the Android operating system and many other Android-based operating systems to distribute and install mobile apps, mobile games, and middleware.

- **Malicious Linux Packages**
  Learn how adversaries usually exploit Debian-based systems by creating malicious repositories for the APT packet manager and distributing them to the victims.
### Python-based Command and Control server

Lab | 19 steps
---
This lab shows how to develop a stable Python-based Command and Control Server using the socket library and creating a reusable script which can be converted into an executable to be run on different targets.

### Python-based Keylogger

Lab | 21 steps
---
Learn and create a Python-based keylogger utilizing Object-oriented programming principles to email the keystrokes to the user using a mail server as the information gathering unit.

### Web-based Command and Control Server

Lab | 19 steps
---
This lab entails a series of Mitre ATT&CK techniques and sub-techniques with the aim of learning how a compromised web server can be used as a Command and Control server to launch attacks to other targets.

### Webshells

Lab | 18 steps
---
In this lab, the student learns to develop and stage several webshells and how to determine which webshell should be uploaded to a web server. The compromised infrastructure is then used to deploy drive-by attacks.

### Stored Firefox Credentials

Lab | 15 steps
---
This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how they can be intertwined to steal saved credentials from firefox.
# MITRE ATT&CK® Initial Access

This cyber range will help you learn the initial access tactics outlined in the MITRE ATT&CK framework. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network.

## Drive-by Compromise

**Lab | 22 steps**

Learn how drive-by Compromise attacks rely on vulnerable users (targets) visiting the infected commonly used websites through which adversaries host malware.

## Broken Access Control

**Lab | 23 steps**

Broken Access Control is one of the most encountered security issues in web applications. This lab will show different versions and exploitation scenarios for this set of security issues.

## Exploiting Web Apps

**Lab | 22 steps**

In this lab you will complete challenges and learn about Padding Oracle Attacks, Server Side Template Injection, Union-based SQLi, Blind SQLi, and Use of a One Way Hash with a Predictable Salt.

## Exploiting Public-Facing Applications

**Lab | 18 steps**

Learn how applications are often connected to databases, standard services (such as SMB or SSH), and other applications with internet-accessible open sockets (such as web servers).

## Rubber Ducky & Bash Bunny

**Lab | 26 steps**

Learn how a malicious actor can use the rubber ducky to inject keystrokes into a system, hack a system, steal credentials, etc.

## Log4j

**Lab | 26 steps**

The Apache Log4j versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack. Get hands-on experience with controlling log messages or log message parameters to execute arbitrary code loaded from LDAP servers.
Valid Accounts

Lab | 21 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to whos how adversaries can obtain and abuse credentials of existing accounts to gain Initial Access, Persistence, Privilege Escalation or Defense Evasion.

Heartbleed

Lab | 18 steps

In this lab, you’ll get hands-on experience compromising secret keys used to identify the service providers and encrypt the traffic, the names and passwords of the users, and the actual content.

Initial Access - CTF

Lab | 25 steps

Exploit a vulnerable Webmin application in order to attach a code snippet to a software product which is used to establish a remote connection.
**MITRE ATT&CK® Execution**

HANDS-ON TRAINING

This cyber range will help you learn the execution tactics outlined in the MITRE ATT&CK framework. Execution consists of techniques that result in adversary-controlled code running on a local or remote system.

<table>
<thead>
<tr>
<th>Language</th>
<th>Lab</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PowerShell</strong></td>
<td>Lab</td>
<td>22</td>
</tr>
<tr>
<td>This lab will cover the basics of PowerShell and later on address scripting, command execution, and resource building utilizing this robust framework.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Unix Shell</strong></td>
<td>Lab</td>
<td>25</td>
</tr>
<tr>
<td>Learn how adversaries may abuse command and script interpreters to execute commands, scripts, or binaries.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Visual Basic</strong></td>
<td>Lab</td>
<td>42</td>
</tr>
<tr>
<td>This lab incorporates a series of Mitre ATT&amp;CK techniques and sub-techniques to show how adversaries can abuse Visual Basic for execution.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Python</strong></td>
<td>Lab</td>
<td>23</td>
</tr>
<tr>
<td>Python is a prevalent scripting/programming language with capabilities to perform many functions. Get hands-on experience using Python libraries to download and execute commands to perform malicious behaviors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>JavaScript</strong></td>
<td>Lab</td>
<td>23</td>
</tr>
<tr>
<td>Learn how adversaries abuse various implementations of JavaScript to execute various behaviors, such as hosting malicious scripts on websites or downloading and executing these scripts files as secondary payloads.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Macros</strong></td>
<td>Lab</td>
<td>19</td>
</tr>
<tr>
<td>This lab incorporates a series of Mitre ATT&amp;CK techniques and sub-techniques to show how documents that leverage macros exploit capabilities that are provided by Microsoft Office or Libre Office for Linux Systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Labs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>User Execution</strong></td>
<td><strong>Exploitation for Client Execution</strong></td>
<td><strong>Execution - CTF</strong></td>
</tr>
<tr>
<td>Lab</td>
<td>23 steps</td>
<td>Lab</td>
</tr>
<tr>
<td>This lab incorporates a series of Mitre ATT&amp;CK techniques and sub techniques to show how victims can be subjected to social engineering to get them to execute malicious code.</td>
<td>This lab incorporates a series of Mitre ATT&amp;CK techniques and sub techniques to show how adversaries may exploit software vulnerabilities in client applications to execute code.</td>
<td>This CTF highlights the range of possibilities attackers can choose from when planning to compromise a target. You will learn how to use Initial Access techniques in order to plan and orchestrate stealthy and persistent attacks.</td>
</tr>
</tbody>
</table>
## MITRE ATT&CK® Persistence

This cyber range will help you learn the persistence tactics outlined in the MITRE ATT&CK framework.

### Traffic Signaling and Pre-OS Boot Lab

- **Lab** | 19 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how adversaries may use port knocking to hide open ports used for persistence and how adversaries may load a modified router configuration file from a Trivial File Transfer Protocol (TFTP) server.

### Compromise Client Software Binary Lab

- **Lab** | 18 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how adversaries modified the OpenSSH binaries to establish persistent access to systems.

### Authentication Process Modification Lab

- **Lab** | 24 steps

Learn how to alter authentication processes to gain access to user credentials and allow unwarranted access to accounts.

### Maintaining Connections Lab

- **Lab** | 18 steps

The lab will showcase how different binaries and programming languages can be used to maintain persistent connections with the target machine.

### Browser Extensions Lab

- **Lab** | 25 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how adversaries may abuse Internet browser extensions to establish persistent access to victim systems.
# MITRE ATT&CK® Privilege Escalation

This cyber range will help you learn the privilege escalation tactics outlined in the MITRE ATT&CK framework.

## Library Hijacking and Shared Libraries

**Lab | 25 steps**

Get hands-on experience with privilege escalation techniques through library hijacking and shared resources for different programming languages.

## Privilege Escalation Tools and Scripts

**Lab | 20 steps**

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how adversaries may use tools and scripts to escalate their privileges.

## Checklist and Commands

**Lab | 24 steps**

The lab highlights important Linux features, processes, and applications that can be exploited for privilege escalation and showcases best practices to protect these resources.

## Exploitation For Privilege Escalation - Applications

**Lab | 16 steps**

This lab highlights when the adversary benefits from a programming error in a program, service, or kernel to execute malicious code.

## Scheduled Tasks

**Lab | 19 steps**

This lab shows how task scheduling utilities can be used to run system commands on specific dates and times.
Network Traffic Analysis Cyber Range

HANDS-ON TRAINING

Gain useful skills related to analyzing network traffic as you work with Terminal Shark (TShark), Scapy and other tools to identify common network protocols, examine malware communications, extract transmitted files, filter output to display specific information, view communication statistics and much more.

---

**Introduction to Terminal Shark**

Lab | 15 steps

Terminal Shark, or TShark, is the command-line version of Wireshark, which is a commonly-used tool for network traffic analysis. This lab is designed to provide an introduction to Terminal Shark, including some of the most common command flags and uses.

NICE Knowledge and Skill Statements:
S0046, S0267

---

**Traffic Replay and Live Traffic Analysis in TShark**

Lab | 12 steps

This lab explores some of the options available when performing live traffic analysis with Terminal Shark (TShark).

NICE Knowledge and Skill Statements:
S0046, S0046, S0120, S0156, S0199, S0221

---

**Extracting Files from Traffic Samples in TShark**

Lab | 14 steps

Traffic captures commonly include files that are of interest to incident responders. This lab explores methods of extracting files from network traffic using Terminal Shark (or TShark).

NICE Knowledge and Skill Statements:
S0046, S0120, S0156, S0199, S0221

---

**Decrypting SSL and TLS in TShark**

Lab | 14 steps

Over half of all Internet traffic is encrypted, and malware makes heavy use of encryption to hide malicious content among legitimate traffic. In this lab, we will decrypt traffic encrypted with SSL and TLS using Terminal Shark.

NICE Knowledge and Skill Statements:
S0046, S0120, S0156, S0199, S0221

---

**TShark and Command Line**

Lab | 12 steps

Explore how Terminal Shark can be combined with Linux Terminal commands for network monitoring.

NICE Knowledge and Skill Statements:
S0046, S0120, S0156, S0199, S0221

---

**Decoding and Decrypting Network Traffic Data**

Lab | 13 steps

This lab demonstrates how to identify and reverse various encoding and encryption algorithms commonly used to obfuscate malware command and control traffic.

NICE Knowledge and Skill Statements:
S0046, S0120, S0156, S0199, S0221
### Identifying Abnormal Traffic

**Lab | 12 steps**

Malware authors and other cybercriminals will often misuse legitimate protocols for command and control. This lab explores some of the ways that this can be accomplished.

**NICE Knowledge and Skill Statements:**
S0046, S0120, S0156, S0199, S0221, S0258

### Scapy for Network Traffic Analysis

**Lab | 15 steps**

Scapy is a Python library for performing network traffic analysis. Using Scapy, it is possible to easily view, manipulate and write scripts using packet data.

**NICE Knowledge and Skill Statements:**
S0046, S0120, S0156, S0199, S0221

### Traffic Generation with Scapy

**Lab | 16 steps**

The purpose of this lab is to explore the use of Scapy for building fake packets, which can be used for a variety of different purposes.

**NICE Knowledge and Skill Statements:**
S0046, S0120, S0156, S0199, S0221

### Leaked Credential Extraction

**Lab | 13 steps**

Many commonly-used network protocols were not designed to be secure by default. This lab demonstrates how these credentials can be identified and extracted.

**NICE Knowledge and Skill Statements:**
S0046, S0156, S0199, S0221, S0267
Networking Cyber Range

BUILD YOUR SKILLS AS YOU PROGRESS THROUGH LABS COVERING A WIDE RANGE OF NETWORKING TOPICS, INCLUDING SWITCHES AND ROUTERS, NETWORKING PROTOCOLS, CONFIGURING AND VERIFYING DIFFERENT NETWORKING DEVICES, AND TROUBLESHOOTING ISSUES. YOU'LL ALSO PERFORM SEVERAL LABS DESIGNED TO VALIDATE YOUR VLAN AND NETWORK MANAGEMENT SKILLS.

### Network Data Collection

**Lab | 17 steps**

Learn how to use existing and custom honeyboxes and other tools to collect network traffic for further analysis.

**NICE Knowledge and Skill Statements:**

S0046, S0051, S0120, S0156, S0199, S0221

### Connection Analysis

**Lab | 17 steps**

Understand connection analysis and what data can be extracted from high-level network traffic data.

**NICE Knowledge and Skill Statements:**

S0046, S0120, S0156, S0199, S0221

### Switch Learning

**Lab | 12 steps**

Discover how switches learn MAC addresses and gain hands-on experience as you practice in the Networking Cyber Range.

**NICE Knowledge and Skill Statements:**

S0041, S0067, S0275

### VLAN Lab 1

**Lab | 53 steps**

Learn how to configure VLANs on Cisco switches as you practice in the Networking Cyber Range.

**NICE Knowledge and Skill Statements:**

S097

### Switch Simlet

**Lab | 24 steps**

Learn about a switch simlet as you practice in the Networking Cyber Range.

**NICE Knowledge and Skill Statements:**

S0041, S0067, S0275

### STP Configuration and Verification

**Lab | 39 steps**

Explore STP configuration and verification as you practice in the Networking Cyber Range.

**NICE Knowledge and Skill Statements:**

S0041, S0067, S0275
<table>
<thead>
<tr>
<th>Lab Title</th>
<th>Steps</th>
<th>NICE Knowledge and Skill Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction to IP Routing</strong></td>
<td>35 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>Basic Router Configuration</strong></td>
<td>56 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>Basic Router Interface Configuration</strong></td>
<td>29 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>VLAN Lab 2 - ROAS</strong></td>
<td>35 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>Routing: Basic OSPF</strong></td>
<td>31 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>OSPF Troubleshooting Examples</strong></td>
<td>34 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>Troubleshoot &amp; Resolve Routing Issues - OSPF</strong></td>
<td>30 steps</td>
<td>S0041, S0067, S0151, S0275</td>
</tr>
<tr>
<td><strong>OSPF Area Types</strong></td>
<td>19 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>Configuring EIGRP</strong></td>
<td>48 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td>Topic</td>
<td>Lab</td>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----</td>
<td>----------------------------------</td>
</tr>
<tr>
<td><strong>EIGRP Configuration and Verification</strong></td>
<td>30 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>EIGRP Simulation</strong></td>
<td>33 steps</td>
<td>S0041, S0067, S0151, S0275</td>
</tr>
<tr>
<td><strong>GRE Tunnels Configuration and Verification</strong></td>
<td>25 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>Introduction to DMVPN</strong></td>
<td>15 steps</td>
<td>S0041, S0067, S097, S0275</td>
</tr>
<tr>
<td><strong>Configuring PPP</strong></td>
<td>68 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>MPLS Layer VPN AToM</strong></td>
<td>15 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>Introduction to MPLS Layer 3 VPN</strong></td>
<td>17 steps</td>
<td>S0041, S0067, S097, S0275</td>
</tr>
<tr>
<td><strong>BGP Weight, Local Preference and MED</strong></td>
<td>22 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
<tr>
<td><strong>HSRP Configuration and Verification</strong></td>
<td>22 steps</td>
<td>S0041, S0067, S0275</td>
</tr>
</tbody>
</table>
Labs

GET STARTED
Use code "learnskills" to get 30 days for $1

Table of contents
Boot camps
Self-paced training
Learning paths
Labs
Projects
NICE mapping
Appendix

GRE-PPP-EIGRP Troubleshooting

Lab | 33 steps

Learn about GRE-PPP-EIGRP troubleshooting as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:
S0041, S0067, S0151, S0275

GLBP Configuration and Verification

Lab | 26 steps

Learn about GLBP configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:
S0041, S0067, S0275

Cisco IOS - Basic Traffic Shaping and Policing

Lab | 31 steps

Explore the basics of traffic shaping and traffic policing on a Cisco IOS router as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:
S0041, S0067, S097, S0275

Quality of Service Configuration and Verification

Lab | 32 steps

Learn about quality of service configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:
S0041, S0067, S0275

DHCP Server Configuration and Verification

Lab | 34 steps

Explore DHCP server configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:
S0041, S0067, S0275

Basic Network Address Translation

Lab | 28 steps

Learn the basics of NAT (Network Address Translation) as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:
S0041, S0067, S0275

Basic Access Control Lists

Lab | 29 steps

Explore standard numbered and named ACLs (access control lists) as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:
S0007, S0041, S0067, S0097, S0275

Basic ACL Configuration

Lab | 30 steps

Learn about configuring basic access-list with deny and permit statements as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:
S0041, S0067, S0275

Advanced ACL Configuration

Lab | 30 steps

Learn about extended ACLs (access control lists) as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:
S0007, S0041, S0067, S0097, S0275
<table>
<thead>
<tr>
<th>Labs</th>
<th>40 steps</th>
<th>Syslog, Telnet, SSH and Banners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab</td>
<td>Explore four different tools available on your Cisco router's IOS as you practice in the Networking Cyber Range.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>S0041, S0067, S0275</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labs</th>
<th>33 steps</th>
<th>Network Management Lab 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab</td>
<td>Learn about network management on Cisco devices, including logging and SNMP, as you practice in the Networking Cyber Range.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>S0275</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labs</th>
<th>27 steps</th>
<th>Network Management Lab 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab</td>
<td>Learn how to configure Internet Control Message Protocol (ICMP) echo-based IP Service Level Agreements (SLAs) as you practice in the Networking Cyber Range.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>S0041, S0275</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labs</th>
<th>23 steps</th>
<th>Cisco TCP Intercept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab</td>
<td>Learn about using the Cisco TCP intercept feature to protect against DoS and DDoS attacks as you practice in the Networking Cyber Range.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>S0041, S0067, S0097, S0275</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labs</th>
<th>33 steps</th>
<th>RIP-V2 Simulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab</td>
<td>Learn about RIP-V2 as you practice in the Networking Cyber Range.</td>
<td></td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td>S0041, S0067, S0275</td>
<td></td>
</tr>
</tbody>
</table>
Penetration Testing Cyber Range

Build your skills as you progress through labs covering a wide range of pentesting topics, including abusing protocols, scanning for vulnerabilities, identifying exploits and delivering payloads, and more. You'll also perform several Capture the Flag (CTF) exercises designed to validate your new pentesting skills.

Linux Fundamentals

Lab | 23 steps
Explore the fundamentals of Linux and gain hands-on experience via the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:
- S0267

Abusing DNS

Lab | 10 steps
Learn about gathering information from DNS records as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:
- S0295

Abusing SNMP

Lab | 10 steps
Learn about getting information from SNMP as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:
- S0051

Wi-Fi Pentesting

Lab | 4 steps
Learn about cracking WEP and WPA2 keys as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:
- S0051

Port and Protocol Scanning with Nmap

Lab | 13 steps
Get familiar with the process of port scanning using Nmap as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:
- S0051

TCP/IP for Hackers

Lab | 21 steps
Learn about using TCP/IP for pentesting as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:
- S0051
<table>
<thead>
<tr>
<th>Labs</th>
<th>Title</th>
<th>Description</th>
<th>NICE Knowledge and Skill Statements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Discovery</td>
<td>Lab</td>
<td>9 steps</td>
<td>Explore finding active hosts on a network as you practice in the Penetration Testing Cyber Range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N0051</td>
</tr>
<tr>
<td>Steady Network Reconnaissance</td>
<td>Lab</td>
<td>19 steps</td>
<td>Learn stealthy scanning techniques with Nmap as you practice in the Penetration Testing Cyber Range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N0051</td>
</tr>
<tr>
<td>Advanced Scanning with Nmap</td>
<td>Lab</td>
<td>7 steps</td>
<td>Hone your Nmap skills as you practice in the Penetration Testing Cyber Range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N0051</td>
</tr>
<tr>
<td>Scanning with Mobile Devices</td>
<td>Lab</td>
<td>8 steps</td>
<td>Learn about running network scans from Android as you practice in the Penetration Testing Cyber Range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N0051</td>
</tr>
<tr>
<td>Sniffing</td>
<td>Lab</td>
<td>18 steps</td>
<td>Discover why few things top having raw access to network traffic as you practice in the Penetration Testing Cyber Range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N0051</td>
</tr>
<tr>
<td>Service Identification</td>
<td>Lab</td>
<td>8 steps</td>
<td>Learn about service identification as you practice in the Penetration Testing Cyber Range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N0051</td>
</tr>
<tr>
<td>CTF 1: DNS and SNMP Reconnaissance</td>
<td>Lab</td>
<td>4 steps</td>
<td>Test your DNS and SNMP reconnaissance skills as you practice in the Penetration Testing Cyber Range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N0051</td>
</tr>
<tr>
<td>Hacking with Android</td>
<td>Lab</td>
<td>9 steps</td>
<td>Learn about launching a remote exploit from an Android device as you practice in the Penetration Testing Cyber Range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N0051</td>
</tr>
<tr>
<td>Credential Harvesting with SET</td>
<td>Lab</td>
<td>14 steps</td>
<td>Learn about stealing passwords as you practice in the Penetration Testing Cyber Range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N0051</td>
</tr>
<tr>
<td>Lab Title</td>
<td>Steps</td>
<td>NICE Knowledge and Skill Statements</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------</td>
<td>-------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Spearphishing</strong></td>
<td>12</td>
<td>S0051</td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td>Explore compromising a system via malicious email as you practice in the Penetration Testing Cyber Range.</td>
<td></td>
</tr>
<tr>
<td><strong>Web App Hacking</strong></td>
<td>26</td>
<td>S0051</td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td>Gain experience with web application hacking as you practice in the Penetration Testing Cyber Range.</td>
<td></td>
</tr>
<tr>
<td><strong>Server Side Exploit</strong></td>
<td>12</td>
<td>S0051</td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td>Learn how to exploit a web server vulnerability as you practice in the Penetration Testing Cyber Range.</td>
<td></td>
</tr>
<tr>
<td><strong>CTF 2: Attacking FTP</strong></td>
<td>4</td>
<td>S0051</td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td>Test your sniffing and password cracking skills as you practice in the Penetration Testing Cyber Range.</td>
<td></td>
</tr>
<tr>
<td><strong>Vulnerability Identification</strong></td>
<td>12</td>
<td>S0051</td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td>Learn about vulnerability identification as you practice in the Penetration Testing Cyber Range.</td>
<td></td>
</tr>
<tr>
<td><strong>Basic SQL Injection</strong></td>
<td>26</td>
<td>S0051</td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td>Discover how to exploit an SQL injection vulnerability as you practice in the Penetration Testing Cyber Range.</td>
<td></td>
</tr>
<tr>
<td><strong>Heartbleed Exploitation</strong></td>
<td>10</td>
<td>S0051</td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td>Learn how to exploit the Heartbleed (OpenSSL) vulnerability as you practice in the Penetration Testing Cyber Range.</td>
<td></td>
</tr>
<tr>
<td><strong>Exploiting Vulnerable Services</strong></td>
<td>15</td>
<td>S0051</td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td>Learn about gaining access to a remote systems as you practice in the Penetration Testing Cyber Range.</td>
<td></td>
</tr>
<tr>
<td><strong>CTF 3: Web Application Exploitation</strong></td>
<td>4</td>
<td>S0051</td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab</td>
<td></td>
<td>Test your web application hacking skills as you practice in the Penetration Testing Cyber Range.</td>
<td></td>
</tr>
<tr>
<td>Labs</td>
<td>Table of contents</td>
<td>Boot camps</td>
<td>Self-paced training</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>

### Labs

<table>
<thead>
<tr>
<th>Lab Name</th>
<th>Steps</th>
<th>Description</th>
<th>NICE Knowledge and Skill Statements:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SQL Injection Chained Exploitation</strong></td>
<td>11 steps</td>
<td>Explore combining SQL injection attacks as you practice in the Penetration Testing Cyber Range.</td>
<td>S0051</td>
</tr>
<tr>
<td><strong>Shellschok Exploitation</strong></td>
<td>11 steps</td>
<td>Learn about exploiting the Shellshock (GNU Bash) vulnerability as you practice in the Penetration Testing Cyber Range.</td>
<td>S0051</td>
</tr>
<tr>
<td><strong>Additional Payloads</strong></td>
<td>24 steps</td>
<td>Explore Metasploit payload options as you practice in the Penetration Testing Cyber Range.</td>
<td>S0051</td>
</tr>
<tr>
<td><strong>Android Exploitation</strong></td>
<td>17 steps</td>
<td>Learn about accessing Android devices remotely as you practice in the Penetration Testing Cyber Range.</td>
<td>S0051</td>
</tr>
<tr>
<td><strong>Client Side Exploits</strong></td>
<td>14 steps</td>
<td>Carry out an example of a client side exploit as you practice in the Penetration Testing Cyber Range.</td>
<td>S0051</td>
</tr>
<tr>
<td><strong>Using Ncat as a Trojan</strong></td>
<td>13 steps</td>
<td>Discover how to maintain access to compromised system with Ncat as you practice in the Penetration Testing Cyber Range.</td>
<td>S0051</td>
</tr>
<tr>
<td><strong>Post-Exploit Password Cracking</strong></td>
<td>12 steps</td>
<td>Learn about cracking hashed passwords gathered from a compromised system as you practice in the Penetration Testing Cyber Range.</td>
<td>S0051</td>
</tr>
<tr>
<td><strong>Covert Channels/Evasion</strong></td>
<td>25 steps</td>
<td>Learn about using encryption for covert communications and IDS evasion as you practice in the Penetration Testing Cyber Range.</td>
<td>S0051</td>
</tr>
<tr>
<td><strong>Intrusion Detection with Snort</strong></td>
<td>24 steps</td>
<td>Get an overview of using intrusion detection with Snort as you practice in the Penetration Testing Cyber Range.</td>
<td>S0025</td>
</tr>
</tbody>
</table>

Use code "learnskills" to get 30 days for $1

GET STARTED
CTF 4: Privilege Escalation

Lab | 3 steps

Test your privilege escalation skills as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:
S0051
# Python Code Security Cyber Range

Build and reinforce your skills as you progress through labs covering a wide range of Python code security topics, including using Bandit, PyT and other tools to find common security issues in Python code, perform taint and control flow analysis, and recognize vulnerabilities that can lead to common application attacks.

## Table of contents
- NICE mapping
- Boot camps
- Learning paths
- Labs
- Projects
- NICE mapping
- Appendix

## Labs

<table>
<thead>
<tr>
<th>Introduction to Python Bandit</th>
<th>Introduction to Python Control Flow Analysis</th>
<th>Command Injection in Python</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lab</strong></td>
<td>13 steps</td>
<td><strong>Lab</strong></td>
</tr>
<tr>
<td>Python bandit is one of the most commonly used Python linters and static analysis tools. This lab introduces the use of bandit for analysis of Python code.</td>
<td>Control flow analysis is useful for identifying mistakes or unexpected flows in a program. This lab demonstrates the use of staticfg for control flow analysis in Python.</td>
<td>A command injection vulnerability enables an attacker to run malicious code on the system where an application is running. This lab demonstrates how to identify, exploit and mitigate these vulnerabilities in Python.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>S0174</td>
<td>S0174</td>
<td>S0174</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>XPath Injection in Python</th>
<th>XML Attacks in Python</th>
<th>Race Conditions in Python</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lab</strong></td>
<td>15 steps</td>
<td><strong>Lab</strong></td>
</tr>
<tr>
<td>XPath is a programming language for extracting data from XML files; however, it is vulnerable to injection attacks. This lab demonstrates vulnerable code and how to exploit and remediate it.</td>
<td>XML is a useful method for storing structured data, but code parsing it can be vulnerable to a number of attacks. This lab demonstrates some of the ways that different XML parsing functions can be exploited in Python.</td>
<td>Race condition vulnerabilities exist when the proper operation of a program depends upon operations being run sequentially back-to-back. This lab demonstrates how to identify, exploit and remediate these vulnerabilities.</td>
</tr>
<tr>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
<td><strong>NICE Knowledge and Skill Statements:</strong></td>
</tr>
<tr>
<td>S0172</td>
<td>S0172</td>
<td>S0172</td>
</tr>
</tbody>
</table>
Cross-Site Scripting in Python

Lab | 16 steps

Cross-site-scripting (XSS) is one of the most common web application vulnerabilities in existence. This lab demonstrates how to identify, exploit and remediate XSS vulnerabilities in Flask web applications.

NICE Knowledge and Skill Statements: S0172

Cross-Site Request Forgery in Python

Lab | 11 steps

CSRF vulnerabilities allow an attacker to force unauthorized actions to be taken on an authenticated user's account. This lab demonstrates how to identify, exploit and remediate these vulnerabilities in Python code.

NICE Knowledge and Skill Statements: S0174

Supply Chain Vulnerabilities in Python

Lab | 12 steps

Very few applications are designed to be completely standalone, and a program's dependencies can introduce vulnerabilities. This lab demonstrates the use of tools for identifying potential supply chain vulnerabilities in Python programs.

NICE Knowledge and Skill Statements: S0174

Unsafe Deserialization in Python

Lab | 14 steps

Serialization is helpful for making Python objects and data writable to files and transferrable over the network. Learn how some serialization options can be vulnerable to exploitation in Python and how to securely serialize data.

NICE Knowledge and Skill Statements: S0172
# RHCSA Cyber Range

This cyber range allows you to practice tasks covered in the Red Hat Certified System Administrator (RHCSA) exam objectives.

## Basic Commands and Help

**Lab | 20 steps**

Learn basic RHEL commands and gain hands-on experience as you practice in the RHCSA Cyber Range.

**NICE Knowledge and Skill Statements:**
S0267

## Login History and Information

**Lab | 11 steps**

In this lab, you will work with common commands that display information about the system’s users and groups as well as other system information, including uptime and kernel information.

**NICE Knowledge and Skill Statements:**
S0067, S0267

## Compression and Archiving

**Lab | 18 steps**

Explore compressing and archiving tools, such as gzip, gunzip, bzip2, bunzip2 and tar, as you practice in the RHCSA Cyber Range.

**NICE Knowledge and Skill Statements:**
S0067, S0158, S0267

## Using vi

**Lab | 7 steps**

Learn about the visual editor as you practice in the RHCSA Cyber Range.

**NICE Knowledge and Skill Statements:**
S0067, S0158, S0267

## File Path and File Types

**Lab | 12 steps**

Learn about file paths and types as you practice in the RHCSA Cyber Range.

