INFOSEC Skills

Outmaneuver adversaries with hands-on training aligned to MITRE ATT&CK® Framework

Learn how to ATT&CK & defend in the Infosec Skills cyber range

Infosec Skills cyber ranges guide learners through realistic scenarios inside the operating environments they'd encounter on the job. Launch a cyber range with one click and learn how to counter the MITRE ATT&CK® Framework tactics and techniques targeting your organization today. From command line basics to advanced adversarial techniques, Infosec Skills cyber ranges teach your team how to:

- Run red and blue team exercises
- Write secure code by example
- Pass dozens technical certifications by gaining hands-on domain knowledge
- Attack and defend cloud-based applications
- And much more

Practical training fueled by OSINT

The MITRE ATT&CK Framework collects publicly available threat intelligence and distills it into an easy-to-understand taxonomy. It categorizes commonly used adversarial tactics, techniques and procedures across the entire lifecycle of a cyber attack.

While ATT&CK tactics explain motivations for and stages of attacks, techniques detail the "how" and offer important insights on how to mitigate advanced persistent threats. Infosec Skills cyber ranges offer dozens of hands-on labs mapped directly to the ATT&CK Framework to help you assess your team's readiness against real cyber threats targeting your organization today.

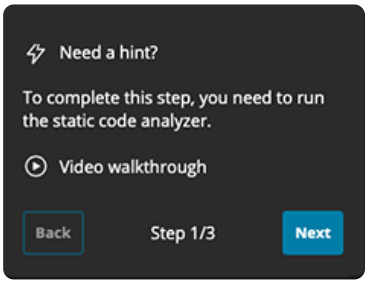
Whether your go-to resource is the Diamond Model or the Lockheed Martin Cyber Kill Chain®, Infosec Skills ATT&CK-based labs complement other models with deeper insights into adversarial maneuvers across all 14 ATT&CK Tactics.

Infosec Skills includes over 250 labs mapped to MITRE ATT&CK Framework. Tactic and technique coverage includes:

ATT&CK Tactics	Sample related Infosec Skills labs	ATT&CK Techniques coverage
Reconnaissance	Local File Inclusion Lab Reconnaissance & Resource Development	T1590 - Gather Victim Network Information T1598 - Phishing for Information
Resource development	Reconnaissance & Resource Development	T1585 - Establish Accounts
Initial access	Sandworm APT Lab	T1195 - Supply Chain Compromise T1078 - Valid Accounts
Execution	Persistance Techniques	T1106 - Native API
Persistence	Persistance Techniques	T1176 - Browser Extensions T1554 - Compromise Client Software Binary
Privilege escalation	Privilege Escalation Techniques	T1548 - Abuse Elevation Control Mechanism T1574 - Hijack execution flow
Defense evasion	Sandworm APT Lab Local File Inclusion Lab More Persistence Techniques	T1070 - Indicator Removal T1036 - Masquerading T1205 - Traffic Signaling
Credential access	Sandworm APT	T1056.001 - Keylogging
Discovery	Working with Processes User Accounts and Privileges	T1057 - Process Discovery T1069 - Permission Groups Discovery
Lateral movement	Persistence Methods	T1091 - Replication Through Removable Media
Collection	Git Secrets Sandworm APT	T1213 - Data from Information Repositories T1056.001 - Keylogging
Command and control	Persistence Techniques Sandworm APT	T1205 - Traffic Signaling T1105 - Ingress Tool Transfer
Exfiltration	Sandworm APT	T1041 - Exfiltration over C2 Channel
Impact	Sandworm APT	T1485 - Data Destruction

Demystify cyber work with clear learning objectives

Infosec Skills cyber ranges meet learners where they are with clear learning objectives and detailed instructions at every step of the lab experience. This goes beyond gamified learning to combine the benefits of experiential learning with actionable, practical guidance and professional development. Advanced learners can dive in and assess their cyber skills with little to no instruction, while beginners can opt for a more guided experience with step-by-step instructions, hints and video explanations.



Relevant to any operating environment or cyber role

Designed with enterprise networks in mind, cyber adversary behaviors detailed within the ATT&CK Framework apply to many of the environments you operate in every day:

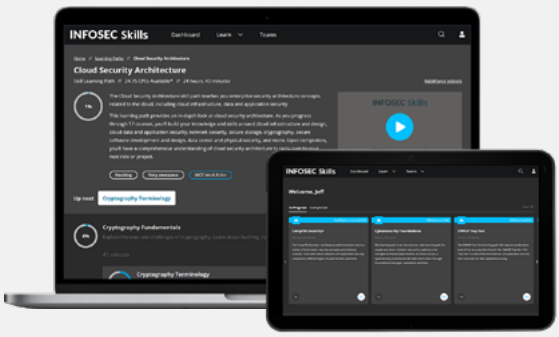
- Windows and Linux systems
- Cloud systems covering Amazon Web Services, Microsoft Azure and Google Cloud Platform
- Software-as-a-Service
- Office 365 and Azure Active Directory

The MITRE ATT&CK Framework is used by red teams, blue teams and cyber threat hunters to anticipate threats and assess cyber risk. Make your team's training even more relevant and effective by combining ATT&CK-based hands-on labs with over 1,200 courses mapped to the NICE Framework Work Roles that best fit your team structure like:

- Cyber Defense Analyst
- Cyber Defense Incident Responder
- Threat / Warning Analyst
- Vulnerability Assessment Analyst
- Exploitation Analyst

Download course catalog

Meet Infosec Skills



Upskill and certify your security, IT and engineering teams with the hands-on cybersecurity training platform that scales to your organization's needs. Assess teams and close skills gaps with hands-on cyber ranges, projects and courses mapped to the NICE Workforce Framework for Cybersecurity and MITRE ATT&CK Framework — or upgrade to a live boot camp for instructor-led training to certify your team, guaranteed.

Infosec Skills includes 1,400+ hands-on courses, cyber ranges and labs to:

- Prepare teams for MITRE ATT&CK tactics and techniques with hands-on labs in cloud-hosted cyber ranges
- Guide team development with 190+ learning paths mapped to the NICE Framework
- Assess knowledge and skills to pinpoint gaps and training needs
- Gauge exam readiness with customizable certification practice exams
- Fast-track certification with 100+ live, instructor-led boot camps

Learn more