**NICE Knowledge and Skill Statements:**
S0067, S0158, S0267

## File and Directory Operations

**Lab | 19 steps**

Learn about file and directory operations as you practice in the Linux Cyber Range.

**NICE Knowledge and Skill Statements:**
S0067, S0158, S0267
Finding and Linking Files
Lab | 13 steps
This lab explores different options for finding files on RHEL systems, based on various criteria, such as size and permissions, and walks through the process of creating soft and hard links.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

File and Directory Permissions
Lab | 18 steps
Learn about file and directory permissions as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

Special Permissions
Lab | 16 steps
Learn about special permissions as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

Access Control Lists
Lab | 15 steps
Learn about access control lists (ACL), including file and directory ACLs, and default ACLs, as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:
S0007, S0067, S0158, S0267

Managing Users
Lab | 24 steps
Practice managing user accounts on RHEL systems, including creating, deleting, and setting passwords.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

Managing Groups
Lab | 13 steps
Practice creating, managing, and deleting group accounts on RHEL systems in this lab.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

Bash Shell
Lab | 18 steps
Learn about the Bash Shell as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267

Regular Expressions & Metacharacters
Lab | 19 steps
Learn about regular expressions and metacharacters as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:
S0267

Working with Processes and Jobs
Lab | 18 steps
Practice common commands for working with processes, such as top, nice/renice, ps and kill, and manage jobs with bg and fg.

NICE Knowledge and Skill Statements:
S0067, S0158, S0267
Job Scheduling

Lab | 12 steps
Learn about job scheduling as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements: S0067, S0158, S0267

Managing packages with rpm

Lab | 22 steps
Learn about managing packages with RPM as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements: S0067, S0158, S0267

Managing packages with DNF

Lab | 13 steps
In this lab, you will practice working with DNF, or “Dandified yum”. It is the next generation of the yum package manager that automatically computes dependencies and makes it easier to maintain groups of machines.

NICE Knowledge and Skill Statements: S0067, S0158, S0267

Managing Application Stream Modules

Lab | 10 steps
In this lab, you will practice working with DNF package manager to look up and manipulate application stream (AppStream) modules.

NICE Knowledge and Skill Statements: S0067, S0158, S0267

Understanding Linux Kernel

Lab | 12 steps
Learn about the Linux kernel as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements: S0067, S0158, S0267

Managing Units & System Tuning

Lab | 33 steps
Practice working with systemd to manage units and control groups, and explore tuned, a system tuning service available in RHEL.

NICE Knowledge and Skill Statements: S0067, S0158, S0267

System Logging

Lab | 17 steps
Learn about system logging, including rsyslog, as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements: S0067, S0158, S0267

Creating and Managing Partitions

Lab | 25 steps
Learn about creating and managing partitions as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements: S0067, S0158, S0267

Storage Optimization with VDO

Lab | 10 steps
Virtual Data Optimizer (VDO) is one of the newer RHEL features, which allows conserving disk space, improving data throughput, and saving on storage costs. In this lab, we will install VDO and use it to create and remove a volume.

NICE Knowledge and Skill Statements: S0067, S0158, S0267
<table>
<thead>
<tr>
<th>Lab Title</th>
<th>Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working with Logical Volume Manager</td>
<td>31 steps</td>
<td>Learn about the Logical Volume Manager (LVM) as you practice in the RHCSA Cyber Range.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>S0067, S0158, S0267</td>
</tr>
<tr>
<td>Working with Stratis Filesystems</td>
<td>14 steps</td>
<td>RH EL 8 introduced a new simplified storage management solution called Stratis. In this lab, you will practice working with Stratis to create, manipulate, and destroy file systems and storage pools.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>S0067, S0158, S0267</td>
</tr>
<tr>
<td>Working with XFS</td>
<td>44 steps</td>
<td>In this lab, you will practice working with X File System (XFS), including creating, mounting, and resizing XFS file systems in VDO, LVM, and Stratis logical volumes.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>S0067, S0158, S0267</td>
</tr>
<tr>
<td>Working with Swap</td>
<td>11 steps</td>
<td>Learn about using swap as you practice in the RHCSA Cyber Range.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>S0067, S0158, S0267</td>
</tr>
<tr>
<td>Working with Remote File Systems and AutoFS</td>
<td>18 steps</td>
<td>Practice working with Network File System (NFS) service and learn how to automatically mount NFS shares with AutoFS.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>S0067, S0158, S0267</td>
</tr>
<tr>
<td>Network information and Chrony</td>
<td>16 steps</td>
<td>Learn about querying network information and about chrony as you practice in the RHCSA Cyber Range.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>S0067, S0158, S0267</td>
</tr>
<tr>
<td>Using Key Based Authentication</td>
<td>5 steps</td>
<td>Learn how to generate, distribute, and use key-based authentication for SSH.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>S0067, S0158, S0267</td>
</tr>
<tr>
<td>Managing Firewall</td>
<td>21 steps</td>
<td>Learn about managing firewalls, including firewalld, as you practice in the RHCSA Cyber Range.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>S0067, S0084, S0158, S0267</td>
</tr>
<tr>
<td>Understanding &amp; managing SELinux</td>
<td>21 steps</td>
<td>In this lab we'll take a look at some of the tools for interacting with SELinux.</td>
</tr>
<tr>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>S0067, S0121, S0158, S0267</td>
</tr>
</tbody>
</table>
SCADA Cyber Range

HANDS-ON TRAINING

Build your skills as you progress through labs covering a wide range of SCADA security topics, including reconnaissance, scanning, honeypots, attacks and exploits. You'll also perform several Capture the Flag (CTF) exercises designed to validate your new SCADA security skills.

Modbus PLC Introduction

Lab | 14 steps

Get an introduction to Modbus and gain hands-on experience via the SCADA Cyber Range.

NICE Knowledge and Skill Statements:
S0051

SNMP Reconnaissance

Lab | 17 steps

Learn about abusing SNMP as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:
S0051

Datasheet Analysis

Lab | 4 steps

Explore getting valuable information from user manuals as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:
S0268

CTF 1

Lab | 4 steps

Test your reconnaissance skills as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:
S0051

Scanning ICS/SCADA Networks

Lab | 17 steps

Learn about scanning SCADA networks as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:
S0051

Attacking the Infrastructure

Lab | 23 steps

Learn about compromising a system as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:
S0052
<table>
<thead>
<tr>
<th>Labs</th>
<th>Firewall Rules for SCADA</th>
<th>Exploiting OS-Level Vulnerabilities</th>
<th>Extracting Network Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lab</td>
<td>17 steps</td>
<td>Lab</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Get insight into SCADA firewall rules as you practice in the SCADA Cyber Range.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td></td>
<td>S0076</td>
<td></td>
<td>S0051</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labs</th>
<th>Wi-Fi Password Cracking</th>
<th>Manipulating Protocol Data</th>
<th>SCADA Honeypot</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lab</td>
<td>4 steps</td>
<td>Lab</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Learn about cracking Wi-Fi passwords as you practice in the SCADA Cyber Range.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td></td>
<td>S0051</td>
<td></td>
<td>S0051</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labs</th>
<th>Snort SCADA Rules</th>
<th>CTF 2</th>
<th>CTF 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lab</td>
<td>19 steps</td>
<td>Lab</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Learn about Snort SCADA rules as you practice in the SCADA Cyber Range.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NICE Knowledge and Skill Statements:</td>
<td></td>
<td>NICE Knowledge and Skill Statements:</td>
</tr>
<tr>
<td></td>
<td>S0025</td>
<td></td>
<td>S0051</td>
</tr>
</tbody>
</table>
Projects

Projects are a series of hands-on exercises designed to reinforce your skills and provide real-world experience. Each exercise tests the practical application of topics covered in the associated learning path. As you work through the challenges, you'll put what you learned into practice and build confidence around your new skills.

Blockchain Security Project

In this project, you'll begin by organizing information into a valid block. Then you'll answer questions related to proposed solutions to the 51% attack and performing a double-spend attack on a Proof of Stake blockchain. Finally, you'll identify smart contract vulnerabilities and the importance of binding values.

Blockchain Security Challenges

File | 1 file
Description of challenges you need to complete as part of this project.

Challenge Walkthrough Video

Video | 4 minutes
This video walks you through the project, explaining what needs to be done in each of the challenges.

Challenge Hints Video

Video | 7 minutes
This video provides useful hints to help you solve the project challenges.

Blockchain Security Challenge Solutions

File | 1 file
This document contains solutions to the project challenges.
Test your understanding of container security with this project. You will review images to reduce risk, make docker images follow best practices, and scan images for vulnerable software.

### Container Security Challenges

File | 1 file

A list of the challenges you will complete as part of this project.

**NICE Knowledge and Skill Statements:**
K0004, K0130, K0189, K0205, K0609, K0610, S0073, S0121

### Container Security Project Walkthrough

Video | 23 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

**NICE Knowledge and Skill Statements:**
K0004, K0130, K0189, K0205, K0609, K0610, S0073, S0121

### Container Security Project Hints

Video | 28 minutes

This video provides useful hints to help you solve the project challenges.

**NICE Knowledge and Skill Statements:**
K0004, K0130, K0189, K0205, K0609, K0610, S0073, S0121

### Container Security Project Solutions

File | 1 file

This document contains solutions to the project challenges.

**NICE Knowledge and Skill Statements:**
K0004, K0130, K0189, K0205, K0609, K0610, S0073, S0121
Cryptography and Cryptanalysis Project

HANDS-ON TRAINING

In this project, you’ll need to find information in encrypted network traffic, circumvent obfuscation to examine malware network communications and configuration samples, break down a hash function operation to find a specific input value and find the values of obfuscated passwords and cookies.

Project Walkthrough Video

Video | 5 minutes

An overview of the process and tasks involved in the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:
S0089, S0199, S0221, S0258

Project Files

File | 6 challenges

This downloadable .zip file contains challenges for the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:
S0089, S0199, S0221, S0258

Cryptography Challenge Questions

File | 1 file

This downloadable file contains challenge questions for the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:
S0089, S0199, S0221, S0258

Project Hints Video

Video | 5 minutes

Get hints to help you complete the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:
S0089, S0199, S0221, S0258

Challenge Questions Solutions

File | 1 file

View the solutions to the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:
S0089, S0199, S0221, S0258
Cyber Threat Hunting Project

Use your cyber threat hunting skills to identify network traffic patterns for anomalies and investigate malware. You'll use Wireshark to examine packet capture files for potential red flags. Then you'll attempt to piece together the threat. Can you identify the malware?

Cyber Threat Hunting Project Walkthrough

Video | 11 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258

Traffic Analysis Exercise

File | 1 file

This contains files you will need to complete the project.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258

Cyber Threat Hunting Challenges

File | 1 file

This contains a description of challenges you need to complete as part of this project.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258

Cyber Threat Hunting Hints

Video | 3 minutes

This video provides useful hints to help you solve the project challenges.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258

Cyber Threat Hunting Challenge Answers

File | 1 file

Check your work on the Threat Hunting project.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258
Cybersecurity Data Science Project

In this project, you’ll analyze a malware sample using classifiers provided in the project files — or with ones you build yourself. You’ll also recognize images created with deepfakes and determine text in a large number of CAPTCHA images.

Project Introduction Video

Video | 5 minutes
An overview of the process and tasks involved in the Cybersecurity Data Science Project.

NICE Knowledge and Skill Statements: S0087, S0252, S0257

Project Files

File | 5 challenges
This downloadable .zip file contains challenges for the Cybersecurity Data Science Project.

NICE Knowledge and Skill Statements: S0087, S0252, S0257

Project Hints Video

Video | 7 minutes
Get hints to help you complete the Cybersecurity Data Science Project.

NICE Knowledge and Skill Statements: S0087, S0252, S0257

Project Solutions

File | 1 file
View the solutions to the Cybersecurity Data Science Project.

NICE Knowledge and Skill Statements: S0087, S0252, S0257
ICS/SCADA Security Fundamentals Project

This project contains three parts and will require you to complete tasks across the MITRE ATT&CK for ICS Framework, the NIST Cybersecurity Framework, risk assessment activities, ICS network architecture design, Packet Capture analysis, and reviewing Intrusion Detection System alert logs.

<table>
<thead>
<tr>
<th>Project walkthrough</th>
<th>README</th>
<th>Ubuntu VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video</td>
<td>File</td>
<td>File</td>
</tr>
<tr>
<td>4 minutes</td>
<td>1 file</td>
<td>1 file</td>
</tr>
<tr>
<td>An overview of the project.</td>
<td>Instructions for the project.</td>
<td>The VM needed for this project.</td>
</tr>
</tbody>
</table>

NICE Knowledge and Skill Statements:
K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

<table>
<thead>
<tr>
<th>Project part 1 challenges</th>
<th>Project part 2 challenges</th>
<th>Project part 3 challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>File</td>
<td>File</td>
</tr>
<tr>
<td>1 file</td>
<td>1 file</td>
<td>1 file</td>
</tr>
<tr>
<td>The challenges for part 1 of the project.</td>
<td>The challenges for part 2 of the project.</td>
<td>The challenges for part 3 of the project.</td>
</tr>
</tbody>
</table>

NICE Knowledge and Skill Statements:
K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

NICE Knowledge and Skill Statements:
K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

NICE Knowledge and Skill Statements:
K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221
Project Hints

Video | 4 minutes

Some tips for completing the project.

NICE Knowledge and Skill Statements:
K0027, K0046, K0062, K0137, K0165, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project part 1 solutions

File | 1 file

The answers for part 1 of the project.

NICE Knowledge and Skill Statements:
K0027, K0046, K0062, K0137, K0165, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project part 2 solutions

File | 1 file

The answers for part 2 of the project.

NICE Knowledge and Skill Statements:
K0027, K0046, K0062, K0137, K0165, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project part 3 solutions

File | 1 file

The answers for part 3 of the project.

NICE Knowledge and Skill Statements:
K0027, K0046, K0062, K0137, K0165, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221
Incident Response Project

HANDS-ON TRAINING

Use tools like Wireshark, Zeek and Volatility to respond to real-world scenarios. You’ll investigate a “watering hole attack” that may have affected someone in the IT department and an SQL injection attack that may have led to credit card data being exfiltrated.

Incident Response Kali VM

File | 1 file

Download the files needed to set up your Kali virtual machine.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258, S0269

Kali VM Instructional Video

Video | 3 minutes

Get an overview of the virtual machine you will use to complete the two incident response projects.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258, S0269

Project 1 Walkthrough Video

Video | 2 minutes

An overview of the first incident response project. You’ll respond to an incident involving an employee being compromised while using tools to practice penetration testing.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258, S0269

Project 1 Files

File | 1 file

This downloadable .zip file contains challenges for the first project, including an overview, 10 challenge questions, a memory dump and pcap file, and the answers to the challenges to verify your work.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258, S0269

Project 2 Walkthrough Video

Video | 2 minutes

An overview of the second incident response project. You’ll respond to an incident involving possible SQL injection that affected credit card data.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258, S0269

Project 2 Files

File | 1 file

This downloadable .zip file contains challenges for the second project, including an overview, 12 challenge questions, a pcap and a memory dump of the primary Card Data Environment (CDE) server, and the answers to the challenges.

NICE Knowledge and Skill Statements:
S0199, S0221, S0258, S0269
Mobile Application Pentesting Project

Hone your iOS and Android application pentesting skills. You will use popular tools such as dex2jar and Hopper, practice working with ADB (Android Debug Bridge) and exploit various application vulnerabilities, including side-channel data leakage, broken cryptography, developer backdoors, insecure data storage and many others.

### Mobile Application Pentesting Exercises

**File | 24 challenges**

An overview of the process and tasks involved in the Mobile Application Pentesting Project

**NICE Knowledge and Skill Statements:**
S0001, S0137

---

### Using OVA Files

**File | 1 file**

A brief explanation of importing Open Virtual Appliance (OVA) files.

**NICE Knowledge and Skill Statements:**
S0001, S0137

---

### Android VM

**File | 1 virtual machine**

An Android virtual machine to use as the pentesting target.

**NICE Knowledge and Skill Statements:**
S0001, S0137

---

### Android Pentesting VM

**File | 1 virtual machine**

A virtual machine to be used as the attacker system for Android application pentesting exercises.

**NICE Knowledge and Skill Statements:**
S0001, S0137

---

### iOS Pentesting Tools and Files

**File | 1 file**

A collection of tools and files needed for completing the iOS application pentesting exercises.

**NICE Knowledge and Skill Statements:**
S0001, S0137
Network Traffic Analysis for Incident Response Project

In this project, you will need to apply your knowledge and use common network traffic analysis tools to solve multiple challenges. Each challenge involves examining a network traffic capture file containing evidence of malicious activity, such as malware infection, data exfiltration and C2 (command-and-control) communications.

**HANDS-ON TRAINING**

**Project Walkthrough Video**

Video | 13 minutes

An overview of the process and tasks involved in the Network Traffic Analysis for Incident Response Project.

**NICE Knowledge and Skill Statements:**
S0092, S0156, S0199, S0221, S0258, S0269

**Project Files**

File | 7 challenges

This downloadable .zip file contains challenges for the Network Traffic Analysis for Incident Response Project.

**NICE Knowledge and Skill Statements:**
S0092, S0156, S0199, S0221, S0258, S0269

**Project Hints Video**

Video | 16 minutes

Get hints to help you complete the Network Traffic Analysis for Incident Response Project.

**Project Solutions**

File | 1 file

View the solutions to the Network Traffic Analysis for Incident Response Project.

**NICE Knowledge and Skill Statements:**
S0092, S0156, S0199, S0221, S0258, S0269
Perform a gap analysis to determine the current state of the organization compared to the target state. You’ll determine and adjust impact levels with information from FIPS 199 and NIST SP 800-60 and identify the high-water mark from the impact levels. You’ll select, map and tailor controls from the NIST SP 800-53 catalog.

**Project Walkthrough Video**

- Video | 13 minutes
- An overview of the process and tasks involved in the NIST Cybersecurity Framework Project.

**Project Files**

- File | 1 challenge
- This downloadable .zip file contains challenges for the NIST Cybersecurity Framework Project.

**Project Solutions**

- File | 1 file
- View the solutions to the NIST Cybersecurity Framework Project.
NIST DoD RMF Project

In this project, you'll be applying the process for selecting system impact levels and choosing security controls based on them. You'll complete the NIST FIPS 200 worksheet for system categorization and perform other tasks related to the RMF application process.

### Project Walkthrough

**Video | 17 minutes**

An overview of the process and tasks involved in the NIST DoD RMF Project.

**NICE Knowledge and Skill Statements:**
S0115, S0147, S0228

### Artifacts List

**File | 1 challenge**

This downloadable file contains a list of artifacts used in the NIST DoD RMF Project.

**NICE Knowledge and Skill Statements:**
S0115, S0147, S0228

### Challenge Questions

**File | 1 file**

This downloadable file contains challenge questions for the NIST DoD RMF Project.

**NICE Knowledge and Skill Statements:**
S0115, S0147, S0228

### Project Artifacts

**File | 1 file**

This downloadable file contains walkthrough artifacts for the NIST DoD RMF Project.

**NICE Knowledge and Skill Statements:**
S0115, S0147, S0228

### Challenge Solutions

**File | 1 file**

View the solutions to the NIST DoD RMF Project.

**NICE Knowledge and Skill Statements:**
S0115, S0147, S0228
Offensive Bash Scripting Project

This Offensive Bash Scripting Project will put your new skills to the test! Your mission will be to hack the virtual machine named Kioptrix 2. This is a scaled-down version of Kioptrix 4 but uses the exact same enumeration process. Plenty of resources will be provided to assist you along solving this puzzle.

### Project Walkthrough

- **Video | 25 minutes**
  This video walks you through the project, explaining what needs to be done in each of the challenges.

  **NICE Knowledge and Skill Statements:** S0051, S0078

### Project Challenges

- **File | 1 file**
  Descriptions of the challenges you need to complete as part of this project.

  **NICE Knowledge and Skill Statements:** S0051, S0078

### Project Resources

- **File | 1 file**
  Links and other useful information for the project.

  **NICE Knowledge and Skill Statements:** S0051, S0078

### Project VM

- **File | 1 file**
  The VM needed for the project.

  **NICE Knowledge and Skill Statements:** S0051, S0078

### Project Hints

- **Video | 3 minutes**
  This video provides useful hints to help you solve the project challenges.

  **NICE Knowledge and Skill Statements:** S0051, S0078

### Project Challenges Solutions

- **File | 1 file**
  Solutions to the challenge questions so you can check your work.

  **NICE Knowledge and Skill Statements:** S0051, S0078
Python for Pentesters Project

Test your understanding of Python for Pentesting in this project consisting of five challenges: create an email sender, create a buffer overflow exploit, write commands to conduct a Wi-Fi attack, start a new web scraping project and write a line of smtp code.

**Project Challenges**

File | 1 file
This file describes all of the challenges

**NICE Knowledge and Skill Statements:**
K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266

**Project Walkthrough**

Video | 4 minutes
This video walks you through the challenges.

**NICE Knowledge and Skill Statements:**
K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266

**Project Hints**

Video | 20 minutes
This video walks you through how to solve the project challenges.

**NICE Knowledge and Skill Statements:**
K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266

**Project Solutions**

File | 1 file
This file shares the project solutions so you can check your work.

**NICE Knowledge and Skill Statements:**
K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266
Purple Team Privilege Escalation Project

HANDS-ON TRAINING

This project contains three labs focused on understanding, exploiting, and mitigating vulnerabilities that allow a user to escalate their privileges. You will learn about sudo abuse, path injection attacks, and how to discover and remove sensitive information from Git repositories.

| Project Files
| Lab 1: Git Secrets Walkthrough
| Lab 2: Path Interception Walkthrough
| Lab 3: Insecure Sudo Walkthrough
| Project Solutions

**Project Files**

File | 1 file

A ZIP file containing the OVA file and instructions for completing the Purple Team Privilege Escalation Project.

**NICE Knowledge and Skill Statements:**

S0266, S0267

**Lab 1: Git Secrets Walkthrough**

Video | 9 minutes

A detailed video walkthrough of the first lab in the Purple Privilege Escalation Project.

**NICE Knowledge and Skill Statements:**

S0266, S0267

**Lab 2: Path Interception Walkthrough**

Video | 14 minutes

A detailed video walkthrough of the second lab in the Purple Privilege Escalation Project.

**NICE Knowledge and Skill Statements:**

S0266, S0267

**Lab 3: Insecure Sudo Walkthrough**

Video | 8 minutes

A detailed video walkthrough of the third lab in the Purple Privilege Escalation Project.

**NICE Knowledge and Skill Statements:**

S0266, S0267

**Project Solutions**

File | 1 file

A document containing the solutions to the Purple Team Privilege Escalation Project challenges.

**NICE Knowledge and Skill Statements:**

S0266, S0267
Purple Team Web Application Security Project

HANDS-ON TRAINING

This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application. You'll intercept web traffic with Burp Suite, perform a local file inclusion attack, practice using a static code analyzer, and learn about mitigation approaches and web application firewalls.

Project Files

File | 1 file
A ZIP file containing the OVA file and instructions for completing the Purple Team Web Application Security Project.

NICE Knowledge and Skill Statements:
S0022, S0025, S0051, S0084, S0172, S0174, S0293

Lab 1: Local File Inclusion (LFI) walkthrough

Video | 8 minutes
A detailed walkthrough of the first lab in the Purple Team Web Application Security Project.

NICE Knowledge and Skill Statements:
S0022, S0025, S0051, S0084, S0172, S0174, S0293

Lab 2: Secure Coding walkthrough

Video | 16 minutes
A detailed walkthrough of the second lab in the Purple Team Web Application Security Project.

NICE Knowledge and Skill Statements:
S0022, S0025, S0051, S0084, S0172, S0174, S0293

Lab 3: Web Application Firewall (WAF) walkthrough

Video | 9 minutes
A detailed walkthrough of the third lab in the Purple Team Web Application Security Project.

NICE Knowledge and Skill Statements:
S0022, S0025, S0051, S0084, S0172, S0174, S0293

Project Solutions

File | 1 file
A document containing the solutions to the Purple Team Web Application Security Project challenges.

NICE Knowledge and Skill Statements:
S0022, S0025, S0051, S0084, S0172, S0174, S0293
Secure Coding Fundamentals Project

In this project, you'll identify vulnerabilities in the provided applications and code samples and discover how those vulnerabilities could be exploited by an attacker. See for yourself how security errors in code can lead to compromised credentials, SQL injections, and buffer overflow and Cross-Site Scripting (XSS) attacks.

**Project Introduction Video**

Video | 4 minutes

An overview of the process and tasks involved in the Secure Coding Fundamentals Project.

**NICE Knowledge and Skill Statements:**
S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266

---

**Project Files**

File | 5 challenges

This downloadable .zip file contains challenges for the Secure Coding Fundamentals Project.

**NICE Knowledge and Skill Statements:**
S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266

---

**Project Hints Video**

Video | 3 minutes

Get hints to help you complete the Secure Coding Fundamentals Project.

**NICE Knowledge and Skill Statements:**
S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266

---

**Project Solutions**

File | 1 file

View the solutions to the Secure Coding Fundamental Project.

**NICE Knowledge and Skill Statements:**
S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266
Secure SDLC Project

HANDS-ON TRAINING

Practice your secure SDLC skills as your progress through four exercises related to threat modeling, static application security testing and white-box security testing using both automated tool-based analysis and manual analysis.

Project Codebase

File | 1 file
Files you will need to complete the project.

NICE Knowledge and Skill Statements:
S0174

Project Applications

File | 1 file
Application needed to complete the project.

NICE Knowledge and Skill Statements:
S0174

Project Challenges

File | 1 file
Description of challenges you need to complete as part of this project.

NICE Knowledge and Skill Statements:
S0174

Exercise 1 Walkthrough

Video | 7 minutes
This video walks you through exercise 1, threat modeling approach using Microsoft Threat Modeling Tool.

NICE Knowledge and Skill Statements:
S0174

Exercises 2, 3, 4 Walkthrough

Video | 12 minutes
This video walks you through exercises 2-4: static application security testing (SAST) using codebase and VCG tool, white-box security testing and manual analysis, and white-box security testing with manual analysis.

NICE Knowledge and Skill Statements:
S0174

Project Solutions

File | 1 file
This document contains solutions to the project challenges.

NICE Knowledge and Skill Statements:
S0174
Securing Linux/UNIX Project

HANDS-ON TRAINING

Test your understanding of securing Linux and UNIX in this project consisting of five challenges. You'll get hands-on experience using sudo, configuring OpenSSH, identifying and configuring access to TCP ports, decrypting and encrypting with GPG, and using SELinux.

Project Walkthrough

Video | 4 minutes
This video walks you through the project, explaining what needs to be done in each of the challenges.

Project OVA

File | 1 file
Files you will need to complete the project.

Project Hints

Video | 5 minutes
This video provides useful hints to help you solve the project challenges.
SIEM Architecture and Process Project

HANDS-ON TRAINING

Test your SIEM skills as you progress through five challenges. We will take a use case surrounding invalid user logon attempts and standardize our username field, visualize our data with a dashboard, enrich our data with last known user information, and create an alert that triggers with the required information.

---

Project Overview and Challenge Documents

File | 1 file
The challenge files and other documents you will need to complete this project.

NICE Knowledge and Skill Statements:
S0173

---

winlogbeat

File | 1 file
Files you will need to complete this project.

NICE Knowledge and Skill Statements:
S0173

---

Virtual Box

File | 1 file
Files you will need to complete this project.

NICE Knowledge and Skill Statements:
S0173

---

Graylog

File | 1 file
Files you will need to complete this project.

NICE Knowledge and Skill Statements:
S0173

---

Standardizing the Username Field Hint

Video | 5 minutes
In this video you are provided hints on how to find the index field you will be required to alter, and how to navigate to a pipeline processing rule.

NICE Knowledge and Skill Statements:
S0173

---

Standardizing the Username Field Answer

Video | 1 minute
In this video you are provided the remaining information required to create the pipeline processing rule to begin standardizing the username field.

NICE Knowledge and Skill Statements:
S0173
<table>
<thead>
<tr>
<th>Table of contents</th>
<th>Boot camps</th>
<th>Self-paced training</th>
<th>Learning paths</th>
<th>Labs</th>
<th>Projects</th>
<th>NICE mapping</th>
<th>Appendix</th>
</tr>
</thead>
</table>

### Creating the Invalid User Logon Dashboard Hint

**Video | 1 minute**

In this video you are provided hints to search for the specific data requirements to create your dashboard for invalid user logons.

**NICE Knowledge and Skill Statements:**
S0173

---

### Creating the Invalid User Logon Dashboard Answer

**Video | 2 minutes**

In this video you are provided with remaining information required to complete your invalid user logon dashboard.

**NICE Knowledge and Skill Statements:**
S0173

---

### Lookup Table Creation Hint

**Video | 2 minutes**

In this video you are provided hints on creating the lookup table required to enrich last successful logons on failed logons.

**NICE Knowledge and Skill Statements:**
S0173

---

### Last User Logon Search Criterion Hint

**Video | 5 minutes**

In this video you are provided hints to create search filter for the mapping of hostnames to last successful logons.

**NICE Knowledge and Skill Statements:**
S0173

---

### Last User Logon Data Enrichment Hint

**Video | 3 minutes**

In this video you are provided the remaining information for the search filter and provided hints to begin mapping hostnames to last successful logged on user.

**NICE Knowledge and Skill Statements:**
S0173

---

### Enriching Last User Logon to Failed Logon Hint

**Video | 3 minutes**

In this video you are provided the remaining information for mapping hostnames to last successful logged on user and hints on enriching failed logons with last known user information.

**NICE Knowledge and Skill Statements:**
S0173

---

### Enriching Last User Logon to Failed Logon Answer

**Video | 2 minutes**

In this video you are provided the remaining information to create the enrichment of last known username on invalid logon attempts.

**NICE Knowledge and Skill Statements:**
S0173

---

### Filtering Non-User Logons From Dashboard Hint

**Video | 2 minutes**

In this video you are provided hints on finding the information required to filter non-interactive and non-invalid username related activity.

**NICE Knowledge and Skill Statements:**
S0173

---

### Filtering Non-User Logons From Dashboard Answer

**Video | 2 minutes**

In this video you are provided the remaining information required to filter the non-interact and non-invalid username related activity.

**NICE Knowledge and Skill Statements:**
S0173
Creating an Alert on Invalid User Logon Attempts Hint

Video | 2 minutes

In this video you are provided hints on creating an alarm to trigger when an invalid logon occurs.

NICE Knowledge and Skill Statements:
S0173

Creating an Alert on Invalid User Logon Attempts Answer

Video | 5 minutes

In this video you are provided the remaining information on creating the alarm to trigger when an invalid logon occurs.

NICE Knowledge and Skill Statements:
S0173
Vulnerability Assessment Project

HANDS-ON TRAINING

Test your skills as your progress through seven challenges leveraging free-to-use security tools and services. Set up your environment using JDK 11, Maven 3.6.3 and Git. Then use SNYK, static application security testing with Coverity Scan and a risk assessment template to discover, identify and rate the CWEs and CVEs.

**Project Walkthrough**

Video | 3 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

**NICE Knowledge and Skill Statements:**
S0001, S0137, S0174

**Project Challenges**

File | 1 file

Description of the challenges you need to complete as part of this project.

**NICE Knowledge and Skill Statements:**
S0001, S0137, S0174

**Project Prerequisites**

File | 1 file

Files and links you will need to complete this project.

**Risk Assessment Template**

File | 1 file

The template you will need to complete this project.

**NICE Knowledge and Skill Statements:**
S0001, S0137, S0174

**Coverity Scan Demo**

Video | 17 minutes

Demonstration of Coverity Scan.

**NICE Knowledge and Skill Statements:**
S0001, S0137, S0174

**OTX Demo**

Video | 5 minutes

Demonstration of OTX.

**NICE Knowledge and Skill Statements:**
S0001, S0137, S0174
<table>
<thead>
<tr>
<th>Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNYK Demo</strong></td>
</tr>
<tr>
<td>Video</td>
</tr>
<tr>
<td>Demonstration of SNYK.</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**
S0001, S0137, S0174

<table>
<thead>
<tr>
<th>Project Challenges Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
</tr>
<tr>
<td>This document contains solutions to the project challenges.</td>
</tr>
</tbody>
</table>

**NICE Knowledge and Skill Statements:**
S0001, S0137, S0174
Vulnerability Management Project

HANDS-ON TRAINING

Put your vulnerability management skills to the test as you progress through a series of challenges. You'll identify risky open ports, find vulnerabilities in the operating system and SMB service, verify vulnerabilities and find their CVSS score, investigate how to remediate the vulnerabilities and more.

Project Walkthrough

Video | 12 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements: S0036

Project Challenges

File | 1 file

A list of questions you will complete as part of this project.

NICE Knowledge and Skill Statements: S0036

Vulnerability Management Metasploitable VM

File | 1 file

Files you will need to complete the project.

NICE Knowledge and Skill Statements: S0036

Project Hints Video

Video | 2 minutes

This video provides useful hints to help you solve the project challenges.

NICE Knowledge and Skill Statements: S0036

Project Challenges Solutions

File | 1 file

This document contains solutions to the project challenges.

NICE Knowledge and Skill Statements: S0036
Web Application Penetesting Project

In this project, you'll explore the most common web application security risks, including SQL injection, Cross-Site scripting (XSS), broken authentication and more. You'll need to apply all your knowledge about web application vulnerabilities and use many different tools and browser utilities to solve the challenges.

Web Application Penetesting Project - Getting Started
File | 13 challenges
This file contains information needed to get started on completing the Web Application Penetesting CTF challenge.

NICE Knowledge and Skill Statements:
S0051, S007B, S0137, S0167

Web Application Penetesting Project - Walkthrough
Video | 3 minutes
An overview of the process and tasks involved in the Web Application Penetesting project.

NICE Knowledge and Skill Statements:
S0051, S007B, S0137, S0167

Web Application Penetesting Project - Solutions
File | 1 file
Solutions to all Web Application Penetesting Project challenges.

NICE Knowledge and Skill Statements:
S0051, S007B, S0137, S0167
Web Server Protection Project

HANDS-ON TRAINING

Secure a real web server in this hands-on project. You will need to work with an Apache web server installed on a virtual machine to implement network filtering, add cookies to access log, harden the host OS, identify tampered binary files and complete other tasks to ensure that your web server is properly protected.

**Project Walkthrough Video**

Video | 19 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

**Project Challenges**

File | 10 challenges

Description of challenges you need to complete as part of this project.

**Project Files**

File | 1 file

Files you will need to complete the project.

**Project VM Keys**

File | 1 file

Key files for the virtual machine used in the project.

**Project Hints Video**

Video | 22 minutes

This video provides useful hints to help you solve the project challenges.

**Project Solutions**

File | 1 file

This document contains solutions to all project challenges.
Windows 10 Host Security Project

HANDS-ON TRAINING

In this project, you’ll first set up a secure Hyper-V lab environment. Next, you’ll practice locating and enabling the virtual trusted platform module and virtualization-based security, encrypting data with BitLocker, sharing files and modifying user permissions, verifying port security provided by Windows Firewall and more.

Project Walkthrough Video

Video | 16 minutes

An overview of the process and tasks involved in the Windows 10 Host Security Project.

NICE Knowledge and Skill Statements:
S0067, S0076, S0079, S0158, S0267, S0268

Project Challenges

File | 7 challenges

This document describes the configuration and challenges for the Windows 10 Host Security Project.

NICE Knowledge and Skill Statements:
S0067, S0076, S0079, S0158, S0267, S0268

Project Hints Video

Video | 8 minutes

Get hints to help you complete the Windows 10 Host Security Project.

NICE Knowledge and Skill Statements:
S0067, S0076, S0079, S0158, S0267, S0268

Solutions

File | 1 file

View the solutions to the Windows 10 Host Security Project.

NICE Knowledge and Skill Statements:
S0067, S0076, S0079, S0158, S0267, S0268
Windows Registry Forensics Project

HANDS-ON TRAINING

Test your Windows Registry Forensics skills by answering 25 challenges. You must first locate the registry files within the file system and export them to be examined. Then you'll use tools such as Registry Explorer, Decode and ShellBag to find the answers.

Windows Registry Forensics Project Challenges

File | 1 file

Gives a detailed explanation of the Windows Registry Forensics project.

NICE Knowledge and Skill Statements:
S0071, S0091

Windows Registry Forensics Project Walkthrough

Video | 37 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:
S0071, S0091
You’ll start with installing Active Directory. Then you’ll practice creating a shared folder and calculating effective permissions, hiding shares from users, encrypting files using the Encrypting File System (EFS) and BitLocker, blocking access via IP addresses and firewall ports, and securing server traffic using certificates.
Writing Secure Code in C++ Project

The project starts with the code of a very simple and unsafe HTTP server. This program receives requests through a TCP socket and returns the requested file or the output of executed commands. The student is guided through discovering the different security issues, describing them and fixing them.

**Project Introduction**

Video | 10 minutes
This video is an introduction to the project.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

**Receiving Requests**

Video | 7 minutes
This video explores the topic of receiving requests.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

**Receiving Requests: The Security Flaw**

Video | 3 minutes
This video takes you through the security flaws in receiving requests.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

**Receiving Requests: A Possible Solution**

Video | 1 minute
Explore a possible solution for flaws in receiving requests.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

**Parsing Requests: The Flaw**

Video | 1 minute
This video takes you through the security flaws in parsing requests.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

**Parsing Requests: A Possible Solution**

Video | 4 minutes
This video explores a possible solution to the flaw in parsing requests.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266
Sending Files: The Flaw

Video | 4 minutes

This video takes you through the security flaws in sending files.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

Sending Files: A Possible Solution

Video | 8 minutes

Take a look at the potential solution for the flaw in sending files.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

Executing Programs: Flaws and Fix

Video | 6 minutes

This video will be your guide to the details of executing programs.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

Executing Programs: A Possible Solution

Video | 4 minutes

This video explores a possible solution to the flaw in executing programs.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

Writing Secure Code in C++ Project VM

File | 1 file

Download the VM you will need to complete the C++ project.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266
Writing Secure Code in Node.js

There are seven challenges spread across three Node.js projects. Part 1 focuses on MongoDB injections and how to prevent them. Part 2 exploits event loop blocking. Part 3 is the one you need if you want to attack and fix a GraphQL API.
## Challenge 4 hint

Video | 4 minute

This video provides useful hints to help you solve the fourth project challenge.

**NICE Knowledge and Skill Statements:**
K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

## Challenge 5 hint

Video | 5 minute

This video provides useful hints to help you solve the fifth project challenge.

**NICE Knowledge and Skill Statements:**
K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

## Challenge 6 hint

Video | 6 minute

This video provides useful hints to help you solve the sixth project challenge.

**NICE Knowledge and Skill Statements:**
K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

## Challenge 7 hint

Video | 7 minute

This video provides useful hints to help you solve the seventh project challenge.

**NICE Knowledge and Skill Statements:**
K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266
Writing Secure Code in Java Project

HANDS-ON TRAINING

Build your Java project, then mitigate the vulnerabilities by adding validation to the inputs. You will also implement spring security on an application.

Project Walkthrough and Hints

Video | 24 minutes

This video walks you through the project, explaining what needs to be done and offering some hints.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

Spring Secure File

File | 1 file

The Spring Secure file you will need for part of the project.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266

Northwind

File | 1 file

The Northwind file you will need to complete part of the project.

NICE Knowledge and Skill Statements:
S0060, S0172, S0239, S0266
Writing Secure Code in PHP Project

Use your secure PHP coding skills to uncover issues in a simple application. Your challenge is to go through the code and find cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, insecure secrets, lack of input sanitation/validation and lack of proper error handling.

HANDS-ON TRAINING

**Writing Secure Code in PHP Project Walkthrough**

- Video | 5 minutes
- This video walks you through the project, explaining what needs to be done in each of the challenges.

**NICE Knowledge and Skill Statements:**
- S0060, S0172, S0239, S0266

**Writing Secure Code in PHP Project Files**

- File | 1 file
- This zip contains files you will need to complete the project.

**NICE Knowledge and Skill Statements:**
- S0060, S0172, S0239, S0266

**Writing Secure Code in PHP Project Hints**

- File | 5 minutes
- This video provides useful hints to help you solve the project challenges.

**NICE Knowledge and Skill Statements:**
- S0060, S0172, S0239, S0266

**Writing Secure Code in PHP Project Solutions**

- File | 1 file
- This document contains solutions to the project challenges.

**NICE Knowledge and Skill Statements:**
- S0060, S0172, S0239, S0266
x86 Disassembly Project

HANDS-ON TRAINING

Practice your x86 skills by using tools like NASM, Makefiles, objdump, gdp and more to complete three projects. You’ll create the quintessential Hello World program, debug an x86 program and tie everything together with a project that leverages input, output and logic flows.

**x86 Project VM**

File | 1 file

Use this virtual machine (VM) to complete the three labs in the Introduction to x86 Disassembly Learning Path.

**LAB: Hello World! Creating the Usual Hello World in x86**

Video | 20 minutes

This project will guide you through building an application written entirely in x86 Assembly.

**LAB: x86 Debugging: Lab to Debug an x86 Program**

Video | 7 minutes

This project will guide you through debugging at the x86 level, plus techniques for locating and fixing bugs.

**LAB: x86 Program with Input, Output and Logic Flows**

Video | 15 minutes

This project will tie together all of the x86 concepts learned so far into a lab that leverages i/o, strings, conditional codes and logic structures.
Training mapped to the NICE Workforce Framework for Cybersecurity

Infosec Skills connects employee job descriptions to an established workforce development framework. Your organization can take a bottoms-up approach to any training initiative by mapping development plans to specific NICE knowledge and skills, work roles or even the competencies deemed most critical to employee success.

How Infosec Skills content is mapped to the framework

Every Infosec Skills course, cyber range or project is audited and mapped to relevant NICE knowledge and skill statements. For example, some of the statements mapped to our “Common malware behavior” course include:

» K0259: Knowledge of malware analysis concepts and methodologies
» K0392: Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.)
» S0131: Skill in analyzing malware
» S0087: Skill in deep analysis of captured malicious code (e.g., malware forensics)

Not using the NICE Framework?
Don’t worry – we’ve got you covered!

Infosec Skills Roles provide training recommendations for 12 of the most common cybersecurity positions, from beginner to advanced. Use these Roles to quickly build employee development plans and maximize training relevancy.
**Authorizing Official (SP-RSK-001)**

Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations and the Nation (CNSSI 4009).

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0028, K0037, K0044, K0048, K0049, K0070, K0146, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0295, K0322, K0342, K0622, K0624</td>
<td>S0034</td>
</tr>
<tr>
<td>ISACA CRISC</td>
<td>K0002, K0003, K0004, K0005, K0013, K0019, K0048, K0054, K0059, K0070, K0101, K0168, K0169, K0199, K0260, K0261, K0262, K0267, K0342</td>
<td>S0034</td>
</tr>
<tr>
<td>CompTIA CASP+</td>
<td>K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0038, K0049, K0059, K0070, K0101, K0146, K0169, K0170, K0179, K0199, K0260, K0261, K0262, K0267, K0342, K0622, K0624</td>
<td></td>
</tr>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0019, K0027, K0044, K0101, K0146, K0261, K0262, K0267</td>
<td>S0034</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSMP</td>
<td>K0002, K0003, K0004, K0013, K0048, K0070, K0101, K0146, K0260, K0261, K0262, K0267</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0040, K0089, K0126</td>
<td>S0367</td>
</tr>
</tbody>
</table>

**Security Control Assessor (SP-RSK-002)**

Conducts independent comprehensive assessments of the management, operational and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST 800-37).

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0006, K0007, K0010, K0018, K0019, K0021, K0026, K0027, K0044, K0056, K0101, K0146, K0261, K0262, K0267, K0322, K0622</td>
<td>S0027, S0034, S0147, S0171, S0273</td>
</tr>
<tr>
<td>ISC2 CGRC (previously - CAP)</td>
<td>K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0019, K0040, K0048, K0054, K0070, K0101, K0168, K0179, K0199, K0260, K0261, K0262, K0267, K0342</td>
<td>S0034, S0078, S0097, S0136, S0137, S0147</td>
</tr>
<tr>
<td>CompTIA CASP+</td>
<td>K0002, K0003, K0004, K0005, K0006, K0007, K0011, K0013, K0018, K0019, K0021, K0026, K0038, K0048, K0049, K0056, K0059, K0070, K0101, K0146, K0169, K0170, K0179, K0199, K0260, K0261, K0262, K0267, K0342, K0622, K0624</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP-ISSMP</td>
<td>K0002, K0003, K0004, K0013, K0021, K0026, K0048, K0070, K0084, K0101, K0146, K0169, K0260, K0261, K0262, K0267, K0342</td>
<td>S0001, S0038, S0171, S0175, S0242</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0009, K0029, K0089, K0100, K0126</td>
<td>S0073, S0110, S0115, S0120, S0124, S0135, S0138, S0141, S0145, S0172, S0173, S0174, S0184, S0239, S0241, S0252, S0278, S0280, S0296, S0367, S0374</td>
</tr>
</tbody>
</table>
## Software Developer (SP-DEV-001)

Develops, creates, maintains and writes/codes new (or modifies existing) computer applications, software or specialized utility programs.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CertNexus Cyber Secure Coder</td>
<td>K0001, K0003, K0004, K0005, K0006, K0028, K0039, K0044, K0068, K0070, K0079, K0080, K0081, K0082, K0084, K0105, K0139, K0140, K0153, K0260, K0261, K0262, K0624</td>
<td>S0014, S0022, S0031, S0034, S0135, S0138, S0149, S0174, S0367</td>
</tr>
<tr>
<td>Certified Mobile and Web App Penetration Tester</td>
<td>K0004, K0060, K0070, K0105, K0140, K0342, K0624</td>
<td>S0001, S0022, S0174</td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0028, K0039, K0044, K0050, K0070, K0073, K0081, K0082, K0153, K0170, K0179, K0199, K0260, K0261, K0262, K0322, K0332, K0342, K0624</td>
<td>S0031, S0034</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSMP</td>
<td>K0002, K0003, K0004, K0070, K0081, K0084, K0154, K0260, K0261, K0262, K0263, K0342, K0343</td>
<td>S0001, S0175</td>
</tr>
<tr>
<td>ISC2 CISSP-ISEEP</td>
<td>K0002, K0004, K0005, K0006, K0028, K0039, K0044, K0070, K0073, K0079, K0081, K0082, K0084, K0086, K0153, K0154, K0170, K0179, K0199, K0624</td>
<td>S0019, S0060</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0016, K0027, K0051, K0066, K0202</td>
<td>S0019, S0060</td>
</tr>
</tbody>
</table>

## Secure Software Assessor (SP-DEV-002)

Analyzes the security of new or existing computer applications, software or specialized utility programs and provides actionable results.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure SDLC</td>
<td>K0005, K0028, K0039, K0044, K0153, K0178, K0263, K0624</td>
<td>S0174</td>
</tr>
<tr>
<td>CertNexus Cyber Secure Coder</td>
<td>K0001, K0003, K0004, K0005, K0006, K0028, K0039, K0044, K0068, K0070, K0079, K0080, K0081, K0082, K0084, K0105, K0139, K0140, K0153, K0178, K0260, K0261, K0262, K0624</td>
<td>S0022, S0031, S0034, S0135, S0138, S0149, S0174, S0367</td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0044, K0070, K0081, K0154, K0178, K0263, K0322, K0342, K0624</td>
<td>S0031, S0138</td>
</tr>
<tr>
<td>CompTIA CySA+</td>
<td>K0002, K0003, K0004, K0005, K0039, K0044, K0070, K0079, K0080, K0081, K0153, K0178, K0179, K0199, K0342, K0624</td>
<td>S0031, S0138</td>
</tr>
<tr>
<td>ISC2 CISSP-ISEP</td>
<td>K0002, K0004, K0005, K0006, K0028, K0039, K0044, K0070, K0073, K0079, K0081, K0082, K0084, K0086, K0153, K0154, K0170, K0178, K0179, K0199, K0624</td>
<td>S0019, S0175</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0016, K0027, K0050, K0051, K0060, K0066, K0202, K0343</td>
<td>S0019, S0175</td>
</tr>
</tbody>
</table>
Enterprise Architect (SP-ARC-001)

Develops and maintains business, systems and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0027, K0044, K0056, K0061, K0074, K0091, K0198, K0264, K0275, K0286, K0287, K0322</td>
<td>S0027</td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0024, K0028, K0037, K0044, K0056, K0061, K0063, K0074, K0075, K0082, K0091, K0198, K0200, K0203, K0211, K0214, K0240, K0264, K0275, K0287, K0291, K0322, K0326, K0332, K0333, K0487, K0516</td>
<td>S0027</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSAP</td>
<td>K0001, K0002, K0004, K0005, K0006, K0028, K0035, K0044, K0074, K0075, K0082, K0091, K0102, K0170, K0179, K0180, K0198, K0203, K0211, K0214, K0240, K0264, K0287, K0291, K0299, K0323, K0333</td>
<td>S0122, S0367</td>
</tr>
<tr>
<td>Security Architecture</td>
<td>K0004, K0005, K0027, K0044, K0075, K0170, K0179, K0211, K0287, K0291, K0293</td>
<td>S0005, S0060, S0374</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0030, K0043, K0060, K0227</td>
<td></td>
</tr>
</tbody>
</table>

Security Architect (SP-ARC-002)

Ensures that the stakeholder security requirements necessary to protect the organization’s mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0007, K0010, K0018, K0019, K0026, K0027, K0044, K0056, K0061, K0074, K0091, K0198, K0261, K0262, K0264, K0275, K0286, K0287, K0322</td>
<td>S0027</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSAP</td>
<td>K0001, K0002, K0004, K0005, K0006, K0007, K0009, K0018, K0019, K0024, K0026, K0027, K0056, K0057, K0061, K0071, K0082, K0093, K0170, K0202, K0260, K0261, K0262, K0291, K0323, K0333, K0336, K0565</td>
<td>S0022, S0122, S0367</td>
</tr>
<tr>
<td>Security Architecture</td>
<td>K0004, K0005, K0027, K0044, K0170, K0211, K0287, K0291, K0293</td>
<td>S0005, S0059, S0061, S0138, S0152, S0168, S0170, S0374</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0011, K0015, K0030, K0036, K0043, K0059, K0060, K0092, K0227, K0277</td>
<td></td>
</tr>
</tbody>
</table>
Research and Development Specialist (SP-TRD-001)

Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0007, K0010, K0018, K0019, K0026, K0027, K0044, K0056, K0061, K0074, K0091, K0198, K0261, K0267, K0267, K0267, K0275, K0286, K0287, K0322</td>
<td>S0027</td>
</tr>
<tr>
<td>ISCC2 CISSP-ISSAP</td>
<td>K0001, K0002, K0004, K0005, K0006, K0007, K0009, K0018, K0019, K0024, K0026, K0027, K0056, K0057, K0061, K0071, K0082, K0093, K0170, K0202, K0260, K0261, K0291, K0332, K0333, K0336, K0565</td>
<td></td>
</tr>
<tr>
<td>ISCC2 CISSP-ISEP</td>
<td>K0002, K0004, K0005, K0006, K0013, K0026, K0035, K0044, K0074, K0082, K0091, K0102, K0170, K0180, K0198, K0211, K0214, K0240, K0264, K0287, K0291, K0323, K0333</td>
<td>S0022, S0122, S0367</td>
</tr>
<tr>
<td>Security Architecture</td>
<td>K0004, K0005, K0027, K0044, K0170, K0211, K0287, K0291, K0293</td>
<td>S0005, S0059, S0061, S0138, S0152, S0168, S0170, S0374</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0011, K0015, K0030, K0036, K0043, K0059, K0060, K0092, K0227, K0277</td>
<td></td>
</tr>
</tbody>
</table>

Systems Requirements Planner (SP-SRP-001)

Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISCC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0019, K0032, K0044, K0047, K0056, K0061, K0063, K0073, K0074, K0090, K0091, K0093, K0169, K0170, K0180, K0200, K0287, K0332, K0333, K0622</td>
<td></td>
</tr>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0018, K0019, K0032, K0044, K0047, K0056, K0061, K0074, K0090, K0091, K0101, K0267, K0287, K0622</td>
<td></td>
</tr>
<tr>
<td>ISCC2 CISSP-ISSAP</td>
<td>K0002, K0004, K0005, K0006, K0032, K0035, K0044, K0047, K0073, K0074, K0082, K0086, K0087, K0090, K0091, K0102, K0164, K0169, K0170, K0180, K0267, K0287, K0333</td>
<td></td>
</tr>
<tr>
<td>ISACA CRISC</td>
<td>K0002, K0003, K0004, K0005, K0018, K0019, K0059, K0066, K0073, K0101, K0168, K0169, K0267</td>
<td></td>
</tr>
<tr>
<td>CompTIA CASP+</td>
<td>K0002, K0003, K0004, K0005, K0006, K0018, K0019, K0035, K0056, K0059, K0087, K0101, K0169, K0170, K0267, K0332, K0622</td>
<td>S0005, S0367</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0043, K0060, K0126</td>
<td></td>
</tr>
</tbody>
</table>
# System Test & Evaluation Specialist (SP-TST-001)

Plans, prepares and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0028, K0037, K0044, K0057, K0091, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0287, K0332</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP-ISSAP</td>
<td>K0001, K0002, K0004, K0005, K0006, K0027, K0057, K0170, K0199, K0203, K0260, K0261, K0262, K0332</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP-ISSEP</td>
<td>K0002, K0004, K0005, K0006, K0028, K0044, K0091, K0102, K0169, K0170, K0179, K0199, K0203, K0287</td>
<td>S0110</td>
</tr>
<tr>
<td>CompTIA CASP+</td>
<td>K0002, K0003, K0004, K0005, K0006, K0169, K0170, K0179, K0199, K0260, K0261, K0262, K0332</td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td>K0003, K0004, K0005, K0287</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0088, K0126, K0139</td>
<td>S0060, S0061, S0367</td>
</tr>
</tbody>
</table>

# Information Systems Security Developer (SP-SYS-001)

Designs, develops, tests and evaluates information system security throughout the systems development life cycle.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP-ISSAP</td>
<td>K0001, K0002, K0004, K0005, K0006, K0018, K0024, K0027, K0050, K0056, K0061, K0065, K0081, K0082, K0093, K0170, K0203, K0260, K0261, K0262, K0308, K0332, K0333, K0336</td>
<td>S0031, S0145</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSEP</td>
<td>K0002, K0004, K0005, K0006, K0028, K0032, K0035, K0044, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0102, K0169, K0170, K0179, K0180, K0203, K0276, K0287, K0333</td>
<td>S0023, S0036</td>
</tr>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0018, K0027, K0032, K0044, K0056, K0061, K0065, K0081, K0090, K0091, K0261, K0262, K0287, K0322</td>
<td>S0034, S0085</td>
</tr>
<tr>
<td>CompTIA A+</td>
<td>K0001, K0030, K0032, K0035, K0036, K0050, K0060, K0061, K0260, K0261, K0262, K0332</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0015, K0066, K0126, K0139, K0297</td>
<td>S0001, S0022, S0367</td>
</tr>
</tbody>
</table>
**Systems Developer (SP-SYS-002)**

Designs, develops, tests and evaluates information systems throughout the systems development life cycle.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP-ISSAP</td>
<td>K0001, K0002, K0004, K0005, K0006, K0018, K0024, K0027, K0050, K0056, K0061, K0065, K0081, K0082, K0093, K0170, K0203, K0260, K0261, K0262, K0308, K0332, K0333, K0336</td>
<td>S0031, S0145</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSEP</td>
<td>K0002, K0004, K0005, K0006, K0028, K0032, K0035, K0044, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0102, K0169, K0170, K0179, K0180, K0203, K0276, K0287, K0333</td>
<td>S0023, S0036</td>
</tr>
<tr>
<td>CompTIA CASP+</td>
<td>K0002, K0003, K0004, K0005, K0006, K0018, K0035, K0049, K0056, K0065, K0081, K0087, K0169, K0170, K0179, K0260, K0261, K0262, K0308, K0332</td>
<td>S0022, S0023, S0036, S0367</td>
</tr>
<tr>
<td>Security Architecture</td>
<td>K0004, K0005, K0027, K0044, K0170, K0179, K0287, K0297</td>
<td>S00022, S0023, S0036, S0367</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0015, K0030, K0036, K0060, K0066, K0126, K0139, K0227</td>
<td>S0025, S0060, S0085, S0097, S0136, S0146</td>
</tr>
</tbody>
</table>

**Database Administrator (OM-DTA-001)**

Administers databases and/or data management systems that allow for the secure storage, query and utilization of data.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0022, K0023, K0056, K0065, K0069, K0083, K0260, K0261, K0262, K0287</td>
<td>S0023, S0031, S0034</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSAP</td>
<td>K0001, K0002, K0004, K0005, K0006, K0021, K0056, K0065, K0260, K0261, K0262</td>
<td>S0031, S0145</td>
</tr>
<tr>
<td>CompTIA CASP+</td>
<td>K0002, K0003, K0004, K0005, K0006, K0021, K0025, K0056, K0065, K0097, K0260, K0261, K0262, K0277</td>
<td>S0023, S0036</td>
</tr>
<tr>
<td>ISC2 CCSP</td>
<td>K0002, K0003, K0004, K0005, K0006, K0021, K0025, K0056, K0065, K0097, K0277, K0287</td>
<td>S00022, S0023, S0036, S0367</td>
</tr>
<tr>
<td>Linux Fundamentals</td>
<td>K0001, K0021, K0056, K0060, K0065, K0069</td>
<td>S0002</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0420</td>
<td>S00022, S0023, S0036, S0367</td>
</tr>
</tbody>
</table>
# Data Analyst (OM-DTA-002)

Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining and research purposes.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA IT Fundamentals (ITF+)</td>
<td>K0004, K0016, K0060, K0068, K0229, K0420</td>
<td>S0060</td>
</tr>
<tr>
<td>Cybersecurity Data Science</td>
<td>K0238</td>
<td>S0089</td>
</tr>
<tr>
<td>Information Security Fundamentals</td>
<td>K0001, K0002, K0005, K0006, K0065, K0129</td>
<td></td>
</tr>
<tr>
<td>Linux Fundamentals</td>
<td>K0001, K0056, K0060, K0065, K0129, K0229, K0236</td>
<td>S0130</td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0016, K0060, K0065, K0069, K0083, K0095</td>
<td>S0094, S0095</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0015, K0025, K0051, K0139, K0140</td>
<td></td>
</tr>
</tbody>
</table>

# Knowledge Manager (OM-KMG-001)

Responsible for the management and administration of processes and tools that enable the organization to identify, document and access intellectual capital and information content.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0095, K0146, K0195, K0260, K0261, K0262, K0287</td>
<td></td>
</tr>
<tr>
<td>CompTIA CASP+</td>
<td>K0002, K0003, K0004, K0005, K0006, K0146, K0194, K0260, K0261, K0262</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Management</td>
<td>K0002, K0003, K0004, K0005, K0006, K013, K0146, K0194, K0260, K0261, K0262, K0287</td>
<td></td>
</tr>
<tr>
<td>Enterprise Security Risk</td>
<td>K0002, K0003, K0004, K0005, K0006, K013, K0146, K0194, K0260, K0261, K0262, K0287</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISC2 CGRC (previously - CAP)</td>
<td>K0002, K0003, K0004, K0005, K0013, K0260, K0261, K0262</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0283, K0315, K0420</td>
<td></td>
</tr>
</tbody>
</table>
Technical Support Specialist (OM-STS-001)

Provides technical support to customers who need assistance utilizing client level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable).

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA A+</td>
<td>K0001, K0088, K0109, K0114, K0116, K0224, K0260, K0261, K0262, K0302</td>
<td>S0142</td>
</tr>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0109, K0194, K0260, K0261, K0262</td>
<td>S0142</td>
</tr>
<tr>
<td>Linux Fundamentals</td>
<td>K0001, K0114, K0116, K0247, K0294</td>
<td>S0142</td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0109</td>
<td></td>
</tr>
<tr>
<td>CompTIA CySA+</td>
<td>K0002, K0003, K0004, K0005, K0242, K0292, K0317</td>
<td>S0365</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0053, K0287</td>
<td></td>
</tr>
</tbody>
</table>

Network Operations Specialist (OM-NET-001)

Plans, implements and operates network services/systems, to include hardware and virtual environments.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0011, K0038, K0049, K0061, K0071, K0104, K0108, K0111, K0113, K0137, K0159, K0179, K0180, K0260, K0261, K0262, K0274, K0332</td>
<td>S0041, S0162</td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0011, K0049, K0104, K0108, K0160, K0179, K0201</td>
<td></td>
</tr>
<tr>
<td>JNCIA-Junos</td>
<td>K0001, K0004, K0005, K0011, K0049, K0061</td>
<td>S0041, S0084, S0170</td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0010, K0049, K0050, K0061, K0071, K0093, K0104, K0113, K0136, K0138, K0159, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0274, K0287, K0332, K0622</td>
<td>S0044, S0041, S0077</td>
</tr>
<tr>
<td>CCNA</td>
<td>K0001, K0004, K0011, K0049, K0061, K0071, K0108, K0111, K0113, K0332</td>
<td>S0004, S0041, S0077</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0029, K0053, K0135</td>
<td>S0079</td>
</tr>
</tbody>
</table>
System Administrator (OM-ADM-001)

Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA A+</td>
<td>K0001, K0050, K0088, K0104, K0117, K0130, K0158, K0260, K0261, K0262, K0274, K0318, K0332</td>
<td>S0073, S0076, S0151</td>
</tr>
<tr>
<td>Linux Fundamentals</td>
<td>K0001, K0049, K0100, K0117, K0318, K0332</td>
<td>S0076, S0143, S0151, S0158</td>
</tr>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0049, K0104, K0130, K0167, K0179, K0260, K0261, K0262, K0274, K0332</td>
<td>S0151</td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0049, K0104, K0130, K0158, K0167, K0179, K0318</td>
<td>S0158</td>
</tr>
<tr>
<td>ISC2 CGRC (previously - CAP)</td>
<td>K0002, K0003, K0004, K0005, K0006, K0053, K0064, K0179, K0260, K0261, K0262</td>
<td>S0153, S0155</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0077</td>
<td>S0033, S0043</td>
</tr>
</tbody>
</table>

Systems Security Analyst (OM-ANA-001)

Responsible for the analysis and development of the integration, testing, operations and maintenance of systems security.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA A+</td>
<td>K0001, K0035, K0036, K0060, K0061, K0260, K0261, K0262</td>
<td>S0167</td>
</tr>
<tr>
<td>CompTIA CySA+</td>
<td>K0002, K0003, K0004, K0005, K0040, K0044, K0049, K0056, K0082, K0179, K0333, K0339</td>
<td>S0027, S0147</td>
</tr>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0018, K0049, K0056, K0061, K0261, K0262, K0263, K0267, K0275, K0287, K0290, K0322</td>
<td>S0031</td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0019, K0024, K0044, K0049, K0056, K0061, K0063, K0075, K0082, K0093, K0179, K0180, K0200, K0203, K0206, K0261, K0262, K0275, K0276, K0285, K0287, K0322, K0332</td>
<td>S0027, S0036</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSEP</td>
<td>K0002, K0004, K0005, K0006, K0035, K0040, K0044, K0075, K0082, K0102, K0179, K0180, K0203, K0267, K0268, K0287, K0333, K0339</td>
<td>S0060, S0141, S0367</td>
</tr>
</tbody>
</table>
# Cyber Legal Advisor (OV-LGA-001)

Provides legal advice and recommendations on relevant topics related to cyber law.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0146, K0165, K0169</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP-ISSEP</td>
<td>K0002, K0004, K0005, K0006, K0048, K0154, K0165, K0169, K0257, K0270</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP-ISSMP</td>
<td>K0002, K0003, K0004, K0048, K0072, K0146, K0154, K0165, K0169</td>
<td></td>
</tr>
<tr>
<td>ISACA CRISC</td>
<td>K0002, K0003, K0004, K0005, K0048, K0072, K0165, K0169</td>
<td></td>
</tr>
<tr>
<td>PMI Project Management</td>
<td>K0002, K0072, K0270</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0126</td>
<td>S0372</td>
</tr>
</tbody>
</table>

# Privacy Officer/Privacy Compliance Manager (OV-LGA-002)

Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy and incident response needs of privacy and security executives and their teams.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0612, K0615</td>
<td></td>
</tr>
<tr>
<td>ISACA CRISC</td>
<td>K0002, K0003, K0004, K0005, K0066, K0168, K0615</td>
<td>S0356</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSMP</td>
<td>K0002, K0003, K0004, K0615</td>
<td></td>
</tr>
<tr>
<td>ISC2 CGRC (previously - CAP)</td>
<td>K0002, K0003, K0004, K0005, K0006, K0168, K0612</td>
<td></td>
</tr>
<tr>
<td>Threat Modeling</td>
<td>K0002, K0004, K0005, K0612</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0614</td>
<td>S0354</td>
</tr>
</tbody>
</table>
Cyber Instructional Curriculum Developer (OV-TEA-001)

Develops, plans, coordinates and evaluates cyber training/education courses, methods and techniques based on instructional needs.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training and Awareness Basics</strong></td>
<td>K0003, K0004, K0005, K0146, K0243, K0245, K0252</td>
<td></td>
</tr>
<tr>
<td><strong>ISACA CRISC</strong></td>
<td>K0002, K0003, K0004, K0005, K0059, K0147</td>
<td></td>
</tr>
<tr>
<td><strong>Enterprise Security Risk Management</strong></td>
<td>K0002, K0003, K0004, K0005, K0006, K0059, K0146, K0147, K0243, K0287</td>
<td>S0070</td>
</tr>
<tr>
<td><strong>Cybersecurity Management</strong></td>
<td>K0002, K0003, K0004, K0005, K0006, K0146, K0243, K0287</td>
<td></td>
</tr>
<tr>
<td><strong>ISC2 CISSP</strong></td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0146, K0243, K0287</td>
<td></td>
</tr>
<tr>
<td><strong>Other learning paths</strong></td>
<td></td>
<td>S0296</td>
</tr>
</tbody>
</table>

Cyber Instructor (OV-TEA-002)

Develops and conducts training or education of personnel within cyber domain.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training and Awareness Basics</strong></td>
<td>K0003, K0004, K0005, K0007, K0146, K0245, K0252, K0313</td>
<td></td>
</tr>
<tr>
<td><strong>ISACA CRISC</strong></td>
<td>K0002, K0003, K0004, K0005, K0007, K0059, K0147</td>
<td>S0070</td>
</tr>
<tr>
<td><strong>EC-Council CEH</strong></td>
<td>K0002, K0115, K0147</td>
<td>S0001, S0051, S0052, S0081, S0156, S0293</td>
</tr>
<tr>
<td><strong>Web Server Protection</strong></td>
<td>K0005, K0006</td>
<td>S0051, S0084, S0121</td>
</tr>
<tr>
<td><strong>CompTIA Security+</strong></td>
<td>K0002, K0005, K0006, K0007, K0130, K0147</td>
<td>S0081</td>
</tr>
<tr>
<td><strong>Other learning paths</strong></td>
<td>K0001, K0215, K0287</td>
<td>S0004, S0057, S0060, S0073, S0075, S0076, S0097, S0131, S0184, S0270, S0356, S0358</td>
</tr>
</tbody>
</table>
Information Systems Security Manager (OV-MGT-001)

Responsible for the cybersecurity of a program, organization, system or enclave.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA CASP+</td>
<td>K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0026, K0033, K0038, K0042, K0048,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K0059, K0070, K0087, K0092, K0101, K0106, K0150, K0151, K0167, K0169, K0170, K0179,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K0199, K0260, K0261, K0262, K0267, K0332, K0342, K0622, K0624</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0026, K0033, K0042, K0048,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K0061, K0070, K0077, K0090, K0150, K0167, K0169, K0170, K0179, K0180, K0199, K0260,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K0261, K0262, K0287, K0332, K0342, K0622, K0624</td>
<td>S0027</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSEP</td>
<td>K0002, K0004, K0005, K0006, K0026, K0040, K0042, K0048, K0070, K0087, K0090, K0106,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K0150, K0167, K0169, K0170, K0179, K0180, K0199, K0267, K0287, K0624</td>
<td></td>
</tr>
<tr>
<td>ISACA CISM</td>
<td>K0002, K0006, K0021, K0026, K0042, K0054, K0072, K0087, K0090, K0101, K0121, K0149,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K0150, K0199, K0267, K0287, K0622</td>
<td>S0027</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSMP</td>
<td>K0002, K0003, K0004, K0021, K0026, K0042, K0046, K0048, K0070, K0072, K0101, K0121,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K0149, K0150, K0169, K0260, K0261, K0262, K0267, K0342</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0043, K0053, K0058, K0126, K0168</td>
<td></td>
</tr>
</tbody>
</table>

Communications Security (COMSEC) Manager (OV-MGT-002)

Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0018, K0026, K0042, K0090, K0101, K0121, K0267, K0287,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K0622</td>
<td>S0027</td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0026, K0042, K0090, K0285, K0287,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K0622</td>
<td></td>
</tr>
<tr>
<td>Security Engineering</td>
<td>K0001, K0002, K0004, K0005, K0006, K0026, K0038, K0042, K0090, K0267, K0287, K0622</td>
<td></td>
</tr>
<tr>
<td>Introduction to Applied Cryptography and Cryptanalysis</td>
<td>K0004, K0005, K0018, K0038, K0622</td>
<td></td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0018, K0026, K0042</td>
<td>S0138</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0126</td>
<td></td>
</tr>
</tbody>
</table>
Cyber Workforce Developer and Manager (OV-SPP-001)

Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0146, K0169, K0215, K0243</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Audit Fundamentals</td>
<td>K0004, K0005, K0006, K0127, K0233</td>
<td></td>
</tr>
<tr>
<td>Training and Awareness Basics</td>
<td>K0003, K0004, K0005, K0146, K0243, K0313</td>
<td></td>
</tr>
<tr>
<td>EC-Council CEH</td>
<td>K0002, K0147, K0309</td>
<td></td>
</tr>
<tr>
<td>ISACA CRISC</td>
<td>K0002, K0003, K0004, K0005, K0072, K0101, K0147, K0168, K0169, K0335</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0234</td>
<td></td>
</tr>
</tbody>
</table>

Cyber Policy and Strategy Planner (OV-SPP-002)

Develops and maintains cybersecurity plans, strategy and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0146, K0624</td>
<td></td>
</tr>
<tr>
<td>EC-Council CEH</td>
<td>K0002, K0070, K0309, K0624</td>
<td></td>
</tr>
<tr>
<td>CompTIA PenTest+</td>
<td>K0003, K0004, K0005, K0070, K0234, K0624</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Audit Fundamentals</td>
<td>K0004, K0005, K0006, K0070, K0127, K0624</td>
<td></td>
</tr>
<tr>
<td>ISACA CRISC</td>
<td>K0002, K0003, K0004, K0005, K0070, K0168, K0335</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0313</td>
<td></td>
</tr>
</tbody>
</table>
Executive Cyber Leadership (OV-EXL-001)

Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CompTIA PenTest+</strong></td>
<td>K0003, K0004, K0005, K0009, K0070, K0106, K0147, K0314, K0624</td>
<td></td>
</tr>
<tr>
<td><strong>Security Engineering</strong></td>
<td>K0001, K0002, K0004, K0005, K0006, K0070, K0106, K0147, K0296, K0624</td>
<td>S0358</td>
</tr>
<tr>
<td><strong>ISC2 CISSP</strong></td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0624</td>
<td></td>
</tr>
<tr>
<td><strong>ISC2 CISSP-ISSMP</strong></td>
<td>K0002, K0003, K0004, K00070, K0296</td>
<td>S0356</td>
</tr>
<tr>
<td><strong>ISC2 CISSP-ISSAP</strong></td>
<td>K0001, K0002, K0004, K0005, K0006, K0009, K0070, K0624</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Program Manager (OV-PMA-001)

Leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ISC2 CISSP</strong></td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0090, K0146, K0165, K0169, K0196, K0198, K0200</td>
<td></td>
</tr>
<tr>
<td><strong>Cybersecurity Management</strong></td>
<td>K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0146, K0148, K0154, K0165, K0169, K0194, K0198, K0200, K0270</td>
<td></td>
</tr>
<tr>
<td><strong>NIST Cybersecurity Framework</strong></td>
<td>K0002, K0004, K0048, K0165</td>
<td>S0372</td>
</tr>
<tr>
<td><strong>ISC2 CISSP-ISSEP</strong></td>
<td>K0002, K0004, K0005, K0006, K0047, K0048, K0090, K0154, K0164, K0165, K0169, K0198, K0257, K0270</td>
<td></td>
</tr>
<tr>
<td><strong>Enterprise Security Risk Management</strong></td>
<td>K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0146, K0148, K0154, K0165, K0169, K0194, K0196, K0270</td>
<td>S0038</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0126</td>
<td></td>
</tr>
</tbody>
</table>
## Information Technology (IT) Project Manager (OV-PMA-002)

Directly manages information technology

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0090, K0146, K0165, K0169, K0196, K0198, K0200</td>
<td></td>
</tr>
<tr>
<td>ISACA CRISC</td>
<td>K0002, K0003, K0004, K0005, K0048, K0059, K0072, K0101, K0165, K0169</td>
<td>S0038</td>
</tr>
<tr>
<td>Enterprise Security Risk Management</td>
<td>K0002, K0003, K0004, K0006, K0047, K0048, K0059, K0072, K0090, K0146, K0148, K0154, K0165, K0169, K0194, K0196, K0270</td>
<td>S0038</td>
</tr>
<tr>
<td>NIST Cybersecurity Framework</td>
<td>K0002, K0004, K0048, K0165</td>
<td>S0372</td>
</tr>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0047, K0090, K0101, K0146, K0154, K0198, K0257, K0270</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0043, K0126, K0164</td>
<td></td>
</tr>
</tbody>
</table>

## Product Support Manager (OV-PMA-003)

Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0090, K0150, K0165, K0169, K0196, K0198, K0200</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP-ISSEP</td>
<td>K0002, K0004, K0005, K0006, K0048, K0090, K0150, K0154, K0164, K0165, K0169, K0198, K0257, K0270</td>
<td></td>
</tr>
<tr>
<td>PMI Project Management Professional (PMP)</td>
<td>K0002, K0072, K0249, K0270</td>
<td></td>
</tr>
<tr>
<td>Enterprise Security Risk Management</td>
<td>K0002, K0003, K0004, K0005, K0006, K0048, K0059, K0072, K0090, K0148, K0154, K0165, K0169, K0194, K0196, K0270</td>
<td>S0038</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSMP</td>
<td>K0002, K0003, K0004, K0048, K0072, K0150, K0154, K0165, K0169, K0196, K0198</td>
<td>S0038</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0043, K0126</td>
<td>S0372</td>
</tr>
</tbody>
</table>
**IT Investment/Portfolio Manager (OV-PMA-004)**

Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0146, K0165, K0169</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP-ISSEP</td>
<td>K0002, K0004, K0005, K0006, K0048, K0154, K0165, K0169, K0257, K0270</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP-ISSMP</td>
<td>K0002, K0003, K0004, K0048, K0072, K0146, K0154, K0165, K0169</td>
<td></td>
</tr>
<tr>
<td>ISACA CRISC</td>
<td>K0002, K0003, K0004, K0005, K0048, K0072, K0165, K0169</td>
<td></td>
</tr>
<tr>
<td>PMI Project Management Professional (PMP)</td>
<td>K0002, K0072, K0270</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0126</td>
<td>S0372</td>
</tr>
</tbody>
</table>

**IT Program Auditor (OV-PMA-005)**

Conducts evaluations of an IT program or its individual components, to determine compliance with published standards.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Audit Fundamentals</td>
<td>K0004, K0005, K0006, K0043, K0126, K0200, K0270</td>
<td>S0085</td>
</tr>
<tr>
<td>ISC2 CGRC (previously - CAP)</td>
<td>K0002, K0003, K0004, K0005, K0006, K0048, K0165</td>
<td>S0038</td>
</tr>
<tr>
<td>ISC2 CISSP-ISSMP</td>
<td>K0002, K0003, K0004, K0048, K0072, K0154, K0165, K0169, K0198</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Administration</td>
<td>K0001, K0002, K0004, K0005, K0006, K0048, K0148, K0165, K0169</td>
<td>S0085</td>
</tr>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0047, K0090, K0154, K0198, K0257, K0270</td>
<td>S0372</td>
</tr>
<tr>
<td>Other learning paths</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Cyber Defense Analyst (PR-CDA-001)

Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA CySA+</td>
<td>K0002, K0003, K0004, K0005, K0007, K0013, K0033, K0040, K0042, K0044, K0049, K0056, K0065, K0070, K0106, K0112, K0161, K0162, K0167, K0177, K0179, K0191, K0192, K0201, K0339, K0342, K0624</td>
<td>S0167</td>
</tr>
<tr>
<td>Cisco Certified CyberOps Associate</td>
<td>K0001, K0042, K0046, K0058, K0061, K0070, K0106, K0143, K0160, K0190, K0191, K0221, K0222, K0301, K0324, K0332, K0342</td>
<td>S0156</td>
</tr>
<tr>
<td>EC-Council CEH</td>
<td>K0002, K0013, K0018, K0019, K0061, K0070, K0106, K0160, K0161, K0177, K0191, K0210, K0261, K0297, K0300, K0301, K0324, K0332, K0339, K0624</td>
<td>S0025, S0078, S0156, S0167</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0015, K0024, K0059, K0107, K0110, K0116, K0139, K0168, K0260, K0262, K0290, K0303</td>
<td>S0054, S0057, S0147, S0367</td>
</tr>
</tbody>
</table>

## Cyber Defense Infrastructure Support Specialist (PR-INF-001)

Tests, implements, deploys, maintains and administers the infrastructure hardware and software.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0021, K0033, K0042, K0044, K0104, K0106, K0179, K0205, K0324</td>
<td>S0121, S0124</td>
</tr>
<tr>
<td>NIST DoD RMF</td>
<td>K0002, K0003, K0004, K0157</td>
<td>S0007, S0077</td>
</tr>
<tr>
<td>CCNA</td>
<td>K0001, K0004, K0033, K0061, K0324, K0332, K0334</td>
<td></td>
</tr>
<tr>
<td>CompTIA IT Fundamentals (ITF+)</td>
<td>K0004, K0021</td>
<td>S0054, S0059, S0079, S0367</td>
</tr>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0021, K0033, K0044, K0061, K0062, K0104, K0179, K0205, K0274, K0324, K0332</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0058, K0135, K0258</td>
<td></td>
</tr>
</tbody>
</table>
Cyber Defense Incident Responder (PR-CIR-001)

Investigates, analyzes and responds to cyber incidents within the network environment or enclave.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0021, K0026, K0033, K0041, K0042, K0046, K0070, K0106, K0167, K0177, K0179, K0221, K0230, K0624</td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td>K0003, K0004, K0005, K0026, K0041, K0042, K0046, K0058, K0062, K0106, K0162, K0287</td>
<td>S0003</td>
</tr>
<tr>
<td>CERT-Certified Computer Security Incident Handler (CSIH)</td>
<td>K0001, K0004, K0034, K0042, K0070, K0106, K0161, K0162, K0177, K0179, K0221, K0332, K0565</td>
<td>S0173, S0365</td>
</tr>
<tr>
<td>EC-Council CEH</td>
<td>K0002, K0070, K0106, K0161, K0177, K0259, K0332, K0565, K0624</td>
<td>S0078</td>
</tr>
<tr>
<td>Certified Computer Forensics Examiner (CCFE)</td>
<td>K0001</td>
<td>S0047</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0157</td>
<td>S0077, S0079, S0080</td>
</tr>
</tbody>
</table>

Vulnerability Assessment Analyst (PR-VAM-001)

Performs assessments of systems and networks within the NE or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0019, K0021, K0033, K0044, K0056, K0070, K0106, K0167, K0177, K0179, K0210, K0301, K0308, K0342, K0624</td>
<td>S0081</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>K0002, K0005, K0006, K0033, K0344</td>
<td>S0001, S0137</td>
</tr>
<tr>
<td>CompTIA PenTest+</td>
<td>K0003, K0004, K0005, K0009, K0068, K0070, K0106, K0177, K0206, K0301, K0342, K0624</td>
<td>S0001, S0051, S0052, S0081</td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0019, K0021, K0033, K0044, K0056, K0061, K0070, K0162, K0167, K0177, K0179, K0203, K0210, K0265, K0287, K0308, K0332, K0342, K0624</td>
<td>S0001, S0025, S0051, S0052, S0081, S0137</td>
</tr>
<tr>
<td>EC-Council CEH</td>
<td>K0002, K0009, K0019, K0061, K0070, K0106, K0161, K0177, K0301, K0308, K0332, K0344, K0624</td>
<td>S0001, S0025, S0051, S0052, S0081, S0137</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0089, K0139, K0224</td>
<td>S0044, S0120, S0171, S0364, S0367</td>
</tr>
</tbody>
</table>
## Threat/Warning Analyst (AN-TWA-001)

Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes and disseminates cyber threat/warning assessments.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0108, K0109, K0177, K0362, K0395, K0417, K0427, K0437, K0446, K0471, K0480, K0516, K0560, K0565, K0604, K0610, K0612, K0614</td>
<td></td>
</tr>
<tr>
<td>Threat Modeling</td>
<td>K0002, K0004, K0005, K0177, K0405, K0440, K0604, K0612</td>
<td>S0218, S0229</td>
</tr>
<tr>
<td>CERT-Certified Computer Security Incident Handler (CSIH)</td>
<td>K0001, K0004, K0108, K0177, K0362, K0395, K0427, K0436, K0444, K0445, K0446, K0449, K0471, K0480, K0516, K0560, K0565, K0603, K0604, K0614</td>
<td></td>
</tr>
<tr>
<td>EC-Council CEH</td>
<td>K0004, K0058, K0108, K0177, K0362, K0409, K0446, K0471, K0480, K0565, K0604</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0362, K0377, K0392, K0395, K0417, K0427, K0437, K0471, K0480, K0511, K0516, K0561, K0565, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0036, K0349, K0431, K0460, K0469</td>
<td>S0228, S0278, S0296</td>
</tr>
</tbody>
</table>

## Exploitation Analyst (AN-EXP-001)

Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0362, K0417, K0470, K0471, K0487, K0489</td>
<td>S0236</td>
</tr>
<tr>
<td>CERT-Certified Computer Security Incident Handler (CSIH)</td>
<td>K0001, K0004, K0108, K0177, K0362, K0444, K0447, K0471, K0489, K0560</td>
<td>S0199, S0258</td>
</tr>
<tr>
<td>Linux Fundamentals</td>
<td>K0001, K0349, K0397, K0444, K0471, K0487, K0529, K0608</td>
<td></td>
</tr>
<tr>
<td>Network Traffic Analysis Cyber Range</td>
<td>K0004, K0005, K0143, K0177, K0362, K0471</td>
<td>S0199, S0258, S0269</td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0108, K0109, K0177, K0362, K0376, K0379, K0397, K0451</td>
<td>S0294</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0131, K0224, K0351, K0354, K0371, K0393, K0394, K0430, K0523, K0535, K0544, K0559</td>
<td>S0184, S0207, S0239</td>
</tr>
</tbody>
</table>
## All-Source Analyst (AN-ASA-001)

Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0108, K0109, K0177, K0221, K0362, K0427, K0480, K0561, K0603, K0610</td>
<td></td>
</tr>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0108, K0109, K0221, K0427, K0556, K0560, K0561, K0598, K0603</td>
<td></td>
</tr>
<tr>
<td>CERT-Certified Computer Security Incident Handler (CSIH)</td>
<td>K0001, K0004, K0108, K0177, K0221, K0362, K0395, K0427, K0436, K0444, K0445, K0446, K0449, K0471, K0480, K0516, K0556, K0560, K0565, K0603, K0604, K0614</td>
<td></td>
</tr>
<tr>
<td>Threat Modeling</td>
<td>K0002, K0004, K0005, K0177, K0405, K0440, K0604, K0612</td>
<td>S0218, S0229</td>
</tr>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0108, K0109, K0177, K0221, K0362, K0395, K0427, K0437, K0446, K0471, K0480, K0516, K0556, K0560, K0604, K0610, K0612, K0614</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0036, K0058, K0349, K0377, K0392, K0409, K0410, K0431, K0460, K0469, K0511</td>
<td>S0278</td>
</tr>
</tbody>
</table>

## Mission Assessment Specialist (AN-ASA-002)

Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0362, K0392, K0395, K0410, K0417, K0427, K0437, K0471, K0480, K0511, K0516, K0561, K0565, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>CERT-Certified Computer Security Incident Handler (CSIH)</td>
<td>K0001, K0004, K0108, K0177, K0362, K0395, K0427, K0436, K0444, K0445, K0446, K0449, K0471, K0480, K0516, K0556, K0560, K0565, K0603, K0604, K0614</td>
<td></td>
</tr>
<tr>
<td>Threat Modeling</td>
<td>K0002, K0004, K0005, K0177, K0405, K0440, K0604, K0612</td>
<td>S0218, S0229</td>
</tr>
<tr>
<td>Linux Fundamentals</td>
<td>K0001, K0036, K0349, K0444, K0471, K0516, K0561, K0565</td>
<td></td>
</tr>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0108, K0109, K0177, K0362, K0395, K0417, K0427, K0437, K0446, K0471, K0480, K0516, K0560, K0565, K0604, K0610, K0612, K0614</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0036, K0058, K0349, K0377, K0392, K0409, K0410, K0431, K0460, K0469, K0511</td>
<td>S0228, S0278, S0296</td>
</tr>
</tbody>
</table>
Target Developer (AN-TGT-001)

Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Certified CyberOps Associate</td>
<td>K0001, K0005, K0362, K0402, K0440, K0516, K0565, K0603</td>
<td></td>
</tr>
<tr>
<td>CompTIA PenTest+</td>
<td>K0003, K0004, K0005, K0177, K0362, K0392, K0409, K0437, K0565</td>
<td>S0278</td>
</tr>
<tr>
<td>ITIL 4 Foundation</td>
<td>K0004</td>
<td>S0296</td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0108, K0109, K0177, K0362, K0379, K0427, K0561, K0603</td>
<td></td>
</tr>
<tr>
<td>CompTIA CySA+</td>
<td>K0002, K0003, K0004, K0005, K0177, K0362, K0381, K0409, K0460, K0561, K0565, K0603, K0604</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0036, K0349, K0351, K0395, K0417, K0431, K0436, K0444, K0445, K0446, K0449, K0471, K0479, K0543, K0555, K0556, K0560, K0598, K0614</td>
<td>S0218, S0228, S0229</td>
</tr>
</tbody>
</table>

Target Network Analyst (AN-TGT-002)

Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0362, K0392, K0395, K0403, K0471, K0487, K0516</td>
<td>S0291</td>
</tr>
<tr>
<td>EC-Council CEH</td>
<td>K0002, K0177, K0362, K0392, K0479, K0544</td>
<td></td>
</tr>
<tr>
<td>CompTIA A+</td>
<td>K0001, K0108, K0109, K0349, K0392, K0395, K0440, K0444, K0471, K0516, K0600</td>
<td></td>
</tr>
<tr>
<td>CompTIA CySA+</td>
<td>K0002, K0003, K0004, K0005, K0177, K0362, K0487, K0567</td>
<td></td>
</tr>
<tr>
<td>CERT-Certified Computer Security Incident Handler (CSIH)</td>
<td>K0001, K0004, K0108, K0177, K0362, K0395, K0436, K0444, K0445, K0449, K0471, K0516</td>
<td>S0219, S0228, S0229, S0261, S0268, S0280</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0379, K0424, K0431, K0472, K0559, K0599</td>
<td></td>
</tr>
</tbody>
</table>
### Multi-Disciplined Language Analyst (AN-LNG-001)

Applies language and culture expertise with target/threat and technical knowledge to process, analyze and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language intensive or interdisciplinary.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0108, K0177, K0488, K0548, K0600</td>
<td>S0241</td>
</tr>
<tr>
<td>CompTIA CySA+</td>
<td>K0002, K0003, K0004, K0005, K0177, K0487, K0488, K0548, K0567</td>
<td></td>
</tr>
<tr>
<td>CompTIA A+</td>
<td>K0001, K0108, K0417, K0491, K0600</td>
<td></td>
</tr>
<tr>
<td>Cisco Certified CyberOps Associate</td>
<td>K0001, K0143, K0493</td>
<td>S0184</td>
</tr>
<tr>
<td>Cybersecurity Data Science</td>
<td>K0177, K0476, K0493</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0377, K0396, K0398, K0431, K0449, K0524, K0579, K0599</td>
<td>S0218</td>
</tr>
</tbody>
</table>

### All Source-Collection Manager (CO-CLO-001)

Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0109, K0177, K0427, K0474, K0480, K0527, K0561, K0610</td>
<td></td>
</tr>
<tr>
<td>CompTIA A+</td>
<td>K0001, K0036, K0109, K0392, K0395, K0412, K0417, K0440, K0444, K0446, K0471, K0480, K0516, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0109, K0361, K0417, K0419, K0427, K0474, K0503, K0560, K0561</td>
<td></td>
</tr>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0005, K0006, K0109, K0177, K0395, K0417, K0427, K0446, K0471, K0474, K0475, K0480, K0516, K0560, K0565, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0109, K0177, K0395, K0417, K0419, K0427, K0471, K0480, K0516, K0527, K0561, K0565, K0579, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0058, K0353, K0364, K0405, K0425, K0431, K0435, K0445, K0449, K0477, K0496, K0584</td>
<td></td>
</tr>
</tbody>
</table>
All Source-Collection Requirements Manager (CO-CLO-002)

Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0395, K0417, K0419, K0427, K0480, K0516, K0527, K0561, K0565, K0579, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0109, K0177, K0395, K0417, K0427, K0446, K0474, K0475, K0480, K0516, K0560, K0565, K0565, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>CompTIA CASP+</td>
<td>K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0431, K0445, K0446, K0527, K0561, K0565, K0610</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Administration</td>
<td>K0001, K0002, K0004, K0005, K0006, K0109, K0177, K0417, K0427, K0445, K0466, K0516, K0527, K0561, K0565, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>Security Engineering</td>
<td>K0001, K0002, K0004, K0005, K0006, K0109, K0177, K0417, K0427, K0445, K0466, K0516, K0527, K0561, K0565, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0036, K0058, K0353, K0361, K0364, K0412, K0425, K0435, K0444, K0477, K0496</td>
<td></td>
</tr>
</tbody>
</table>

Cyber Intel Planner (CO-OPL-001)

Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0362, K0377, K0392, K0395, K0399, K0403, K0417, K0427, K0455, K0471, K0480, K0511, K0519, K0561, K0565, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Administration</td>
<td>K0001, K0002, K0004, K0005, K0006, K0362, K0377, K0395, K0403, K0417, K0427, K0445, K0446, K0471, K0561, K0565, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td>CompTIA Network+</td>
<td>K0001, K0002, K0004, K0108, K0109, K0362, K0395, K0417, K0427, K0446, K0471, K0480, K0560, K0565, K0599, K0610, K0612, K0614</td>
<td></td>
</tr>
<tr>
<td>CompTIA CySA+</td>
<td>K0002, K0003, K0004, K0005, K0362, K0432, K0460, K0504, K0561, K0565, K0603, K0612</td>
<td></td>
</tr>
<tr>
<td>ISACA CISA</td>
<td>K0002, K0003, K0004, K0005, K0108, K0109, K0417, K0427, K0432, K0501, K0504, K0556, K0560, K0561, K0589, K0598, K0603</td>
<td>S0273</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0036, K0349, K0379, K0405, K0408, K0411, K0431, K0435, K0436, K0440, K0444, K0506, K0512, K0518, K0586</td>
<td>S0186, S0218, S0278, S0296</td>
</tr>
</tbody>
</table>
Cyber Ops Planner (CO-OPL-002)

Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization and enables integration during the execution of cyber actions.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ISC2 CISSP</strong></td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0362, K0377, K0392, K0395, K0399, K0403, K0417, K0455, K0471, K0480, K0511, K0516, K0519, K0561, K0565, K0610, K0612</td>
<td></td>
</tr>
<tr>
<td><strong>CompTIA Network+</strong></td>
<td>K0001, K0002, K0004, K0108, K0109, K0362, K0395, K0417, K0446, K0471, K0480, K0516, K0560, K0565, K0599, K0610, K0612, K0614</td>
<td></td>
</tr>
<tr>
<td><strong>ISACA CISA</strong></td>
<td>K0002, K0003, K0004, K0005, K0108, K0109, K0417, K0432, K0501, K0504, K0556, K0560, K0561, K0589, K0598, K0603</td>
<td>S0273</td>
</tr>
<tr>
<td><strong>PMI Project Management</strong></td>
<td>K0002, K0379, K0506, K0512</td>
<td></td>
</tr>
<tr>
<td><strong>CERT-Certified Computer</strong></td>
<td>K0001, K0004, K0108, K0362, K0395, K0436, K0444, K0445, K0446, K0471, K0480, K0516, K0556, K0560, K0565, K0603, K0614</td>
<td></td>
</tr>
<tr>
<td><strong>Security Incident Handler</strong></td>
<td>K0002, K0004, K0005, K0108, K0109, K0417, K0432, K0501, K0504, K0556, K0560, K0561, K0589, K0598, K0603</td>
<td></td>
</tr>
<tr>
<td><strong>Other learning paths</strong></td>
<td>K0036, K0349, K0408, K0411, K0431, K0435, K0518, K0586</td>
<td>S0186, S0218, S0296</td>
</tr>
</tbody>
</table>

Partner Integration Planner (CO-OPL-003)

Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ISC2 CISSP</strong></td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0362, K0377, K0392, K0395, K0403, K0417, K0455, K0511</td>
<td></td>
</tr>
<tr>
<td><strong>CompTIA Network+</strong></td>
<td>K0001, K0002, K0004, K0108, K0109, K0362, K0395, K0417, K0599</td>
<td></td>
</tr>
<tr>
<td><strong>ISC2 CISSP-ISSAP</strong></td>
<td>K0001, K0002, K0004, K0005, K0006, K0395, K0403, K0417, K0432, K0455</td>
<td></td>
</tr>
<tr>
<td><strong>ISACA CISA</strong></td>
<td>K0002, K0003, K0004, K0005, K0108, K0109, K0417, K0432, K0501, K0504, K0598</td>
<td></td>
</tr>
<tr>
<td><strong>Threat Modeling</strong></td>
<td>K0002, K0004, K0005</td>
<td>S0218</td>
</tr>
<tr>
<td><strong>Other learning paths</strong></td>
<td>K0379, K0408, K0411, K0431, K0435, K0436, K0444, K0506, K0512</td>
<td>S0186, S0296</td>
</tr>
</tbody>
</table>
# Cyber Operator (CO-OPS-001)

Conducts collection, processing and/or geolocation of systems to exploit, locate and/or track targets of interest. Performs network navigation, tactical forensic analysis and, when directed, executing on-net operations.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CompTIA Security+</strong></td>
<td>K0002, K0005, K0006, K0021, K0109, K0363, K0379, K0403, K0427, K0428, K0433, K0452, K0480, K0530, K0536, K0573, K0609</td>
<td>S0267</td>
</tr>
<tr>
<td><strong>ISC2 CISSP</strong></td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0109, K0373, K0403, K0427, K0433, K0438, K0452, K0480, K0516, K0565</td>
<td>S0236</td>
</tr>
<tr>
<td><strong>Cisco Certified CyberOps Associate</strong></td>
<td>K0001, K0430, K0440, K0516, K0565, K0608</td>
<td>S0221</td>
</tr>
<tr>
<td><strong>CERT-Certified Computer Security Incident Handler (CSIH)</strong></td>
<td>K0001, K0004, K0363, K0375, K0427, K0428, K0433, K0438, K0452, K0480, K0486, K0516, K0560, K0565, K0573</td>
<td>S0062, S0192, S0221, S0267, S0270, S0298</td>
</tr>
<tr>
<td><strong>EC-Council CEH</strong></td>
<td>K0002, K0009, K0373, K0375, K0427, K0428, K0430, K0480, K0536, K0565</td>
<td>S0221, S0242, S0267, S0293, S0295</td>
</tr>
<tr>
<td><strong>Other learning paths</strong></td>
<td>K0051, K0224, K0372, K0406, K0420, K0429, K0481, K0531</td>
<td>S0206, S0252, S0257, S0266, S0275, S0282</td>
</tr>
</tbody>
</table>

# Cyber Crime Investigator (IN-INV-001)

Identifies, collects, examines and preserves evidence using controlled and documented analytical and investigative techniques.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ISC2 CISSP</strong></td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0118, K0123, K0125, K0128, K0155, K0156, K0209, K0244, K0251, K0624</td>
<td>S0062, S0192, S0221, S0267, S0270, S0298</td>
</tr>
<tr>
<td><strong>CompTIA CASP+</strong></td>
<td>K0002, K0003, K0004, K0005, K0006, K0070, K0118, K0125, K0128, K0624</td>
<td></td>
</tr>
<tr>
<td><strong>Linux Fundamentals</strong></td>
<td>K0001, K0070, K0114</td>
<td></td>
</tr>
<tr>
<td><strong>Incident Response</strong></td>
<td>K0003, K0004, K0005, K0046, K0110</td>
<td></td>
</tr>
<tr>
<td><strong>Certified Computer Forensics Examiner (CCFE)</strong></td>
<td>K0001, K0107, K0118, K0123, K0125, K0128, K0156, K0168</td>
<td>S0047, S0068</td>
</tr>
<tr>
<td><strong>Other learning paths</strong></td>
<td>K0231, K0351</td>
<td></td>
</tr>
</tbody>
</table>
Law Enforcement/Counterintelligence
Forensics Analyst *(IN-FOR-001)*

Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Computer Forensics Examiner (CCFE)</td>
<td>K0001, K0007, K0117, K0118, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0156, K0168, K0182, K0184, K0185, K0305</td>
<td>S0047, S0062, S0065, S0068, S0071, S0075, S0090, S0091, S0092</td>
</tr>
<tr>
<td>Certified Mobile Forensics Examiner (CMFE)</td>
<td>K0017, K0060, K0118, K0122, K0128, K0133, K0134</td>
<td>S0047, S0065, S0071, S0091</td>
</tr>
<tr>
<td>ISC2 CISSP</td>
<td>K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0021, K0042, K0070, K0077, K0109, K0118, K0122, K0123, K0125, K0128, K0132, K0133, K0145, K0155, K0156, K0167, K0179, K0184, K0305, K0624</td>
<td>S0046, S0062, S0067, S0071, S0075, S0090, S0091</td>
</tr>
<tr>
<td>CERT-Certified Computer Security Incident Handler (CSIH)</td>
<td>K0001, K0004, K0017, K0042, K0060, K0070, K0117, K0118, K0122, K0128, K0132, K0133, K0145, K0179, K0185</td>
<td>S0046, S0062, S0067, S0071, S0075, S0090, S0091</td>
</tr>
<tr>
<td>Certified Reverse Engineering Analyst (CREA)</td>
<td>K0183, K0186, K0188, K0189</td>
<td>S0087, S0092, S0093</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0119, K0187</td>
<td>S0032, S0069, S0073, S0074, S0089</td>
</tr>
</tbody>
</table>

Cyber Defense Forensics Analyst *(IN-FOR-002)*

Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

<table>
<thead>
<tr>
<th>Core path name</th>
<th>Knowledge statements</th>
<th>Skill statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompTIA Security+</td>
<td>K0002, K0005, K0006, K0018, K0021, K0042, K0070, K0109, K0118, K01145, K0167, K0179, K0255, K0301, K0624</td>
<td>S0089</td>
</tr>
<tr>
<td>Certified Computer Forensics Examiner (CCFE)</td>
<td>K0001, K0117, K0118, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0156, K0168, K0182, K0184, K0185, K0304</td>
<td>S0047, S0062, S0065, S0068, S0071, S0075, S0090, S0091, S0092</td>
</tr>
<tr>
<td>Certified Reverse Engineering Analyst (CREA)</td>
<td>K0183, K0186, K0188, K0189</td>
<td>S0087, S0092, S0093, S0131</td>
</tr>
<tr>
<td>CERT-Certified Computer Security Incident Handler (CSIH)</td>
<td>K0001, K0004, K0018, K0042, K0060, K0070, K0117, K0118, K0122, K0132, K0133, K0145, K0179, K0185, K0255, K0301, K0304</td>
<td>S0062, S0067, S0071, S0075, S0090, S0091, S0156</td>
</tr>
<tr>
<td>CompTIA CySA+</td>
<td>K0002, K0003, K0004, K0005, K0042, K0070, K0118, K0122, K0128, K0132, K0133, K0134, K0145, K0167, K0179, K0183, K0186, K0301, K0304, K0624</td>
<td>S0032, S0069, S0073, S0074</td>
</tr>
<tr>
<td>Other learning paths</td>
<td>K0077, K0119, K0155, K0187, K0224</td>
<td>S0032, S0069, S0073, S0074</td>
</tr>
</tbody>
</table>
The following table contains the knowledge and skill statements found in the NICE Workforce Framework for Cybersecurity. The first six knowledge statements are common to all 52 of the cybersecurity work roles in the framework.

<table>
<thead>
<tr>
<th>Knowledge ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0001</td>
<td>Knowledge of computer networking concepts and protocols, and network security methodologies.</td>
</tr>
<tr>
<td>K0002</td>
<td>Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).</td>
</tr>
<tr>
<td>K0003</td>
<td>Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.</td>
</tr>
<tr>
<td>K0004</td>
<td>Knowledge of cybersecurity and privacy principles.</td>
</tr>
<tr>
<td>K0005</td>
<td>Knowledge of cyber threats and vulnerabilities.</td>
</tr>
<tr>
<td>K0006</td>
<td>Knowledge of specific operational impacts of cybersecurity lapses.</td>
</tr>
<tr>
<td>K0007</td>
<td>Knowledge of authentication, authorization, and access control methods.</td>
</tr>
<tr>
<td>K0008</td>
<td>Knowledge of applicable business processes and operations of customer organizations.</td>
</tr>
<tr>
<td>K0009</td>
<td>Knowledge of application vulnerabilities.</td>
</tr>
<tr>
<td>K0010</td>
<td>Knowledge of communication methods, principles, and concepts that support the network infrastructure.</td>
</tr>
<tr>
<td>K0011</td>
<td>Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.</td>
</tr>
<tr>
<td>K0012</td>
<td>Knowledge of capabilities and requirements analysis.</td>
</tr>
<tr>
<td>K0013</td>
<td>Knowledge of cyber defense and vulnerability assessment tools and their capabilities.</td>
</tr>
<tr>
<td>K0014</td>
<td>Knowledge of complex data structures.</td>
</tr>
<tr>
<td>K0015</td>
<td>Knowledge of computer algorithms.</td>
</tr>
<tr>
<td>K0016</td>
<td>Knowledge of computer programming principles.</td>
</tr>
<tr>
<td>K0017</td>
<td>Knowledge of concepts and practices of processing digital forensic data.</td>
</tr>
<tr>
<td>K0018</td>
<td>Knowledge of encryption algorithms.</td>
</tr>
<tr>
<td>K0019</td>
<td>Knowledge of cryptography and cryptographic key management concepts.</td>
</tr>
<tr>
<td>K0020</td>
<td>Knowledge of data administration and data standardization policies.</td>
</tr>
<tr>
<td>K0021</td>
<td>Knowledge of data backup and recovery.</td>
</tr>
<tr>
<td>K0022</td>
<td>Knowledge of data mining and data warehousing principles.</td>
</tr>
<tr>
<td>K0023</td>
<td>Knowledge of database management systems, query languages, table relationships, and views.</td>
</tr>
<tr>
<td>K0024</td>
<td>Knowledge of database systems.</td>
</tr>
<tr>
<td>K0025</td>
<td>Knowledge of digital rights management.</td>
</tr>
<tr>
<td>K0026</td>
<td>Knowledge of business continuity and disaster recovery continuity of operations plans.</td>
</tr>
<tr>
<td>K0027</td>
<td>Knowledge of organization’s enterprise information security architecture.</td>
</tr>
<tr>
<td>K0028</td>
<td>Knowledge of organization’s evaluation and validation requirements.</td>
</tr>
<tr>
<td>K0029</td>
<td>Knowledge of organization’s Local and Wide Area Network connections.</td>
</tr>
<tr>
<td>K0030</td>
<td>Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).</td>
</tr>
<tr>
<td>K0031</td>
<td>Knowledge of enterprise messaging systems and associated software.</td>
</tr>
<tr>
<td>K0032</td>
<td>Knowledge of resiliency and redundancy.</td>
</tr>
<tr>
<td>K0033</td>
<td>Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0034</td>
<td>Knowledge of network services and protocols interactions that provide network communications.</td>
</tr>
<tr>
<td>K0035</td>
<td>Knowledge of installation, integration, and optimization of system components.</td>
</tr>
<tr>
<td>K0036</td>
<td>Knowledge of human-computer interaction principles.</td>
</tr>
<tr>
<td>K0037</td>
<td>Knowledge of Security Assessment and Authorization process.</td>
</tr>
<tr>
<td>K0038</td>
<td>Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.</td>
</tr>
<tr>
<td>K0039</td>
<td>Knowledge of cybersecurity and privacy principles and methods that apply to software development.</td>
</tr>
<tr>
<td>K0040</td>
<td>Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).</td>
</tr>
<tr>
<td>K0041</td>
<td>Knowledge of incident categories, incident responses, and timelines for responses.</td>
</tr>
<tr>
<td>K0042</td>
<td>Knowledge of incident response and handling methodologies.</td>
</tr>
<tr>
<td>K0043</td>
<td>Knowledge of industry-standard and organizationally accepted analysis principles and methods.</td>
</tr>
<tr>
<td>K0044</td>
<td>Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).</td>
</tr>
<tr>
<td>K0045</td>
<td>Knowledge of information security systems engineering principles (NIST SP 800-160).</td>
</tr>
<tr>
<td>K0046</td>
<td>Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.</td>
</tr>
<tr>
<td>K0047</td>
<td>Knowledge of information technology (IT) architectural concepts and frameworks.</td>
</tr>
<tr>
<td>K0048</td>
<td>Knowledge of Risk Management Framework (RMF) requirements.</td>
</tr>
<tr>
<td>K0049</td>
<td>Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).</td>
</tr>
<tr>
<td>K0050</td>
<td>Knowledge of local area and wide area networking principles and concepts including bandwidth management.</td>
</tr>
<tr>
<td>K0051</td>
<td>Knowledge of low-level computer languages (e.g., assembly languages).</td>
</tr>
<tr>
<td>K0052</td>
<td>Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).</td>
</tr>
<tr>
<td>K0053</td>
<td>Knowledge of measures or indicators of system performance and availability.</td>
</tr>
<tr>
<td>K0054</td>
<td>Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.</td>
</tr>
<tr>
<td>K0055</td>
<td>Knowledge of microprocessors.</td>
</tr>
<tr>
<td>K0056</td>
<td>Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).</td>
</tr>
<tr>
<td>K0057</td>
<td>Knowledge of network hardware devices and functions.</td>
</tr>
<tr>
<td>K0058</td>
<td>Knowledge of network traffic analysis methods.</td>
</tr>
<tr>
<td>K0059</td>
<td>Knowledge of new and emerging information technology (IT) and cybersecurity technologies.</td>
</tr>
<tr>
<td>K0060</td>
<td>Knowledge of operating systems.</td>
</tr>
<tr>
<td>K0061</td>
<td>Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).</td>
</tr>
<tr>
<td>K0062</td>
<td>Knowledge of packet-level analysis.</td>
</tr>
<tr>
<td>K0063</td>
<td>Knowledge of parallel and distributed computing concepts.</td>
</tr>
<tr>
<td>K0064</td>
<td>Knowledge of performance tuning tools and techniques.</td>
</tr>
<tr>
<td>K0065</td>
<td>Knowledge of policy-based and risk adaptive access controls.</td>
</tr>
<tr>
<td>K0066</td>
<td>Knowledge of Privacy Impact Assessments.</td>
</tr>
<tr>
<td>K0067</td>
<td>Knowledge of process engineering concepts.</td>
</tr>
<tr>
<td>K0068</td>
<td>Knowledge of programming language structures and logic.</td>
</tr>
<tr>
<td>K0069</td>
<td>Knowledge of query languages such as SQL (structured query language).</td>
</tr>
<tr>
<td>K0070</td>
<td>Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0071</td>
<td>Knowledge of remote access technology concepts.</td>
</tr>
<tr>
<td>K0072</td>
<td>Knowledge of resource management principles and techniques.</td>
</tr>
<tr>
<td>K0073</td>
<td>Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).</td>
</tr>
<tr>
<td>K0074</td>
<td>Knowledge of key concepts in security management (e.g., Release Management, Patch Management).</td>
</tr>
<tr>
<td>K0075</td>
<td>Knowledge of security system design tools, methods, and techniques.</td>
</tr>
<tr>
<td>K0076</td>
<td>Knowledge of server administration and systems engineering theories, concepts, and methods.</td>
</tr>
<tr>
<td>K0077</td>
<td>Knowledge of server and client operating systems.</td>
</tr>
<tr>
<td>K0078</td>
<td>Knowledge of server diagnostic tools and fault identification techniques.</td>
</tr>
<tr>
<td>K0079</td>
<td>Knowledge of software debugging principles.</td>
</tr>
<tr>
<td>K0080</td>
<td>Knowledge of software design tools, methods, and techniques.</td>
</tr>
<tr>
<td>K0081</td>
<td>Knowledge of software development models (e.g., Waterfall Model, Spiral Model).</td>
</tr>
<tr>
<td>K0082</td>
<td>Knowledge of software engineering.</td>
</tr>
<tr>
<td>K0083</td>
<td>Knowledge of sources, characteristics, and uses of the organization's data assets.</td>
</tr>
<tr>
<td>K0084</td>
<td>Knowledge of structured analysis principles and methods.</td>
</tr>
<tr>
<td>K0086</td>
<td>Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.</td>
</tr>
<tr>
<td>K0087</td>
<td>Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.</td>
</tr>
<tr>
<td>K0088</td>
<td>Knowledge of systems administration concepts.</td>
</tr>
<tr>
<td>K0089</td>
<td>Knowledge of systems diagnostic tools and fault identification techniques.</td>
</tr>
<tr>
<td>K0090</td>
<td>Knowledge of system life cycle management principles, including software security and usability.</td>
</tr>
<tr>
<td>K0091</td>
<td>Knowledge of systems testing and evaluation methods.</td>
</tr>
<tr>
<td>K0092</td>
<td>Knowledge of technology integration processes.</td>
</tr>
<tr>
<td>K0093</td>
<td>Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).</td>
</tr>
<tr>
<td>K0094</td>
<td>Knowledge of the capabilities and functionality associated with content creation technologies (e.g., wikis, social networking, content management systems, blogs).</td>
</tr>
<tr>
<td>K0095</td>
<td>Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines).</td>
</tr>
<tr>
<td>K0096</td>
<td>Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint).</td>
</tr>
<tr>
<td>K0097</td>
<td>Knowledge of the characteristics of physical and virtual data storage media.</td>
</tr>
<tr>
<td>K0098</td>
<td>Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.</td>
</tr>
<tr>
<td>K0100</td>
<td>Knowledge of the enterprise information technology (IT) architecture.</td>
</tr>
<tr>
<td>K0101</td>
<td>Knowledge of the organization's enterprise information technology (IT) goals and objectives.</td>
</tr>
<tr>
<td>K0102</td>
<td>Knowledge of the systems engineering process.</td>
</tr>
<tr>
<td>K0103</td>
<td>Knowledge of the type and frequency of routine hardware maintenance.</td>
</tr>
<tr>
<td>K0104</td>
<td>Knowledge of Virtual Private Network (VPN) security.</td>
</tr>
<tr>
<td>K0105</td>
<td>Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web service description language).</td>
</tr>
<tr>
<td>K0106</td>
<td>Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.</td>
</tr>
<tr>
<td>K0107</td>
<td>Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.</td>
</tr>
<tr>
<td>K0108</td>
<td>Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).</td>
</tr>
<tr>
<td>K0109</td>
<td>Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).</td>
</tr>
<tr>
<td>K0110</td>
<td>Knowledge of adversarial tactics, techniques, and procedures.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0111</td>
<td>Knowledge of network tools (e.g., ping, traceroute, nslookup)</td>
</tr>
<tr>
<td>K0112</td>
<td>Knowledge of defense-in-depth principles and network security architecture.</td>
</tr>
<tr>
<td>K0113</td>
<td>Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).</td>
</tr>
<tr>
<td>K0114</td>
<td>Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).</td>
</tr>
<tr>
<td>K0115</td>
<td>Knowledge that technology that can be exploited.</td>
</tr>
<tr>
<td>K0116</td>
<td>Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).</td>
</tr>
<tr>
<td>K0117</td>
<td>Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).</td>
</tr>
<tr>
<td>K0118</td>
<td>Knowledge of processes for seizing and preserving digital evidence.</td>
</tr>
<tr>
<td>K0119</td>
<td>Knowledge of hacking methodologies.</td>
</tr>
<tr>
<td>K0120</td>
<td>Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.</td>
</tr>
<tr>
<td>K0121</td>
<td>Knowledge of information security program management and project management principles and techniques.</td>
</tr>
<tr>
<td>K0122</td>
<td>Knowledge of investigative implications of hardware, Operating Systems, and network technologies.</td>
</tr>
<tr>
<td>K0123</td>
<td>Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).</td>
</tr>
<tr>
<td>K0124</td>
<td>Knowledge of multiple cognitive domains and tools and methods applicable for learning in each domain.</td>
</tr>
<tr>
<td>K0125</td>
<td>Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.</td>
</tr>
<tr>
<td>K0126</td>
<td>Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)</td>
</tr>
<tr>
<td>K0127</td>
<td>Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).</td>
</tr>
<tr>
<td>K0128</td>
<td>Knowledge of types and collection of persistent data.</td>
</tr>
<tr>
<td>K0129</td>
<td>Knowledge of command-line tools (e.g., mkdir, mv, ls, passwd, grep).</td>
</tr>
<tr>
<td>K0130</td>
<td>Knowledge of virtualization technologies and virtual machine development and maintenance.</td>
</tr>
<tr>
<td>K0131</td>
<td>Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.</td>
</tr>
<tr>
<td>K0132</td>
<td>Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.</td>
</tr>
<tr>
<td>K0133</td>
<td>Knowledge of types of digital forensics data and how to recognize them.</td>
</tr>
<tr>
<td>K0134</td>
<td>Knowledge of deployable forensics.</td>
</tr>
<tr>
<td>K0135</td>
<td>Knowledge of web filtering technologies.</td>
</tr>
<tr>
<td>K0136</td>
<td>Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).</td>
</tr>
<tr>
<td>K0137</td>
<td>Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).</td>
</tr>
<tr>
<td>K0138</td>
<td>Knowledge of Wi-Fi.</td>
</tr>
<tr>
<td>K0139</td>
<td>Knowledge of interpreted and compiled computer languages.</td>
</tr>
<tr>
<td>K0140</td>
<td>Knowledge of secure coding techniques.</td>
</tr>
<tr>
<td>K0142</td>
<td>Knowledge of collection management processes, capabilities, and limitations.</td>
</tr>
<tr>
<td>K0143</td>
<td>Knowledge of front-end collection systems, including traffic collection, filtering, and selection.</td>
</tr>
<tr>
<td>K0144</td>
<td>Knowledge of social dynamics of computer attackers in a global context.</td>
</tr>
<tr>
<td>K0145</td>
<td>Knowledge of security event correlation tools.</td>
</tr>
<tr>
<td>K0146</td>
<td>Knowledge of the organization's core business/mission processes.</td>
</tr>
<tr>
<td>K0147</td>
<td>Knowledge of emerging security issues, risks, and vulnerabilities.</td>
</tr>
<tr>
<td>K0148</td>
<td>Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.</td>
</tr>
<tr>
<td>K0149</td>
<td>Knowledge of organization's risk tolerance and/or risk management approach.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>K0150</td>
<td>Knowledge of enterprise incident response program, roles, and responsibilities.</td>
</tr>
<tr>
<td>K0151</td>
<td>Knowledge of current and emerging threats/threat vectors.</td>
</tr>
<tr>
<td>K0152</td>
<td>Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).</td>
</tr>
<tr>
<td>K0153</td>
<td>Knowledge of software quality assurance process.</td>
</tr>
<tr>
<td>K0154</td>
<td>Knowledge of supply chain risk management standards, processes, and practices.</td>
</tr>
<tr>
<td>K0155</td>
<td>Knowledge of electronic evidence law.</td>
</tr>
<tr>
<td>K0156</td>
<td>Knowledge of legal rules of evidence and court procedure.</td>
</tr>
<tr>
<td>K0157</td>
<td>Knowledge of cyber defense and information security policies, procedures, and regulations.</td>
</tr>
<tr>
<td>K0158</td>
<td>Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).</td>
</tr>
<tr>
<td>K0159</td>
<td>Knowledge of Voice over IP (VoIP).</td>
</tr>
<tr>
<td>K0160</td>
<td>Knowledge of the common attack vectors on the network layer.</td>
</tr>
<tr>
<td>K0161</td>
<td>Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).</td>
</tr>
<tr>
<td>K0162</td>
<td>Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).</td>
</tr>
<tr>
<td>K0163</td>
<td>Knowledge of critical information technology (IT) procurement requirements.</td>
</tr>
<tr>
<td>K0164</td>
<td>Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).</td>
</tr>
<tr>
<td>K0165</td>
<td>Knowledge of risk/threat assessment.</td>
</tr>
<tr>
<td>K0167</td>
<td>Knowledge of system administration, network, and operating system hardening techniques.</td>
</tr>
<tr>
<td>K0168</td>
<td>Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.</td>
</tr>
<tr>
<td>K0169</td>
<td>Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.</td>
</tr>
<tr>
<td>K0170</td>
<td>Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.</td>
</tr>
<tr>
<td>K0171</td>
<td>Knowledge of hardware reverse engineering techniques.</td>
</tr>
<tr>
<td>K0172</td>
<td>Knowledge of middleware (e.g., enterprise service bus and message queuing).</td>
</tr>
<tr>
<td>K0174</td>
<td>Knowledge of networking protocols.</td>
</tr>
<tr>
<td>K0175</td>
<td>Knowledge of software reverse engineering techniques.</td>
</tr>
<tr>
<td>K0176</td>
<td>Knowledge of Extensible Markup Language (XML) schemas.</td>
</tr>
<tr>
<td>K0177</td>
<td>Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).</td>
</tr>
<tr>
<td>K0178</td>
<td>Knowledge of secure software deployment methodologies, tools, and practices.</td>
</tr>
<tr>
<td>K0179</td>
<td>Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).</td>
</tr>
<tr>
<td>K0180</td>
<td>Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.</td>
</tr>
<tr>
<td>K0182</td>
<td>Knowledge of data carving tools and techniques (e.g., Foremost).</td>
</tr>
<tr>
<td>K0183</td>
<td>Knowledge of reverse engineering concepts.</td>
</tr>
<tr>
<td>K0184</td>
<td>Knowledge of anti-forensics tactics, techniques, and procedures.</td>
</tr>
<tr>
<td>K0185</td>
<td>Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).</td>
</tr>
<tr>
<td>K0186</td>
<td>Knowledge of debugging procedures and tools.</td>
</tr>
<tr>
<td>K0187</td>
<td>Knowledge of file type abuse by adversaries for anomalous behavior.</td>
</tr>
<tr>
<td>K0188</td>
<td>Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).</td>
</tr>
<tr>
<td>K0189</td>
<td>Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device).</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0190</td>
<td>Knowledge of encryption methodologies.</td>
</tr>
<tr>
<td>K0191</td>
<td>Knowledge of signature implementation impact for viruses, malware, and attacks.</td>
</tr>
<tr>
<td>K0192</td>
<td>Knowledge of Windows/Unix ports and services.</td>
</tr>
<tr>
<td>K0193</td>
<td>Knowledge of advanced data remediation security features in databases.</td>
</tr>
<tr>
<td>K0194</td>
<td>Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.</td>
</tr>
<tr>
<td>K0195</td>
<td>Knowledge of data classification standards and methodologies based on sensitivity and other risk factors.</td>
</tr>
<tr>
<td>K0196</td>
<td>Knowledge of Import/Export Regulations related to cryptography and other security technologies.</td>
</tr>
<tr>
<td>K0197</td>
<td>Knowledge of database access application programming interfaces (e.g., Java Database Connectivity [JDBC]).</td>
</tr>
<tr>
<td>K0198</td>
<td>Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).</td>
</tr>
<tr>
<td>K0199</td>
<td>Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).</td>
</tr>
<tr>
<td>K0200</td>
<td>Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).</td>
</tr>
<tr>
<td>K0201</td>
<td>Knowledge of symmetric key rotation techniques and concepts.</td>
</tr>
<tr>
<td>K0202</td>
<td>Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).</td>
</tr>
<tr>
<td>K0203</td>
<td>Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).</td>
</tr>
<tr>
<td>K0204</td>
<td>Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes).</td>
</tr>
<tr>
<td>K0205</td>
<td>Knowledge of basic system, network, and OS hardening techniques.</td>
</tr>
<tr>
<td>K0206</td>
<td>Knowledge of ethical hacking principles and techniques.</td>
</tr>
<tr>
<td>K0207</td>
<td>Knowledge of circuit analysis.</td>
</tr>
<tr>
<td>K0208</td>
<td>Knowledge of computer based training and e-learning services.</td>
</tr>
<tr>
<td>K0209</td>
<td>Knowledge of covert communication techniques.</td>
</tr>
<tr>
<td>K0210</td>
<td>Knowledge of data backup and restoration concepts.</td>
</tr>
<tr>
<td>K0211</td>
<td>Knowledge of confidentiality, integrity, and availability requirements.</td>
</tr>
<tr>
<td>K0212</td>
<td>Knowledge of cybersecurity-enabled software products.</td>
</tr>
<tr>
<td>K0213</td>
<td>Knowledge of instructional design and evaluation models (e.g., ADDIE, Smith/Ragan model, Gagne's Events of Instruction, Kirkpatrick's model of evaluation).</td>
</tr>
<tr>
<td>K0214</td>
<td>Knowledge of the Risk Management Framework Assessment Methodology.</td>
</tr>
<tr>
<td>K0215</td>
<td>Knowledge of organizational training policies.</td>
</tr>
<tr>
<td>K0216</td>
<td>Knowledge of learning levels (i.e., Bloom's Taxonomy of learning).</td>
</tr>
<tr>
<td>K0218</td>
<td>Knowledge of learning styles (e.g., assimilator, auditory, kinesthetic).</td>
</tr>
<tr>
<td>K0220</td>
<td>Knowledge of modes of learning (e.g., rote learning, observation).</td>
</tr>
<tr>
<td>K0221</td>
<td>Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).</td>
</tr>
<tr>
<td>K0222</td>
<td>Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.</td>
</tr>
<tr>
<td>K0224</td>
<td>Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.</td>
</tr>
<tr>
<td>K0226</td>
<td>Knowledge of organizational training systems.</td>
</tr>
<tr>
<td>K0227</td>
<td>Knowledge of various types of computer architectures.</td>
</tr>
<tr>
<td>K0228</td>
<td>Knowledge of taxonomy and semantic ontology theory.</td>
</tr>
<tr>
<td>K0229</td>
<td>Knowledge of applications that can log errors, exceptions, and application faults and logging.</td>
</tr>
<tr>
<td>K0230</td>
<td>Knowledge of cloud service models and how those models can limit incident response.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0231</td>
<td>Knowledge of crisis management protocols, processes, and techniques.</td>
</tr>
<tr>
<td>K0233</td>
<td>Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.</td>
</tr>
<tr>
<td>K0234</td>
<td>Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation).</td>
</tr>
<tr>
<td>K0235</td>
<td>Knowledge of how to leverage research and development centers, think tanks, academic research, and industry systems.</td>
</tr>
<tr>
<td>K0236</td>
<td>Knowledge of how to utilize Hadoop, Java, Python, SQL, Hive, and Pig to explore data.</td>
</tr>
<tr>
<td>K0237</td>
<td>Knowledge of industry best practices for service desk.</td>
</tr>
<tr>
<td>K0238</td>
<td>Knowledge of machine learning theory and principles.</td>
</tr>
<tr>
<td>K0239</td>
<td>Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.</td>
</tr>
<tr>
<td>K0240</td>
<td>Knowledge of multi-level security systems and cross domain solutions.</td>
</tr>
<tr>
<td>K0241</td>
<td>Knowledge of organizational human resource policies, processes, and procedures.</td>
</tr>
<tr>
<td>K0242</td>
<td>Knowledge of organizational security policies.</td>
</tr>
<tr>
<td>K0243</td>
<td>Knowledge of organizational training and education policies, processes, and procedures.</td>
</tr>
<tr>
<td>K0244</td>
<td>Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.</td>
</tr>
<tr>
<td>K0245</td>
<td>Knowledge of principles and processes for conducting training and education needs assessment.</td>
</tr>
<tr>
<td>K0246</td>
<td>Knowledge of relevant concepts, procedures, software, equipment, and technology applications.</td>
</tr>
<tr>
<td>K0247</td>
<td>Knowledge of remote access processes, tools, and capabilities related to customer support.</td>
</tr>
<tr>
<td>K0248</td>
<td>Knowledge of strategic theory and practice.</td>
</tr>
<tr>
<td>K0249</td>
<td>Knowledge of sustainment technologies, processes and strategies.</td>
</tr>
<tr>
<td>K0250</td>
<td>Knowledge of Test &amp; Evaluation processes for learners.</td>
</tr>
<tr>
<td>K0251</td>
<td>Knowledge of the judicial process, including the presentation of facts and evidence.</td>
</tr>
<tr>
<td>K0252</td>
<td>Knowledge of training and education principles and methods for curriculum design, teaching and instruction for individuals and groups, and the measurement of training and education effects.</td>
</tr>
<tr>
<td>K0254</td>
<td>Knowledge of binary analysis.</td>
</tr>
<tr>
<td>K0255</td>
<td>Knowledge of network architecture concepts including topology, protocols, and components.</td>
</tr>
<tr>
<td>K0257</td>
<td>Knowledge of information technology (IT) acquisition/procurement requirements.</td>
</tr>
<tr>
<td>K0258</td>
<td>Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).</td>
</tr>
<tr>
<td>K0259</td>
<td>Knowledge of malware analysis concepts and methodologies.</td>
</tr>
<tr>
<td>K0260</td>
<td>Knowledge of Personally Identifiable Information (PII) data security standards.</td>
</tr>
<tr>
<td>K0261</td>
<td>Knowledge of Payment Card Industry (PCI) data security standards.</td>
</tr>
<tr>
<td>K0262</td>
<td>Knowledge of Personal Health Information (PHI) data security standards.</td>
</tr>
<tr>
<td>K0263</td>
<td>Knowledge of information technology (IT) risk management policies, requirements, and procedures.</td>
</tr>
<tr>
<td>K0264</td>
<td>Knowledge of program protection planning (e.g., information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements).</td>
</tr>
<tr>
<td>K0265</td>
<td>Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.</td>
</tr>
<tr>
<td>K0266</td>
<td>Knowledge of how to evaluate the trustworthiness of the supplier and/or product.</td>
</tr>
<tr>
<td>K0267</td>
<td>Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.</td>
</tr>
<tr>
<td>K0268</td>
<td>Knowledge of forensic footprint identification.</td>
</tr>
<tr>
<td>K0269</td>
<td>Knowledge of mobile communications architecture.</td>
</tr>
<tr>
<td>K0270</td>
<td>Knowledge of the acquisition/procurement life cycle process.</td>
</tr>
<tr>
<td>K0271</td>
<td>Knowledge of operating system structures and internals (e.g., process management, directory structure, installed applications).</td>
</tr>
<tr>
<td>K0272</td>
<td>Knowledge of network analysis tools used to identify software communications vulnerabilities.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0274</td>
<td>Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi), paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.</td>
</tr>
<tr>
<td>K0275</td>
<td>Knowledge of configuration management techniques.</td>
</tr>
<tr>
<td>K0276</td>
<td>Knowledge of security management.</td>
</tr>
<tr>
<td>K0277</td>
<td>Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features).</td>
</tr>
<tr>
<td>K0278</td>
<td>Knowledge of current and emerging data remediation security features in databases.</td>
</tr>
<tr>
<td>K0280</td>
<td>Knowledge of systems engineering theories, concepts, and methods.</td>
</tr>
<tr>
<td>K0281</td>
<td>Knowledge of information technology (IT) service catalogues.</td>
</tr>
<tr>
<td>K0283</td>
<td>Knowledge of use cases related to collaboration and content synchronization across platforms (e.g., Mobile, PC, Cloud).</td>
</tr>
<tr>
<td>K0284</td>
<td>Knowledge of developing and applying user credential management system.</td>
</tr>
<tr>
<td>K0285</td>
<td>Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.</td>
</tr>
<tr>
<td>K0286</td>
<td>Knowledge of N-tiered typologies (e.g. including server and client operating systems).</td>
</tr>
<tr>
<td>K0287</td>
<td>Knowledge of an organization’s information classification program and procedures for information compromise.</td>
</tr>
<tr>
<td>K0288</td>
<td>Knowledge of industry standard security models.</td>
</tr>
<tr>
<td>K0289</td>
<td>Knowledge of system/server diagnostic tools and fault identification techniques.</td>
</tr>
<tr>
<td>K0290</td>
<td>Knowledge of systems security testing and evaluation methods.</td>
</tr>
<tr>
<td>K0291</td>
<td>Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)</td>
</tr>
<tr>
<td>K0292</td>
<td>Knowledge of the operations and processes for incident, problem, and event management.</td>
</tr>
<tr>
<td>K0293</td>
<td>Knowledge of integrating the organization’s goals and objectives into the architecture.</td>
</tr>
<tr>
<td>K0294</td>
<td>Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.</td>
</tr>
<tr>
<td>K0295</td>
<td>Knowledge of confidentiality, integrity, and availability principles.</td>
</tr>
<tr>
<td>K0296</td>
<td>Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.</td>
</tr>
<tr>
<td>K0297</td>
<td>Knowledge of countermeasure design for identified security risks.</td>
</tr>
<tr>
<td>K0299</td>
<td>Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.</td>
</tr>
<tr>
<td>K0300</td>
<td>Knowledge of network mapping and recreating network topologies.</td>
</tr>
<tr>
<td>K0301</td>
<td>Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).</td>
</tr>
<tr>
<td>K0302</td>
<td>Knowledge of the basic operation of computers.</td>
</tr>
<tr>
<td>K0303</td>
<td>Knowledge of the use of sub-netting tools.</td>
</tr>
<tr>
<td>K0304</td>
<td>Knowledge of concepts and practices of processing digital forensic data.</td>
</tr>
<tr>
<td>K0305</td>
<td>Knowledge of data concealment (e.g. encryption algorithms and steganography).</td>
</tr>
<tr>
<td>K0308</td>
<td>Knowledge of cryptology.</td>
</tr>
<tr>
<td>K0309</td>
<td>Knowledge of emerging technologies that have potential for exploitation.</td>
</tr>
<tr>
<td>K0310</td>
<td>Knowledge of hacking methodologies.</td>
</tr>
<tr>
<td>K0311</td>
<td>Knowledge of industry indicators useful for identifying technology trends.</td>
</tr>
<tr>
<td>K0312</td>
<td>Knowledge of intelligence gathering principles, policies, and procedures including legal authorities and restrictions.</td>
</tr>
<tr>
<td>K0313</td>
<td>Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research &amp; Development).</td>
</tr>
<tr>
<td>K0314</td>
<td>Knowledge of industry technologies’ potential cybersecurity vulnerabilities.</td>
</tr>
<tr>
<td>K0315</td>
<td>Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing information.</td>
</tr>
<tr>
<td>K0316</td>
<td>Knowledge of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0317</td>
<td>Knowledge of procedures used for documenting and querying reported incidents, problems, and events.</td>
</tr>
<tr>
<td>K0318</td>
<td>Knowledge of operating system command-line tools.</td>
</tr>
<tr>
<td>K0319</td>
<td>Knowledge of technical delivery capabilities and their limitations.</td>
</tr>
<tr>
<td>K0320</td>
<td>Knowledge of organization's evaluation and validation criteria.</td>
</tr>
<tr>
<td>K0321</td>
<td>Knowledge of engineering concepts as applied to computer architecture and associated computer hardware/software.</td>
</tr>
<tr>
<td>K0322</td>
<td>Knowledge of embedded systems.</td>
</tr>
<tr>
<td>K0323</td>
<td>Knowledge of system fault tolerance methodologies.</td>
</tr>
<tr>
<td>K0324</td>
<td>Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.</td>
</tr>
<tr>
<td>K0325</td>
<td>Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).</td>
</tr>
<tr>
<td>K0326</td>
<td>Knowledge of demilitarized zones.</td>
</tr>
<tr>
<td>K0330</td>
<td>Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.</td>
</tr>
<tr>
<td>K0332</td>
<td>Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.</td>
</tr>
<tr>
<td>K0333</td>
<td>Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.</td>
</tr>
<tr>
<td>K0334</td>
<td>Knowledge of network traffic analysis (tools, methodologies, processes).</td>
</tr>
<tr>
<td>K0335</td>
<td>Knowledge of current and emerging cyber technologies.</td>
</tr>
<tr>
<td>K0336</td>
<td>Knowledge of access authentication methods.</td>
</tr>
<tr>
<td>K0338</td>
<td>Knowledge of data mining techniques.</td>
</tr>
<tr>
<td>K0339</td>
<td>Knowledge of how to use network analysis tools to identify vulnerabilities.</td>
</tr>
<tr>
<td>K0341</td>
<td>Knowledge of foreign disclosure policies and import/export control regulations as related to cybersecurity.</td>
</tr>
<tr>
<td>K0342</td>
<td>Knowledge of penetration testing principles, tools, and techniques.</td>
</tr>
<tr>
<td>K0343</td>
<td>Knowledge of root cause analysis techniques.</td>
</tr>
<tr>
<td>K0344</td>
<td>Knowledge of an organization's threat environment.</td>
</tr>
<tr>
<td>K0346</td>
<td>Knowledge of principles and methods for integrating system components.</td>
</tr>
<tr>
<td>K0347</td>
<td>Knowledge and understanding of operational design.</td>
</tr>
<tr>
<td>K0349</td>
<td>Knowledge of website types, administration, functions, and content management system (CMS).</td>
</tr>
<tr>
<td>K0350</td>
<td>Knowledge of accepted organization planning systems.</td>
</tr>
<tr>
<td>K0351</td>
<td>Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.</td>
</tr>
<tr>
<td>K0352</td>
<td>Knowledge of forms of intelligence support needs, topics, and focus areas.</td>
</tr>
<tr>
<td>K0353</td>
<td>Knowledge of possible circumstances that would result in changing collection management authorities.</td>
</tr>
<tr>
<td>K0354</td>
<td>Knowledge of relevant reporting and dissemination procedures.</td>
</tr>
<tr>
<td>K0355</td>
<td>Knowledge of all-source reporting and dissemination procedures.</td>
</tr>
<tr>
<td>K0356</td>
<td>Knowledge of analytic tools and techniques for language, voice and/or graphic material.</td>
</tr>
<tr>
<td>K0357</td>
<td>WITHDRAWN: Knowledge of analytical constructs and their use in assessing the operational environment. (See K0224)</td>
</tr>
<tr>
<td>K0358</td>
<td>Knowledge of analytical standards and the purpose of intelligence confidence levels.</td>
</tr>
<tr>
<td>K0359</td>
<td>Knowledge of approved intelligence dissemination processes.</td>
</tr>
<tr>
<td>K0361</td>
<td>Knowledge of asset availability, capabilities and limitations.</td>
</tr>
<tr>
<td>K0362</td>
<td>Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).</td>
</tr>
<tr>
<td>K0363</td>
<td>Knowledge of auditing and logging procedures (including server-based logging).</td>
</tr>
<tr>
<td>K0364</td>
<td>Knowledge of available databases and tools necessary to assess appropriate collection tasking.</td>
</tr>
<tr>
<td>K0368</td>
<td>Knowledge of implants that enable cyber collection and/or preparation activities.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0371</td>
<td>Knowledge of principles of the collection development processes (e.g., Dialed Number Recognition, Social Network Analysis).</td>
</tr>
<tr>
<td>K0372</td>
<td>Knowledge of programming concepts (e.g., levels, structures, compiled vs. interpreted languages).</td>
</tr>
<tr>
<td>K0373</td>
<td>Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.</td>
</tr>
<tr>
<td>K0374</td>
<td>WITHDRAWN: Knowledge of basic structure, architecture, and design of modern digital and telephony networks. (See K0599)</td>
</tr>
<tr>
<td>K0375</td>
<td>Knowledge of wireless applications vulnerabilities.</td>
</tr>
<tr>
<td>K0376</td>
<td>Knowledge of internal and external customers and partner organizations, including information needs, objectives, structure, capabilities, etc.</td>
</tr>
<tr>
<td>K0377</td>
<td>Knowledge of classification and control markings standards, policies and procedures.</td>
</tr>
<tr>
<td>K0379</td>
<td>Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.</td>
</tr>
<tr>
<td>K0380</td>
<td>Knowledge of collaborative tools and environments.</td>
</tr>
<tr>
<td>K0381</td>
<td>Knowledge of collateral damage and estimating impact(s).</td>
</tr>
<tr>
<td>K0382</td>
<td>Knowledge of collection capabilities and limitations.</td>
</tr>
<tr>
<td>K0383</td>
<td>Knowledge of collection capabilities, accesses, performance specifications, and constraints utilized to satisfy collection plan.</td>
</tr>
<tr>
<td>K0384</td>
<td>Knowledge of collection management functionality (e.g., positions, functions, responsibilities, products, reporting requirements).</td>
</tr>
<tr>
<td>K0386</td>
<td>Knowledge of collection management tools.</td>
</tr>
<tr>
<td>K0387</td>
<td>Knowledge of collection planning process and collection plan.</td>
</tr>
<tr>
<td>K0388</td>
<td>Knowledge of collection searching/analyzing techniques and tools for chat/buddy list, emerging technologies, VOIP, Media Over IP, VPN, VSAT/wireless, web mail and cookies.</td>
</tr>
<tr>
<td>K0389</td>
<td>Knowledge of collection sources including conventional and non-conventional sources.</td>
</tr>
<tr>
<td>K0390</td>
<td>Knowledge of collection strategies.</td>
</tr>
<tr>
<td>K0391</td>
<td>Knowledge of collection systems, capabilities, and processes.</td>
</tr>
<tr>
<td>K0392</td>
<td>Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).</td>
</tr>
<tr>
<td>K0393</td>
<td>Knowledge of common networking devices and their configurations.</td>
</tr>
<tr>
<td>K0394</td>
<td>Knowledge of common reporting databases and tools.</td>
</tr>
<tr>
<td>K0395</td>
<td>Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).</td>
</tr>
<tr>
<td>K0396</td>
<td>Knowledge of computer programming concepts, including computer languages, programming, testing, debugging, and file types.</td>
</tr>
<tr>
<td>K0397</td>
<td>Knowledge of security concepts in operating systems (e.g., Linux, Unix.)</td>
</tr>
<tr>
<td>K0398</td>
<td>Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).</td>
</tr>
<tr>
<td>K0399</td>
<td>Knowledge of crisis action planning and time sensitive planning procedures.</td>
</tr>
<tr>
<td>K0400</td>
<td>Knowledge of crisis action planning for cyber operations.</td>
</tr>
<tr>
<td>K0401</td>
<td>Knowledge of criteria for evaluating collection products.</td>
</tr>
<tr>
<td>K0402</td>
<td>Knowledge of criticality and vulnerability factors (e.g., value, recuperation, cushion, countermeasures) for target selection and applicability to the cyber domain.</td>
</tr>
<tr>
<td>K0403</td>
<td>Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.</td>
</tr>
<tr>
<td>K0404</td>
<td>Knowledge of current collection requirements.</td>
</tr>
<tr>
<td>K0405</td>
<td>Knowledge of current computer-based intrusion sets.</td>
</tr>
<tr>
<td>K0406</td>
<td>Knowledge of current software and methodologies for active defense and system hardening.</td>
</tr>
<tr>
<td>K0407</td>
<td>Knowledge of customer information needs.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0408</td>
<td>Knowledge of cyber actions (i.e. cyber defense, information gathering, environment preparation, cyber-attack) principles, capabilities, limitations, and effects.</td>
</tr>
<tr>
<td>K0409</td>
<td>Knowledge of cyber intelligence/information collection capabilities and repositories.</td>
</tr>
<tr>
<td>K0410</td>
<td>Knowledge of cyber laws and their effect on Cyber planning.</td>
</tr>
<tr>
<td>K0411</td>
<td>Knowledge of cyber laws and legal considerations and their effect on cyber planning.</td>
</tr>
<tr>
<td>K0412</td>
<td>Knowledge of cyber lexicon/terminology</td>
</tr>
<tr>
<td>K0413</td>
<td>Knowledge of cyber operation objectives, policies, and legalities.</td>
</tr>
<tr>
<td>K0414</td>
<td>Knowledge of cyber operations support or enabling processes.</td>
</tr>
<tr>
<td>K0415</td>
<td>Knowledge of cyber operations terminology/lexicon.</td>
</tr>
<tr>
<td>K0416</td>
<td>Knowledge of cyber operations.</td>
</tr>
<tr>
<td>K0417</td>
<td>Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).</td>
</tr>
<tr>
<td>K0418</td>
<td>Knowledge of data flow process for terminal or environment collection.</td>
</tr>
<tr>
<td>K0419</td>
<td>Knowledge of database administration and maintenance.</td>
</tr>
<tr>
<td>K0420</td>
<td>Knowledge of database theory.</td>
</tr>
<tr>
<td>K0421</td>
<td>Knowledge of databases, portals and associated dissemination vehicles.</td>
</tr>
<tr>
<td>K0422</td>
<td>Knowledge of deconfliction processes and procedures.</td>
</tr>
<tr>
<td>K0423</td>
<td>Knowledge of deconfliction reporting to include external organization interaction.</td>
</tr>
<tr>
<td>K0424</td>
<td>Knowledge of denial and deception techniques.</td>
</tr>
<tr>
<td>K0425</td>
<td>Knowledge of different organization objectives at all levels, including subordinate, lateral and higher.</td>
</tr>
<tr>
<td>K0426</td>
<td>Knowledge of dynamic and deliberate targeting.</td>
</tr>
<tr>
<td>K0427</td>
<td>Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).</td>
</tr>
<tr>
<td>K0428</td>
<td>Knowledge of encryption algorithms and tools for wireless local area networks (WLANs).</td>
</tr>
<tr>
<td>K0429</td>
<td>Knowledge of enterprise-wide information management.</td>
</tr>
<tr>
<td>K0430</td>
<td>Knowledge of evasion strategies and techniques.</td>
</tr>
<tr>
<td>K0431</td>
<td>Knowledge of evolving/emerging communications technologies.</td>
</tr>
<tr>
<td>K0432</td>
<td>Knowledge of existing, emerging, and long-range issues related to cyber operations strategy, policy, and organization.</td>
</tr>
<tr>
<td>K0433</td>
<td>Knowledge of forensic implications of operating system structure and operations.</td>
</tr>
<tr>
<td>K0435</td>
<td>Knowledge of fundamental cyber concepts, principles, limitations, and effects.</td>
</tr>
<tr>
<td>K0436</td>
<td>Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber-attack, cyber defense), principles, capabilities, limitations, and effects.</td>
</tr>
<tr>
<td>K0437</td>
<td>Knowledge of general Supervisory control and data acquisition (SCADA) system components.</td>
</tr>
<tr>
<td>K0438</td>
<td>Knowledge of mobile cellular communications architecture (e.g., LTE, CDMA, GSM/EDGE and UMTS/HSPA).</td>
</tr>
<tr>
<td>K0439</td>
<td>Knowledge of governing authorities for targeting.</td>
</tr>
<tr>
<td>K0440</td>
<td>Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability.</td>
</tr>
<tr>
<td>K0442</td>
<td>Knowledge of how converged technologies impact cyber operations (e.g., digital, telephony, wireless).</td>
</tr>
<tr>
<td>K0443</td>
<td>WITHDRAWN: Knowledge of how hubs, switches, routers work together in the design of a network. (See K0143)</td>
</tr>
<tr>
<td>K0444</td>
<td>Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).</td>
</tr>
<tr>
<td>K0445</td>
<td>Knowledge of how modern digital and telephony networks impact cyber operations.</td>
</tr>
<tr>
<td>K0446</td>
<td>Knowledge of how modern wireless communications systems impact cyber operations.</td>
</tr>
<tr>
<td>K0447</td>
<td>Knowledge of how to collect, view, and identify essential information on targets of interest from metadata (e.g., email, http).</td>
</tr>
<tr>
<td>K0448</td>
<td>Knowledge of how to establish priorities for resources.</td>
</tr>
<tr>
<td>K0449</td>
<td>Knowledge of how to extract, analyze, and use metadata.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0451</td>
<td>Knowledge of identification and reporting processes.</td>
</tr>
<tr>
<td>K0452</td>
<td>Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.</td>
</tr>
<tr>
<td>K0453</td>
<td>Knowledge of indications and warning.</td>
</tr>
<tr>
<td>K0454</td>
<td>Knowledge of information needs.</td>
</tr>
<tr>
<td>K0455</td>
<td>Knowledge of information security concepts, facilitating technologies and methods.</td>
</tr>
<tr>
<td>K0456</td>
<td>Knowledge of intelligence capabilities and limitations.</td>
</tr>
<tr>
<td>K0457</td>
<td>Knowledge of intelligence confidence levels.</td>
</tr>
<tr>
<td>K0458</td>
<td>Knowledge of intelligence disciplines.</td>
</tr>
<tr>
<td>K0459</td>
<td>Knowledge of intelligence employment requirements (i.e., logistical, communications support, maneuverability, legal restrictions, etc.).</td>
</tr>
<tr>
<td>K0460</td>
<td>Knowledge of intelligence preparation of the environment and similar processes.</td>
</tr>
<tr>
<td>K0461</td>
<td>Knowledge of intelligence production processes.</td>
</tr>
<tr>
<td>K0462</td>
<td>Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.</td>
</tr>
<tr>
<td>K0463</td>
<td>Knowledge of intelligence requirements tasking systems.</td>
</tr>
<tr>
<td>K0464</td>
<td>Knowledge of intelligence support to planning, execution, and assessment.</td>
</tr>
<tr>
<td>K0465</td>
<td>Knowledge of internal and external partner cyber operations capabilities and tools.</td>
</tr>
<tr>
<td>K0466</td>
<td>Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information.</td>
</tr>
<tr>
<td>K0467</td>
<td>Knowledge of internal and external partner organization capabilities and limitations (those with tasking, collection, processing, exploitation and dissemination responsibilities).</td>
</tr>
<tr>
<td>K0468</td>
<td>Knowledge of internal and external partner reporting.</td>
</tr>
<tr>
<td>K0469</td>
<td>Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.</td>
</tr>
<tr>
<td>K0470</td>
<td>Knowledge of Internet and routing protocols.</td>
</tr>
<tr>
<td>K0471</td>
<td>Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).</td>
</tr>
<tr>
<td>K0472</td>
<td>Knowledge of intrusion detection systems and signature development.</td>
</tr>
<tr>
<td>K0473</td>
<td>Knowledge of intrusion sets.</td>
</tr>
<tr>
<td>K0474</td>
<td>Knowledge of key cyber threat actors and their equities.</td>
</tr>
<tr>
<td>K0475</td>
<td>Knowledge of key factors of the operational environment and threat.</td>
</tr>
<tr>
<td>K0476</td>
<td>Knowledge of language processing tools and techniques.</td>
</tr>
<tr>
<td>K0477</td>
<td>Knowledge of leadership's Intent and objectives.</td>
</tr>
<tr>
<td>K0478</td>
<td>Knowledge of legal considerations in targeting.</td>
</tr>
<tr>
<td>K0479</td>
<td>Knowledge of malware analysis and characteristics.</td>
</tr>
<tr>
<td>K0480</td>
<td>Knowledge of malware.</td>
</tr>
<tr>
<td>K0481</td>
<td>Knowledge of methods and techniques used to detect various exploitation activities.</td>
</tr>
<tr>
<td>K0482</td>
<td>Knowledge of methods for ascertaining collection asset posture and availability.</td>
</tr>
<tr>
<td>K0483</td>
<td>Knowledge of methods to integrate and summarize information from any potential sources.</td>
</tr>
<tr>
<td>K0484</td>
<td>Knowledge of midpoint collection (process, objectives, organization, targets, etc.).</td>
</tr>
<tr>
<td>K0485</td>
<td>Knowledge of network administration.</td>
</tr>
<tr>
<td>K0486</td>
<td>Knowledge of network construction and topology.</td>
</tr>
<tr>
<td>K0487</td>
<td>Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).</td>
</tr>
<tr>
<td>K0488</td>
<td>Knowledge of network security implementations (e.g., host-based IDS, IPS, access control lists), including their function and placement in a network.</td>
</tr>
<tr>
<td>K0489</td>
<td>Knowledge of network topology.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0491</td>
<td>Knowledge of networking and Internet communications fundamentals (i.e. devices, device configuration, hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.).</td>
</tr>
<tr>
<td>K0492</td>
<td>Knowledge of non-traditional collection methodologies.</td>
</tr>
<tr>
<td>K0493</td>
<td>Knowledge of obfuscation techniques (e.g., TOR/Onion/anonymizers, VPN/VPS, encryption).</td>
</tr>
<tr>
<td>K0494</td>
<td>Knowledge of objectives, situation, operational environment, and the status and disposition of internal and external partner collection capabilities available to support planning.</td>
</tr>
<tr>
<td>K0495</td>
<td>Knowledge of ongoing and future operations.</td>
</tr>
<tr>
<td>K0496</td>
<td>Knowledge of operational asset constraints.</td>
</tr>
<tr>
<td>K0497</td>
<td>Knowledge of operational effectiveness assessment.</td>
</tr>
<tr>
<td>K0498</td>
<td>Knowledge of operational planning processes.</td>
</tr>
<tr>
<td>K0499</td>
<td>Knowledge of operations security.</td>
</tr>
<tr>
<td>K0500</td>
<td>Knowledge of organization and/or partner collection systems, capabilities, and processes (e.g., collection and protocol processors).</td>
</tr>
<tr>
<td>K0501</td>
<td>Knowledge of organization cyber operations programs, strategies, and resources.</td>
</tr>
<tr>
<td>K0502</td>
<td>Knowledge of organization decision support tools and/or methods.</td>
</tr>
<tr>
<td>K0503</td>
<td>Knowledge of organization formats of resource and asset readiness reporting, its operational relevance and intelligence collection impact.</td>
</tr>
<tr>
<td>K0504</td>
<td>Knowledge of organization issues, objectives, and operations in cyber as well as regulations and policy directives governing cyber operations.</td>
</tr>
<tr>
<td>K0505</td>
<td>Knowledge of organization objectives and associated demand on collection management.</td>
</tr>
<tr>
<td>K0506</td>
<td>Knowledge of organization objectives, leadership priorities, and decision-making risks.</td>
</tr>
<tr>
<td>K0507</td>
<td>Knowledge of organization or partner exploitation of digital networks.</td>
</tr>
<tr>
<td>K0508</td>
<td>Knowledge of organization policies and planning concepts for partnering with internal and/or external organizations.</td>
</tr>
<tr>
<td>K0509</td>
<td>Knowledge of organizational and partner authorities, responsibilities, and contributions to achieving objectives.</td>
</tr>
<tr>
<td>K0510</td>
<td>Knowledge of organizational and partner policies, tools, capabilities, and procedures.</td>
</tr>
<tr>
<td>K0511</td>
<td>Knowledge of organizational hierarchy and cyber decision-making processes.</td>
</tr>
<tr>
<td>K0512</td>
<td>Knowledge of organizational planning concepts.</td>
</tr>
<tr>
<td>K0513</td>
<td>Knowledge of organizational priorities, legal authorities and requirements submission processes.</td>
</tr>
<tr>
<td>K0514</td>
<td>Knowledge of organizational structures and associated intelligence capabilities.</td>
</tr>
<tr>
<td>K0516</td>
<td>Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.</td>
</tr>
<tr>
<td>K0517</td>
<td>Knowledge of post implementation review (PIR) approval process.</td>
</tr>
<tr>
<td>K0518</td>
<td>Knowledge of planning activity initiation.</td>
</tr>
<tr>
<td>K0519</td>
<td>Knowledge of planning timelines adaptive, crisis action, and time-sensitive planning.</td>
</tr>
<tr>
<td>K0520</td>
<td>Knowledge of principles and practices related to target development such as target knowledge, associations, communication systems, and infrastructure.</td>
</tr>
<tr>
<td>K0521</td>
<td>Knowledge of priority information, how it is derived, where it is published, how to access, etc.</td>
</tr>
<tr>
<td>K0522</td>
<td>Knowledge of production exploitation and dissemination needs and architectures.</td>
</tr>
<tr>
<td>K0523</td>
<td>Knowledge of products and nomenclature of major vendors (e.g., security suites - Trend Micro, Symantec, McAfee, Outpost, and Panda) and how those products affect exploitation and reduce vulnerabilities.</td>
</tr>
<tr>
<td>K0524</td>
<td>Knowledge of relevant laws, regulations, and policies.</td>
</tr>
<tr>
<td>K0525</td>
<td>Knowledge of required intelligence planning products associated with cyber operational planning.</td>
</tr>
<tr>
<td>K0526</td>
<td>Knowledge of research strategies and knowledge management.</td>
</tr>
<tr>
<td>K0527</td>
<td>Knowledge of risk management and mitigation strategies.</td>
</tr>
<tr>
<td>K0528</td>
<td>Knowledge of satellite-based communication systems.</td>
</tr>
<tr>
<td>K0529</td>
<td>Knowledge of scripting</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0530</td>
<td>Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation.</td>
</tr>
<tr>
<td>K0531</td>
<td>Knowledge of security implications of software configurations.</td>
</tr>
<tr>
<td>K0532</td>
<td>Knowledge of specialized target language (e.g., acronyms, jargon, technical terminology, code words).</td>
</tr>
<tr>
<td>K0533</td>
<td>Knowledge of specific target identifiers, and their usage.</td>
</tr>
<tr>
<td>K0534</td>
<td>Knowledge of staff management, assignment, and allocation processes.</td>
</tr>
<tr>
<td>K0535</td>
<td>Knowledge of strategies and tools for target research.</td>
</tr>
<tr>
<td>K0536</td>
<td>Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).</td>
</tr>
<tr>
<td>K0538</td>
<td>Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities.</td>
</tr>
<tr>
<td>K0539</td>
<td>Knowledge of target communication profiles and their key elements (e.g., target associations, activities, communication infrastructure).</td>
</tr>
<tr>
<td>K0540</td>
<td>Knowledge of target communication tools and techniques.</td>
</tr>
<tr>
<td>K0541</td>
<td>Knowledge of target cultural references, dialects, expressions, idioms, and abbreviations.</td>
</tr>
<tr>
<td>K0542</td>
<td>Knowledge of target development (i.e., concepts, roles, responsibilities, products, etc.).</td>
</tr>
<tr>
<td>K0543</td>
<td>Knowledge of target estimated repair and recuperation times.</td>
</tr>
<tr>
<td>K0544</td>
<td>Knowledge of target intelligence gathering and operational preparation techniques and life cycles.</td>
</tr>
<tr>
<td>K0545</td>
<td>Knowledge of target language(s).</td>
</tr>
<tr>
<td>K0546</td>
<td>Knowledge of target list development (i.e. Restricted, Joint, Candidate, etc.).</td>
</tr>
<tr>
<td>K0547</td>
<td>Knowledge of target methods and procedures.</td>
</tr>
<tr>
<td>K0548</td>
<td>Knowledge of target or threat cyber actors and procedures.</td>
</tr>
<tr>
<td>K0549</td>
<td>Knowledge of target vetting and validation procedures.</td>
</tr>
<tr>
<td>K0550</td>
<td>Knowledge of target, including related current events, communication profile, actors, and history (language, culture) and/or frame of reference.</td>
</tr>
<tr>
<td>K0551</td>
<td>Knowledge of targeting cycles.</td>
</tr>
<tr>
<td>K0552</td>
<td>Knowledge of tasking mechanisms.</td>
</tr>
<tr>
<td>K0553</td>
<td>Knowledge of tasking processes for organic and subordinate collection assets.</td>
</tr>
<tr>
<td>K0554</td>
<td>Knowledge of tasking, collection, processing, exploitation and dissemination.</td>
</tr>
<tr>
<td>K0555</td>
<td>Knowledge of TCP/IP networking protocols.</td>
</tr>
<tr>
<td>K0556</td>
<td>Knowledge of telecommunications fundamentals.</td>
</tr>
<tr>
<td>K0557</td>
<td>Knowledge of terminal or environmental collection (process, objectives, organization, targets, etc.).</td>
</tr>
<tr>
<td>K0558</td>
<td>Knowledge of the available tools and applications associated with collection requirements and collection management.</td>
</tr>
<tr>
<td>K0559</td>
<td>Knowledge of the basic structure, architecture, and design of converged applications.</td>
</tr>
<tr>
<td>K0560</td>
<td>Knowledge of the basic structure, architecture, and design of modern communication networks.</td>
</tr>
<tr>
<td>K0561</td>
<td>Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).</td>
</tr>
<tr>
<td>K0562</td>
<td>Knowledge of the capabilities and limitations of new and emerging collection capabilities, accesses and/or processes.</td>
</tr>
<tr>
<td>K0563</td>
<td>Knowledge of the capabilities, limitations and tasking methodologies of internal and external collections as they apply to planned cyber activities.</td>
</tr>
<tr>
<td>K0564</td>
<td>Knowledge of the characteristics of targeted communication networks (e.g., capacity, functionality, paths, critical nodes).</td>
</tr>
<tr>
<td>K0565</td>
<td>Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.</td>
</tr>
<tr>
<td>K0566</td>
<td>Knowledge of the critical information requirements and how they're used in planning.</td>
</tr>
<tr>
<td>K0567</td>
<td>Knowledge of the data flow from collection origin to repositories and tools.</td>
</tr>
<tr>
<td>K0568</td>
<td>Knowledge of the definition of collection management and collection management authority.</td>
</tr>
<tr>
<td>K0569</td>
<td>Knowledge of the existent tasking, collection, processing, exploitation and dissemination architecture.</td>
</tr>
<tr>
<td>Knowledge ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>K0570</td>
<td>Knowledge of the factors of threat that could impact collection operations.</td>
</tr>
<tr>
<td>K0571</td>
<td>Knowledge of the feedback cycle in collection processes.</td>
</tr>
<tr>
<td>K0572</td>
<td>Knowledge of the functions and capabilities of internal teams that emulate threat activities to benefit the organization.</td>
</tr>
<tr>
<td>K0573</td>
<td>Knowledge of the fundamentals of digital forensics to extract actionable intelligence.</td>
</tr>
<tr>
<td>K0574</td>
<td>Knowledge of the impact of language analysis on on-net operator functions.</td>
</tr>
<tr>
<td>K0575</td>
<td>Knowledge of the impacts of internal and external partner staffing estimates.</td>
</tr>
<tr>
<td>K0576</td>
<td>Knowledge of the information environment.</td>
</tr>
<tr>
<td>K0577</td>
<td>Knowledge of the intelligence frameworks, processes, and related systems.</td>
</tr>
<tr>
<td>K0578</td>
<td>Knowledge of the intelligence requirements development and request for information processes.</td>
</tr>
<tr>
<td>K0579</td>
<td>Knowledge of the organization, roles and responsibilities of higher, lower and adjacent sub-elements.</td>
</tr>
<tr>
<td>K0580</td>
<td>Knowledge of the organization's established format for collection plan.</td>
</tr>
<tr>
<td>K0581</td>
<td>Knowledge of the organization's planning, operations and targeting cycles.</td>
</tr>
<tr>
<td>K0582</td>
<td>Knowledge of the organizational planning and staffing process.</td>
</tr>
<tr>
<td>K0583</td>
<td>Knowledge of the organizational plans/directives/guidance that describe objectives.</td>
</tr>
<tr>
<td>K0584</td>
<td>Knowledge of the organizational policies/procedures for temporary transfer of collection authority.</td>
</tr>
<tr>
<td>K0585</td>
<td>Knowledge of the organizational structure as it pertains to full spectrum cyber operations, including the functions, responsibilities, and interrelationships among distinct internal elements.</td>
</tr>
<tr>
<td>K0586</td>
<td>Knowledge of the outputs of course of action and exercise analysis.</td>
</tr>
<tr>
<td>K0587</td>
<td>Knowledge of the POC's, databases, tools and applications necessary to establish environment preparation and surveillance products.</td>
</tr>
<tr>
<td>K0588</td>
<td>Knowledge of the priority information requirements from subordinate, lateral and higher levels of the organization.</td>
</tr>
<tr>
<td>K0589</td>
<td>Knowledge of the process used to assess the performance and impact of operations.</td>
</tr>
<tr>
<td>K0590</td>
<td>Knowledge of the processes to synchronize operational assessment procedures with the critical information requirement process.</td>
</tr>
<tr>
<td>K0591</td>
<td>Knowledge of the production responsibilities and organic analysis and production capabilities.</td>
</tr>
<tr>
<td>K0592</td>
<td>Knowledge of the purpose and contribution of target templates.</td>
</tr>
<tr>
<td>K0593</td>
<td>Knowledge of the range of cyber operations and their underlying intelligence support needs, topics, and focus areas.</td>
</tr>
<tr>
<td>K0594</td>
<td>Knowledge of the relationships between end states, objectives, effects, lines of operation, etc.</td>
</tr>
<tr>
<td>K0595</td>
<td>Knowledge of the relationships of operational objectives, intelligence requirements, and intelligence production tasks.</td>
</tr>
<tr>
<td>K0596</td>
<td>Knowledge of the request for information process.</td>
</tr>
<tr>
<td>K0597</td>
<td>Knowledge of the role of network operations in supporting and facilitating other organization operations.</td>
</tr>
<tr>
<td>K0598</td>
<td>Knowledge of the structure and intent of organization specific plans, guidance and authorizations.</td>
</tr>
<tr>
<td>K0599</td>
<td>Knowledge of the structure, architecture, and design of modern digital and telephony networks.</td>
</tr>
<tr>
<td>K0600</td>
<td>Knowledge of the structure, architecture, and design of modern wireless communications systems.</td>
</tr>
<tr>
<td>K0601</td>
<td>Knowledge of the systems/architecture/communications used for coordination.</td>
</tr>
<tr>
<td>K0602</td>
<td>Knowledge of collection disciplines and capabilities.</td>
</tr>
<tr>
<td>K0603</td>
<td>Knowledge of the ways in which targets or threats use the Internet.</td>
</tr>
<tr>
<td>K0604</td>
<td>Knowledge of threat and/or target systems.</td>
</tr>
<tr>
<td>K0605</td>
<td>Knowledge of tipping, cueing, mixing, and redundancy.</td>
</tr>
<tr>
<td>K0606</td>
<td>Knowledge of transcript development processes and techniques (e.g., verbatim, gist, summaries).</td>
</tr>
<tr>
<td>K0607</td>
<td>Knowledge of translation processes and techniques.</td>
</tr>
<tr>
<td>K0608</td>
<td>Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).</td>
</tr>
</tbody>
</table>
## Knowledge ID Description

<table>
<thead>
<tr>
<th>Knowledge ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0609</td>
<td>Knowledge of virtual machine technologies.</td>
</tr>
<tr>
<td>K0610</td>
<td>Knowledge of virtualization products (VMware, Virtual PC).</td>
</tr>
<tr>
<td>K0612</td>
<td>Knowledge of what constitutes a “threat” to a network.</td>
</tr>
<tr>
<td>K0613</td>
<td>Knowledge of who the organization's operational planners are, how and where they can be contacted, and what are their expectations.</td>
</tr>
<tr>
<td>K0614</td>
<td>Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.</td>
</tr>
<tr>
<td>K0615</td>
<td>Knowledge of privacy disclosure statements based on current laws.</td>
</tr>
<tr>
<td>K0622</td>
<td>Knowledge of controls related to the use, processing, storage, and transmission of data.</td>
</tr>
<tr>
<td>K0624</td>
<td>Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)</td>
</tr>
<tr>
<td>K0628</td>
<td>Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.</td>
</tr>
</tbody>
</table>

## Skill ID Description

<table>
<thead>
<tr>
<th>Skill ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0001</td>
<td>Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.</td>
</tr>
<tr>
<td>S0002</td>
<td>Skill in allocating storage capacity in the design of data management systems.</td>
</tr>
<tr>
<td>S0003</td>
<td>Skill of identifying, capturing, containing, and reporting malware.</td>
</tr>
<tr>
<td>S0004</td>
<td>Skill in analyzing network traffic capacity and performance characteristics.</td>
</tr>
<tr>
<td>S0005</td>
<td>Skill in applying and incorporating information technologies into proposed solutions.</td>
</tr>
<tr>
<td>S0006</td>
<td>Skill in applying confidentiality, integrity, and availability principles.</td>
</tr>
<tr>
<td>S0007</td>
<td>Skill in applying host/network access controls (e.g., access control list).</td>
</tr>
<tr>
<td>S0008</td>
<td>Skill in applying organization-specific systems analysis principles and techniques.</td>
</tr>
<tr>
<td>S0009</td>
<td>WITHDRAWN: Skill in assessing the robustness of security systems and designs. (See S0027)</td>
</tr>
<tr>
<td>S0010</td>
<td>Skill in conducting capabilities and requirements analysis.</td>
</tr>
<tr>
<td>S0011</td>
<td>Skill in conducting information searches.</td>
</tr>
<tr>
<td>S0012</td>
<td>Skill in conducting knowledge mapping (e.g., map of knowledge repositories).</td>
</tr>
<tr>
<td>S0013</td>
<td>Skill in conducting queries and developing algorithms to analyze data structures.</td>
</tr>
<tr>
<td>S0014</td>
<td>Skill in conducting software debugging.</td>
</tr>
<tr>
<td>S0015</td>
<td>Skill in conducting test events.</td>
</tr>
<tr>
<td>S0016</td>
<td>Skill in configuring and optimizing software.</td>
</tr>
<tr>
<td>S0017</td>
<td>Skill in creating and utilizing mathematical or statistical models.</td>
</tr>
<tr>
<td>S0018</td>
<td>Skill in creating policies that reflect system security objectives.</td>
</tr>
<tr>
<td>S0019</td>
<td>Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.</td>
</tr>
<tr>
<td>S0020</td>
<td>Skill in developing and deploying signatures.</td>
</tr>
<tr>
<td>S0021</td>
<td>Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data).</td>
</tr>
<tr>
<td>S0022</td>
<td>Skill in designing countermeasures to identified security risks.</td>
</tr>
<tr>
<td>S0023</td>
<td>Skill in designing security controls based on cybersecurity principles and tenets.</td>
</tr>
<tr>
<td>S0024</td>
<td>Skill in designing the integration of hardware and software solutions.</td>
</tr>
<tr>
<td>S0025</td>
<td>Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).</td>
</tr>
<tr>
<td>S0026</td>
<td>Skill in determining an appropriate level of test rigor for a given system.</td>
</tr>
<tr>
<td>S0027</td>
<td>Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.</td>
</tr>
<tr>
<td>S0028</td>
<td>Skill in developing data dictionaries.</td>
</tr>
<tr>
<td>Skill ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>S0029</td>
<td>Skill in developing data models.</td>
</tr>
<tr>
<td>S0030</td>
<td>Skill in developing operations-based testing scenarios.</td>
</tr>
<tr>
<td>S0031</td>
<td>Skill in developing and applying security system access controls.</td>
</tr>
<tr>
<td>S0032</td>
<td>Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.</td>
</tr>
<tr>
<td>S0033</td>
<td>Skill in diagnosing connectivity problems.</td>
</tr>
<tr>
<td>S0034</td>
<td>Skill in discerning the protection needs (i.e., security controls) of information systems and networks.</td>
</tr>
<tr>
<td>S0035</td>
<td>Skill in establishing a routing schema.</td>
</tr>
<tr>
<td>S0036</td>
<td>Skill in evaluating the adequacy of security designs.</td>
</tr>
<tr>
<td>S0037</td>
<td>Skill in generating queries and reports.</td>
</tr>
<tr>
<td>S0038</td>
<td>Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.</td>
</tr>
<tr>
<td>S0039</td>
<td>Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.</td>
</tr>
<tr>
<td>S0040</td>
<td>Skill in implementing, maintaining, and improving established network security practices.</td>
</tr>
<tr>
<td>S0041</td>
<td>Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.</td>
</tr>
<tr>
<td>S0042</td>
<td>Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.).</td>
</tr>
<tr>
<td>S0043</td>
<td>Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).</td>
</tr>
<tr>
<td>S0044</td>
<td>Skill in mimicking threat behaviors.</td>
</tr>
<tr>
<td>S0045</td>
<td>Skill in optimizing database performance.</td>
</tr>
<tr>
<td>S0046</td>
<td>Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).</td>
</tr>
<tr>
<td>S0047</td>
<td>Skill in preserving evidence integrity according to standard operating procedures or national standards.</td>
</tr>
<tr>
<td>S0048</td>
<td>Skill in systems integration testing.</td>
</tr>
<tr>
<td>S0049</td>
<td>Skill in the measuring and reporting of intellectual capital.</td>
</tr>
<tr>
<td>S0050</td>
<td>Skill in design modeling and building use cases (e.g., unified modeling language).</td>
</tr>
<tr>
<td>S0051</td>
<td>Skill in the use of penetration testing tools and techniques.</td>
</tr>
<tr>
<td>S0052</td>
<td>Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).</td>
</tr>
<tr>
<td>S0053</td>
<td>Skill in tuning sensors.</td>
</tr>
<tr>
<td>S0054</td>
<td>Skill in using incident handling methodologies.</td>
</tr>
<tr>
<td>S0055</td>
<td>Skill in using knowledge management technologies.</td>
</tr>
<tr>
<td>S0056</td>
<td>Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).</td>
</tr>
<tr>
<td>S0057</td>
<td>Skill in using protocol analyzers.</td>
</tr>
<tr>
<td>S0058</td>
<td>Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.</td>
</tr>
<tr>
<td>S0059</td>
<td>Skill in using Virtual Private Network (VPN) devices and encryption.</td>
</tr>
<tr>
<td>S0060</td>
<td>Skill in writing code in a currently supported programming language (e.g., Java, C++).</td>
</tr>
<tr>
<td>S0061</td>
<td>Skill in writing test plans.</td>
</tr>
<tr>
<td>S0062</td>
<td>Skill in analyzing memory dumps to extract information.</td>
</tr>
<tr>
<td>S0063</td>
<td>Skill in collecting data from a variety of cyber defense resources.</td>
</tr>
<tr>
<td>S0064</td>
<td>Skill in developing and executing technical training programs and curricula.</td>
</tr>
<tr>
<td>S0065</td>
<td>Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).</td>
</tr>
<tr>
<td>S0066</td>
<td>Skill in identifying gaps in technical capabilities.</td>
</tr>
<tr>
<td>S0067</td>
<td>Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).</td>
</tr>
<tr>
<td>S0068</td>
<td>Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.</td>
</tr>
<tr>
<td>Skill ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>S0069</td>
<td>Skill in setting up a forensic workstation.</td>
</tr>
<tr>
<td>S0070</td>
<td>Skill in talking to others to convey information effectively.</td>
</tr>
<tr>
<td>S0071</td>
<td>Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).</td>
</tr>
<tr>
<td>S0072</td>
<td>Skill in using scientific rules and methods to solve problems.</td>
</tr>
<tr>
<td>S0073</td>
<td>Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).</td>
</tr>
<tr>
<td>S0074</td>
<td>Skill in physically disassembling PCs.</td>
</tr>
<tr>
<td>S0075</td>
<td>Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).</td>
</tr>
<tr>
<td>S0076</td>
<td>Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).</td>
</tr>
<tr>
<td>S0077</td>
<td>Skill in securing network communications.</td>
</tr>
<tr>
<td>S0078</td>
<td>Skill in recognizing and categorizing types of vulnerabilities and associated attacks.</td>
</tr>
<tr>
<td>S0079</td>
<td>Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).</td>
</tr>
<tr>
<td>S0080</td>
<td>Skill in performing damage assessments.</td>
</tr>
<tr>
<td>S0081</td>
<td>Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).</td>
</tr>
<tr>
<td>S0082</td>
<td>Skill in evaluating test plans for applicability and completeness.</td>
</tr>
<tr>
<td>S0083</td>
<td>Skill in integrating black box security testing tools into quality assurance process of software releases.</td>
</tr>
<tr>
<td>S0084</td>
<td>Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).</td>
</tr>
<tr>
<td>S0085</td>
<td>Skill in conducting audits or reviews of technical systems.</td>
</tr>
<tr>
<td>S0086</td>
<td>Skill in evaluating the trustworthiness of the supplier and/or product.</td>
</tr>
<tr>
<td>S0087</td>
<td>Skill in deep analysis of captured malicious code (e.g., malware forensics).</td>
</tr>
<tr>
<td>S0088</td>
<td>Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).</td>
</tr>
<tr>
<td>S0089</td>
<td>Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).</td>
</tr>
<tr>
<td>S0090</td>
<td>Skill in analyzing anomalous code as malicious or benign.</td>
</tr>
<tr>
<td>S0091</td>
<td>Skill in analyzing volatile data.</td>
</tr>
<tr>
<td>S0092</td>
<td>Skill in identifying obfuscation techniques.</td>
</tr>
<tr>
<td>S0093</td>
<td>Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.</td>
</tr>
<tr>
<td>S0094</td>
<td>Skill in reading Hexadecimal data.</td>
</tr>
<tr>
<td>S0095</td>
<td>Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode).</td>
</tr>
<tr>
<td>S0096</td>
<td>Skill in reading and interpreting signatures (e.g., snort).</td>
</tr>
<tr>
<td>S0097</td>
<td>Skill in applying security controls.</td>
</tr>
<tr>
<td>S0098</td>
<td>WITHDRAWN: Skill in detecting host and network based intrusions via intrusion detection technologies. (See S0025)</td>
</tr>
<tr>
<td>S0100</td>
<td>Skill in utilizing or developing learning activities (e.g., scenarios, instructional games, interactive exercises).</td>
</tr>
<tr>
<td>S0101</td>
<td>Skill in utilizing technologies (e.g., SmartBoards, websites, computers, projectors) for instructional purposes.</td>
</tr>
<tr>
<td>S0102</td>
<td>Skill in applying technical delivery capabilities.</td>
</tr>
<tr>
<td>S0103</td>
<td>Skill in assessing the predictive power and subsequent generalizability of a model.</td>
</tr>
<tr>
<td>S0104</td>
<td>Skill in conducting Test Readiness Reviews.</td>
</tr>
<tr>
<td>S0106</td>
<td>Skill in data pre-processing (e.g., imputation, dimensionality reduction, normalization, transformation, extraction, filtering, smoothing).</td>
</tr>
<tr>
<td>S0107</td>
<td>Skill in designing and documenting overall program Test &amp; Evaluation strategies.</td>
</tr>
<tr>
<td>S0108</td>
<td>Skill in developing workforce and position qualification standards.</td>
</tr>
<tr>
<td>S0109</td>
<td>Skill in identifying hidden patterns or relationships.</td>
</tr>
<tr>
<td>S0110</td>
<td>Skill in identifying Test &amp; Evaluation infrastructure (people, ranges, tools, instrumentation) requirements.</td>
</tr>
<tr>
<td>Skill ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>S0111</td>
<td>Skill in interfacing with customers.</td>
</tr>
<tr>
<td>S0112</td>
<td>Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events.</td>
</tr>
<tr>
<td>S0113</td>
<td>Skill in performing format conversions to create a standard representation of the data.</td>
</tr>
<tr>
<td>S0114</td>
<td>Skill in performing sensitivity analysis.</td>
</tr>
<tr>
<td>S0115</td>
<td>Skill in preparing Test &amp; Evaluation reports.</td>
</tr>
<tr>
<td>S0116</td>
<td>Skill in designing multi-level security/cross domain solutions.</td>
</tr>
<tr>
<td>S0117</td>
<td>Skill in providing Test &amp; Evaluation resource estimate.</td>
</tr>
<tr>
<td>S0118</td>
<td>Skill in developing machine understandable semantic ontologies.</td>
</tr>
<tr>
<td>S0119</td>
<td>Skill in Regression Analysis (e.g., Hierarchical Stepwise, Generalized Linear Model, Ordinary Least Squares, Tree-Based Methods, Logistic).</td>
</tr>
<tr>
<td>S0120</td>
<td>Skill in reviewing logs to identify evidence of past intrusions.</td>
</tr>
<tr>
<td>S0121</td>
<td>Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).</td>
</tr>
<tr>
<td>S0122</td>
<td>Skill in the use of design methods.</td>
</tr>
<tr>
<td>S0123</td>
<td>Skill in transformation analytics (e.g., aggregation, enrichment, processing).</td>
</tr>
<tr>
<td>S0124</td>
<td>Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.</td>
</tr>
<tr>
<td>S0125</td>
<td>Skill in using basic descriptive statistics and techniques (e.g., normality, model distribution, scatter plots).</td>
</tr>
<tr>
<td>S0126</td>
<td>Skill in using data analysis tools (e.g., Excel, STATA SAS, SPSS).</td>
</tr>
<tr>
<td>S0127</td>
<td>Skill in using data mapping tools.</td>
</tr>
<tr>
<td>S0128</td>
<td>Skill in using manpower and personnel IT systems.</td>
</tr>
<tr>
<td>S0129</td>
<td>Skill in using outlier identification and removal techniques.</td>
</tr>
<tr>
<td>S0130</td>
<td>Skill in writing scripts using R, Python, PIG, HIVE, SQL, etc.</td>
</tr>
<tr>
<td>S0131</td>
<td>Skill in analyzing malware.</td>
</tr>
<tr>
<td>S0132</td>
<td>Skill in conducting bit-level analysis.</td>
</tr>
<tr>
<td>S0133</td>
<td>Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.</td>
</tr>
<tr>
<td>S0134</td>
<td>Skill in conducting reviews of systems.</td>
</tr>
<tr>
<td>S0135</td>
<td>Skill in secure test plan design (e.g. unit, integration, system, acceptance).</td>
</tr>
<tr>
<td>S0136</td>
<td>Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.</td>
</tr>
<tr>
<td>S0137</td>
<td>Skill in conducting application vulnerability assessments.</td>
</tr>
<tr>
<td>S0138</td>
<td>Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).</td>
</tr>
<tr>
<td>S0139</td>
<td>Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).</td>
</tr>
<tr>
<td>S0140</td>
<td>Skill in applying the systems engineering process.</td>
</tr>
<tr>
<td>S0141</td>
<td>Skill in assessing security systems designs.</td>
</tr>
<tr>
<td>S0142</td>
<td>Skill in conducting research for troubleshooting novel client-level problems.</td>
</tr>
<tr>
<td>S0143</td>
<td>Skill in conducting system/server planning, management, and maintenance.</td>
</tr>
<tr>
<td>S0144</td>
<td>Skill in correcting physical and technical problems that impact system/server performance.</td>
</tr>
<tr>
<td>S0145</td>
<td>Skill in integrating and applying policies that meet system security objectives.</td>
</tr>
<tr>
<td>S0146</td>
<td>Skill in creating policies that enable systems to meet performance objectives (e.g. traffic routing, SLA’s, CPU specifications).</td>
</tr>
<tr>
<td>S0147</td>
<td>Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).</td>
</tr>
<tr>
<td>S0148</td>
<td>Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.</td>
</tr>
<tr>
<td>S0149</td>
<td>Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.</td>
</tr>
<tr>
<td>Skill ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>S0150</td>
<td>Skill in implementing and testing network infrastructure contingency and recovery plans.</td>
</tr>
<tr>
<td>S0151</td>
<td>Skill in troubleshooting failed system components (i.e., servers).</td>
</tr>
<tr>
<td>S0152</td>
<td>Skill in translating operational requirements into protection needs (i.e., security controls).</td>
</tr>
<tr>
<td>S0153</td>
<td>Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.</td>
</tr>
<tr>
<td>S0154</td>
<td>Skill in installing system and component upgrades. (i.e., servers, appliances, network devices).</td>
</tr>
<tr>
<td>S0155</td>
<td>Skill in monitoring and optimizing system/server performance.</td>
</tr>
<tr>
<td>S0156</td>
<td>Skill in performing packet-level analysis.</td>
</tr>
<tr>
<td>S0157</td>
<td>Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.).</td>
</tr>
<tr>
<td>S0158</td>
<td>Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).</td>
</tr>
<tr>
<td>S0159</td>
<td>Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.</td>
</tr>
<tr>
<td>S0160</td>
<td>Skill in the use of design modeling (e.g., unified modeling language).</td>
</tr>
<tr>
<td>S0162</td>
<td>Skill in applying various subnet techniques (e.g., CIDR).</td>
</tr>
<tr>
<td>S0166</td>
<td>Skill in identifying gaps in technical delivery capabilities.</td>
</tr>
<tr>
<td>S0167</td>
<td>Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).</td>
</tr>
<tr>
<td>S0168</td>
<td>Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks.</td>
</tr>
<tr>
<td>S0169</td>
<td>Skill in conducting trend analysis.</td>
</tr>
<tr>
<td>S0170</td>
<td>Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).</td>
</tr>
<tr>
<td>S0171</td>
<td>Skill in performing impact/risk assessments.</td>
</tr>
<tr>
<td>S0172</td>
<td>Skill in applying secure coding techniques.</td>
</tr>
<tr>
<td>S0173</td>
<td>Skill in using security event correlation tools.</td>
</tr>
<tr>
<td>S0174</td>
<td>Skill in using code analysis tools.</td>
</tr>
<tr>
<td>S0175</td>
<td>Skill in performing root cause analysis.</td>
</tr>
<tr>
<td>S0176</td>
<td>Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.</td>
</tr>
<tr>
<td>S0177</td>
<td>Skill in analyzing a target’s communication networks.</td>
</tr>
<tr>
<td>S0178</td>
<td>Skill in analyzing essential network data (e.g., router configuration files, routing protocols).</td>
</tr>
<tr>
<td>S0179</td>
<td>Skill in analyzing language processing tools to provide feedback to enhance tool development.</td>
</tr>
<tr>
<td>S0181</td>
<td>Skill in analyzing midpoint collection data.</td>
</tr>
<tr>
<td>S0182</td>
<td>Skill in analyzing target communications internals and externals collected from wireless LANs.</td>
</tr>
<tr>
<td>S0183</td>
<td>Skill in analyzing terminal or environment collection data.</td>
</tr>
<tr>
<td>S0184</td>
<td>Skill in analyzing traffic to identify network devices.</td>
</tr>
<tr>
<td>S0185</td>
<td>Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.</td>
</tr>
<tr>
<td>S0186</td>
<td>Skill in applying crisis planning procedures.</td>
</tr>
<tr>
<td>S0187</td>
<td>Skill in applying various analytical methods, tools, and techniques (e.g., competing hypotheses; chain of reasoning; scenario methods; denial and deception detection; high impact-low probability; network/association or link analysis; Bayesian, Delphi, and Pattern analyses).</td>
</tr>
<tr>
<td>S0188</td>
<td>Skill in assessing a target’s frame of reference (e.g., motivation, technical capability, organizational structure, sensitivities).</td>
</tr>
<tr>
<td>S0189</td>
<td>Skill in assessing and/or estimating effects generated during and after cyber operations.</td>
</tr>
<tr>
<td>S0190</td>
<td>Skill in assessing current tools to identify needed improvements.</td>
</tr>
<tr>
<td>S0191</td>
<td>Skill in assessing the applicability of available analytical tools to various situations.</td>
</tr>
<tr>
<td>S0192</td>
<td>Skill in auditing firewalls, perimeters, routers, and intrusion detection systems.</td>
</tr>
<tr>
<td>Skill ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>S0193</td>
<td>Skill in complying with the legal restrictions for targeted information.</td>
</tr>
<tr>
<td>S0194</td>
<td>Skill in conducting non-attributable research.</td>
</tr>
<tr>
<td>S0195</td>
<td>Skill in conducting research using all available sources.</td>
</tr>
<tr>
<td>S0196</td>
<td>Skill in conducting research using deep web.</td>
</tr>
<tr>
<td>S0197</td>
<td>Skill in conducting social network analysis, buddy list analysis, and/or cookie analysis.</td>
</tr>
<tr>
<td>S0198</td>
<td>Skill in conducting social network analysis.</td>
</tr>
<tr>
<td>S0199</td>
<td>Skill in creating and extracting important information from packet captures.</td>
</tr>
<tr>
<td>S0200</td>
<td>Skill in creating collection requirements in support of data acquisition activities.</td>
</tr>
<tr>
<td>S0201</td>
<td>Skill in creating plans in support of remote operations. (i.e., hot/warm/cold/alternative sites, disaster recovery).</td>
</tr>
<tr>
<td>S0202</td>
<td>Skill in data mining techniques (e.g., searching file systems) and analysis.</td>
</tr>
<tr>
<td>S0203</td>
<td>Skill in defining and characterizing all pertinent aspects of the operational environment.</td>
</tr>
<tr>
<td>S0204</td>
<td>Skill in depicting source or collateral data on a network map.</td>
</tr>
<tr>
<td>S0205</td>
<td>Skill in determining appropriate targeting options through the evaluation of available capabilities against desired effects.</td>
</tr>
<tr>
<td>S0206</td>
<td>Skill in determining installed patches on various operating systems and identifying patch signatures.</td>
</tr>
<tr>
<td>S0207</td>
<td>Skill in determining the effect of various router and firewall configurations on traffic patterns and network performance in both LAN and WAN environments.</td>
</tr>
<tr>
<td>S0208</td>
<td>Skill in determining the physical location of network devices.</td>
</tr>
<tr>
<td>S0209</td>
<td>Skill in developing and executing comprehensive cyber operations assessment programs for assessing and validating operational performance characteristics.</td>
</tr>
<tr>
<td>S0210</td>
<td>Skill in developing intelligence reports.</td>
</tr>
<tr>
<td>S0211</td>
<td>Skill in developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.</td>
</tr>
<tr>
<td>S0212</td>
<td>Skill in disseminating items of highest intelligence value in a timely manner.</td>
</tr>
<tr>
<td>S0213</td>
<td>Skill in documenting and communicating complex technical and programmatic information.</td>
</tr>
<tr>
<td>S0214</td>
<td>Skill in evaluating accesses for intelligence value.</td>
</tr>
<tr>
<td>S0215</td>
<td>Skill in evaluating and interpreting metadata.</td>
</tr>
<tr>
<td>S0216</td>
<td>Skill in evaluating available capabilities against desired effects to provide effective courses of action.</td>
</tr>
<tr>
<td>S0217</td>
<td>Skill in evaluating data sources for relevance, reliability, and objectivity.</td>
</tr>
<tr>
<td>S0218</td>
<td>Skill in evaluating information for reliability, validity, and relevance.</td>
</tr>
<tr>
<td>S0219</td>
<td>Skill in evaluating information to recognize relevance, priority, etc.</td>
</tr>
<tr>
<td>S0220</td>
<td>Skill in exploiting/querying organizational and/or partner collection databases.</td>
</tr>
<tr>
<td>S0221</td>
<td>Skill in extracting information from packet captures.</td>
</tr>
<tr>
<td>S0222</td>
<td>Skill in fusion analysis.</td>
</tr>
<tr>
<td>S0223</td>
<td>Skill in generating operation plans in support of mission and target requirements.</td>
</tr>
<tr>
<td>S0224</td>
<td>Skill in gisting target communications.</td>
</tr>
<tr>
<td>S0225</td>
<td>Skill in identifying a target's communications networks.</td>
</tr>
<tr>
<td>S0226</td>
<td>Skill in identifying a target's network characteristics.</td>
</tr>
<tr>
<td>S0227</td>
<td>Skill in identifying alternative analytical interpretations to minimize unanticipated outcomes.</td>
</tr>
<tr>
<td>S0228</td>
<td>Skill in identifying critical target elements, to include critical target elements for the cyber domain.</td>
</tr>
<tr>
<td>S0229</td>
<td>Skill in identifying cyber threats which may jeopardize organization and/or partner interests.</td>
</tr>
<tr>
<td>S0230</td>
<td>Skill in identifying how a target communicates.</td>
</tr>
<tr>
<td>S0231</td>
<td>Skill in identifying intelligence gaps and limitations.</td>
</tr>
<tr>
<td>S0232</td>
<td>Skill in identifying language issues that may have an impact on organization objectives.</td>
</tr>
<tr>
<td>S0234</td>
<td>Skill in identifying leads for target development.</td>
</tr>
<tr>
<td>Skill ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>S0235</td>
<td>Skill in identifying non-target regional languages and dialects</td>
</tr>
<tr>
<td>S0236</td>
<td>Skill in identifying the devices that work at each level of protocol models.</td>
</tr>
<tr>
<td>S0237</td>
<td>Skill in identifying, locating, and tracking targets via geospatial analysis techniques</td>
</tr>
<tr>
<td>S0238</td>
<td>Skill in information prioritization as it relates to operations.</td>
</tr>
<tr>
<td>S0239</td>
<td>Skill in interpreting compiled and interpretive programming languages.</td>
</tr>
<tr>
<td>S0240</td>
<td>Skill in interpreting metadata and content as applied by collection systems.</td>
</tr>
<tr>
<td>S0241</td>
<td>Skill in interpreting traceroute results, as they apply to network analysis and reconstruction.</td>
</tr>
<tr>
<td>S0242</td>
<td>Skill in interpreting vulnerability scanner results to identify vulnerabilities.</td>
</tr>
<tr>
<td>S0243</td>
<td>Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).</td>
</tr>
<tr>
<td>S0244</td>
<td>Skill in managing client relationships, including determining client needs/requirements, managing client expectations, and demonstrating commitment to delivering quality results.</td>
</tr>
<tr>
<td>S0245</td>
<td>Skill in navigating network visualization software.</td>
</tr>
<tr>
<td>S0246</td>
<td>Skill in number normalization.</td>
</tr>
<tr>
<td>S0247</td>
<td>Skill in performing data fusion from existing intelligence for enabling new and continued collection.</td>
</tr>
<tr>
<td>S0248</td>
<td>Skill in performing target system analysis.</td>
</tr>
<tr>
<td>S0249</td>
<td>Skill in preparing and presenting briefings.</td>
</tr>
<tr>
<td>S0250</td>
<td>Skill in preparing plans and related correspondence.</td>
</tr>
<tr>
<td>S0251</td>
<td>Skill in prioritizing target language material.</td>
</tr>
<tr>
<td>S0252</td>
<td>Skill in processing collected data for follow-on analysis.</td>
</tr>
<tr>
<td>S0253</td>
<td>Skill in providing analysis on target-related matters (e.g., language, cultural, communications).</td>
</tr>
<tr>
<td>S0254</td>
<td>Skill in providing analysis to aid writing phased after action reports.</td>
</tr>
<tr>
<td>S0255</td>
<td>Skill in providing real-time, actionable geolocation information utilizing target infrastructures.</td>
</tr>
<tr>
<td>S0256</td>
<td>Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.</td>
</tr>
<tr>
<td>S0257</td>
<td>Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data).</td>
</tr>
<tr>
<td>S0258</td>
<td>Skill in recognizing and interpreting malicious network activity in traffic.</td>
</tr>
<tr>
<td>S0259</td>
<td>Skill in recognizing denial and deception techniques of the target.</td>
</tr>
<tr>
<td>S0260</td>
<td>Skill in recognizing midpoint opportunities and essential information.</td>
</tr>
<tr>
<td>S0261</td>
<td>Skill in recognizing relevance of information.</td>
</tr>
<tr>
<td>S0262</td>
<td>Skill in recognizing significant changes in a target’s communication patterns.</td>
</tr>
<tr>
<td>S0263</td>
<td>Skill in recognizing technical information that may be used for leads for metadata analysis.</td>
</tr>
<tr>
<td>S0264</td>
<td>Skill in recognizing technical information that may be used for leads to enable remote operations (data includes users, passwords, email addresses, IP ranges of the target, frequency in DNI behavior, mail servers, domain servers, SMTP header information).</td>
</tr>
<tr>
<td>S0265</td>
<td>Skill in recognizing technical information that may be used for target development including intelligence development.</td>
</tr>
<tr>
<td>S0266</td>
<td>Skill in relevant programming languages (e.g., C++, Python, etc.).</td>
</tr>
<tr>
<td>S0267</td>
<td>Skill in remote command line and Graphic User Interface (GUI) tool usage.</td>
</tr>
<tr>
<td>S0268</td>
<td>Skill in researching essential information.</td>
</tr>
<tr>
<td>S0269</td>
<td>Skill in researching vulnerabilities and exploits utilized in traffic.</td>
</tr>
<tr>
<td>S0270</td>
<td>Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools.</td>
</tr>
<tr>
<td>S0271</td>
<td>Skill in reviewing and editing assessment products.</td>
</tr>
<tr>
<td>S0272</td>
<td>Skill in reviewing and editing intelligence products from various sources for cyber operations.</td>
</tr>
<tr>
<td>S0273</td>
<td>Skill in reviewing and editing plans.</td>
</tr>
<tr>
<td>Skill ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>S0274</td>
<td>Skill in reviewing and editing target materials.</td>
</tr>
<tr>
<td>S0275</td>
<td>Skill in server administration.</td>
</tr>
<tr>
<td>S0276</td>
<td>Skill in survey, collection, and analysis of wireless LAN metadata.</td>
</tr>
<tr>
<td>S0277</td>
<td>Skill in synthesizing, analyzing, and prioritizing meaning across data sets.</td>
</tr>
<tr>
<td>S0278</td>
<td>Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).</td>
</tr>
<tr>
<td>S0279</td>
<td>Skill in target development in direct support of collection operations.</td>
</tr>
<tr>
<td>S0280</td>
<td>Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementation of new technologies).</td>
</tr>
<tr>
<td>S0281</td>
<td>Skill in technical writing.</td>
</tr>
<tr>
<td>S0282</td>
<td>Skill in testing and evaluating tools for implementation.</td>
</tr>
<tr>
<td>S0283</td>
<td>Skill in transcribing target language communications.</td>
</tr>
<tr>
<td>S0284</td>
<td>Skill in translating target graphic and/or voice language materials.</td>
</tr>
<tr>
<td>S0285</td>
<td>Skill in using Boolean operators to construct simple and complex queries.</td>
</tr>
<tr>
<td>S0286</td>
<td>Skill in using databases to identify target-relevant information.</td>
</tr>
<tr>
<td>S0287</td>
<td>Skill in using geospatial data and applying geospatial resources.</td>
</tr>
<tr>
<td>S0288</td>
<td>Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).</td>
</tr>
<tr>
<td>S0289</td>
<td>Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.</td>
</tr>
<tr>
<td>S0290</td>
<td>Skill in using non-attributable networks.</td>
</tr>
<tr>
<td>S0291</td>
<td>Skill in using research methods including multiple, different sources to reconstruct a target network.</td>
</tr>
<tr>
<td>S0292</td>
<td>Skill in using targeting databases and software packages.</td>
</tr>
<tr>
<td>S0293</td>
<td>Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.</td>
</tr>
<tr>
<td>S0294</td>
<td>Skill in using trace route tools and interpreting the results as they apply to network analysis and reconstruction.</td>
</tr>
<tr>
<td>S0295</td>
<td>Skill in using various open source data collection tools (online trade, DNS, mail, etc.).</td>
</tr>
<tr>
<td>S0296</td>
<td>Skill in utilizing feedback to improve processes, products, and services.</td>
</tr>
<tr>
<td>S0297</td>
<td>Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).</td>
</tr>
<tr>
<td>S0298</td>
<td>Skill in verifying the integrity of all files. (e.g., checksums, Exclusive OR, secure hashes, check constraints, etc.).</td>
</tr>
<tr>
<td>S0299</td>
<td>Skill in wireless network target analysis, templating, and geolocation.</td>
</tr>
<tr>
<td>S0300</td>
<td>Skill in writing (and submitting) requirements to meet gaps in technical capabilities.</td>
</tr>
<tr>
<td>S0301</td>
<td>Skill in writing about facts and ideas in a clear, convincing, and organized manner.</td>
</tr>
<tr>
<td>S0302</td>
<td>Skill in writing effectiveness reports.</td>
</tr>
<tr>
<td>S0303</td>
<td>Skill in writing, reviewing and editing cyber-related intelligence/assessment products from multiple sources.</td>
</tr>
<tr>
<td>S0304</td>
<td>Skill to access information on current assets available, usage.</td>
</tr>
<tr>
<td>S0305</td>
<td>Skill to access the databases where plans/directives/guidance are maintained.</td>
</tr>
<tr>
<td>S0306</td>
<td>Skill to analyze strategic guidance for issues requiring clarification and/or additional guidance.</td>
</tr>
<tr>
<td>S0307</td>
<td>Skill to analyze target or threat sources of strength and morale.</td>
</tr>
<tr>
<td>S0308</td>
<td>Skill to anticipate intelligence capability employment requirements.</td>
</tr>
<tr>
<td>S0309</td>
<td>Skill to anticipate key target or threat activities which are likely to prompt a leadership decision.</td>
</tr>
<tr>
<td>S0310</td>
<td>Skill to apply analytical standards to evaluate intelligence products.</td>
</tr>
<tr>
<td>S0311</td>
<td>Skill to apply the capabilities, limitations and tasking methodologies of available platforms, sensors, architectures and apparatus as they apply to organization objectives.</td>
</tr>
<tr>
<td>S0312</td>
<td>Skill to apply the process used to assess the performance and impact of cyber operations.</td>
</tr>
<tr>
<td>S0313</td>
<td>Skill to articulate a needs statement/requirement and integrate new and emerging collection capabilities, accesses and/or processes into collection operations.</td>
</tr>
<tr>
<td>Skill ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>S0314</td>
<td>Skill to articulate intelligence capabilities available to support execution of the plan.</td>
</tr>
<tr>
<td>S0315</td>
<td>Skill to articulate the needs of joint planners to all-source analysts.</td>
</tr>
<tr>
<td>S0316</td>
<td>Skill to associate Intelligence gaps to priority information requirements and observables.</td>
</tr>
<tr>
<td>S0317</td>
<td>Skill to compare indicators/observables with requirements.</td>
</tr>
<tr>
<td>S0318</td>
<td>Skill to conceptualize the entirety of the intelligence process in the multiple domains and dimensions.</td>
</tr>
<tr>
<td>S0319</td>
<td>Skill to convert intelligence requirements into intelligence production tasks.</td>
</tr>
<tr>
<td>S0320</td>
<td>Skill to coordinate the development of tailored intelligence products.</td>
</tr>
<tr>
<td>S0321</td>
<td>Skill to correlate intelligence priorities to the allocation of intelligence resources/assets.</td>
</tr>
<tr>
<td>S0322</td>
<td>Skill to craft indicators of operational progress/success.</td>
</tr>
<tr>
<td>S0323</td>
<td>Skill to create and maintain up-to-date planning documents and tracking of services/production.</td>
</tr>
<tr>
<td>S0324</td>
<td>Skill to determine feasibility of collection.</td>
</tr>
<tr>
<td>S0325</td>
<td>Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information needed.</td>
</tr>
<tr>
<td>S0326</td>
<td>Skill to distinguish between notional and actual resources and their applicability to the plan under development.</td>
</tr>
<tr>
<td>S0327</td>
<td>Skill to ensure that the collection strategy leverages all available resources.</td>
</tr>
<tr>
<td>S0328</td>
<td>Skill to evaluate factors of the operational environment to objectives, and information requirements.</td>
</tr>
<tr>
<td>S0329</td>
<td>Skill to evaluate requests for information to determine if response information exists.</td>
</tr>
<tr>
<td>S0330</td>
<td>Skill to evaluate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.</td>
</tr>
<tr>
<td>S0331</td>
<td>Skill to express orally and in writing the relationship between intelligence capability limitations and decision-making risk and impacts on the overall operation.</td>
</tr>
<tr>
<td>S0332</td>
<td>Skill to extract information from available tools and applications associated with collection requirements and collection operations management.</td>
</tr>
<tr>
<td>S0333</td>
<td>Skill to graphically depict decision support materials containing intelligence and partner capability estimates.</td>
</tr>
<tr>
<td>S0334</td>
<td>Skill to identify and apply tasking, collection, processing, exploitation and dissemination to associated collection disciplines.</td>
</tr>
<tr>
<td>S0335</td>
<td>Skill to identify Intelligence gaps.</td>
</tr>
<tr>
<td>S0336</td>
<td>Skill to identify when priority information requirements are satisfied.</td>
</tr>
<tr>
<td>S0337</td>
<td>Skill to implement established procedures for evaluating collection management and operations activities.</td>
</tr>
<tr>
<td>S0338</td>
<td>Skill to interpret planning guidance to discern level of analytical support required.</td>
</tr>
<tr>
<td>S0339</td>
<td>Skill to interpret readiness reporting, its operational relevance and intelligence collection impact.</td>
</tr>
<tr>
<td>S0340</td>
<td>Skill to monitor target or threat situation and environmental factors.</td>
</tr>
<tr>
<td>S0341</td>
<td>Skill to monitor threat effects to partner capabilities and maintain a running estimate.</td>
</tr>
<tr>
<td>S0342</td>
<td>Skill to optimize collection system performance through repeated adjustment, testing, and re-adjustment.</td>
</tr>
<tr>
<td>S0343</td>
<td>Skill to orchestrate intelligence planning teams, coordinate collection and production support, and monitor status.</td>
</tr>
<tr>
<td>S0344</td>
<td>Skill to prepare and deliver reports, presentations and briefings, to include using visual aids or presentation technology.</td>
</tr>
<tr>
<td>S0345</td>
<td>Skill to relate intelligence resources/assets to anticipated intelligence requirements.</td>
</tr>
<tr>
<td>S0346</td>
<td>Skill to resolve conflicting collection requirements.</td>
</tr>
<tr>
<td>S0347</td>
<td>Skill to review performance specifications and historical information about collection assets.</td>
</tr>
<tr>
<td>S0348</td>
<td>Skill to specify collections and/or taskings that must be conducted in the near term.</td>
</tr>
<tr>
<td>S0349</td>
<td>Skill to synchronize operational assessment procedures with the critical information requirement process.</td>
</tr>
<tr>
<td>S0350</td>
<td>Skill to synchronize planning activities and required intelligence support.</td>
</tr>
<tr>
<td>S0351</td>
<td>Skill to translate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.</td>
</tr>
<tr>
<td>S0352</td>
<td>Skill to use collaborative tools and environments for collection operations.</td>
</tr>
<tr>
<td>S0353</td>
<td>Skill to use systems and/or tools to track collection requirements and determine if they are satisfied.</td>
</tr>
<tr>
<td>Skill ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>S0354</td>
<td>Skill in creating policies that reflect the business’s core privacy objectives.</td>
</tr>
<tr>
<td>S0355</td>
<td>Skill in negotiating vendor agreements and evaluating vendor privacy practices.</td>
</tr>
<tr>
<td>S0356</td>
<td>Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).</td>
</tr>
<tr>
<td>S0357</td>
<td>Skill to anticipate new security threats.</td>
</tr>
<tr>
<td>S0358</td>
<td>Skill to remain aware of evolving technical infrastructures.</td>
</tr>
<tr>
<td>S0359</td>
<td>Skill to use critical thinking to analyze organizational patterns and relationships.</td>
</tr>
<tr>
<td>S0360</td>
<td>Skill to analyze and assess internal and external partner cyber operations capabilities and tools.</td>
</tr>
<tr>
<td>S0361</td>
<td>Skill to analyze and assess internal and external partner intelligence processes and the development of information requirements and essential information.</td>
</tr>
<tr>
<td>S0362</td>
<td>Skill to analyze and assess internal and external partner organization capabilities and limitations (those with tasking, collection, processing, exploitation and dissemination responsibilities).</td>
</tr>
<tr>
<td>S0363</td>
<td>Skill to analyze and assess internal and external partner reporting.</td>
</tr>
<tr>
<td>S0364</td>
<td>Skill to develop insights about the context of an organization’s threat environment.</td>
</tr>
<tr>
<td>S0365</td>
<td>Skill to design incident response for cloud service models.</td>
</tr>
<tr>
<td>S0367</td>
<td>Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).</td>
</tr>
<tr>
<td>S0369</td>
<td>Skill to identify sources, characteristics, and uses of the organization’s data assets.</td>
</tr>
<tr>
<td>S0370</td>
<td>Skill to use cyber defense Service Provider reporting structure and processes within one’s own organization.</td>
</tr>
<tr>
<td>S0372</td>
<td>Skill to translate, track, and prioritize information needs and intelligence collection requirements across the extended enterprise.</td>
</tr>
<tr>
<td>S0374</td>
<td>Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations.</td>
</tr>
</tbody>
</table>