INFOSEC Boot Camps

CAREER IMMERSIVE

Future-proof your career.

Cybersecurity Foundations Immersive Boot Camp

Future-proof your career and gain valuable skills in as little as 26 weeks with the Infosec Cybersecurity Foundations Immersive Boot Camp.

OVERVIEW

This program is an intensive course that covers a wide range of critical topics about information security and its role in today's technology. The program is designed to provide students with a deep understanding of information security, and they will learn to identify and protect vulnerable systems through hands-on research and guidance from instructors.

The curriculum focuses on foundational Windows troubleshooting, where students will navigate complex scenario-based labs to develop critical skills such as effective communication, documentation, terminal operations, performance monitoring and software application management. They will also learn to resolve and document tech issues and incidents using the CompTIA troubleshooting methodology alongside the ITIL service management framework.

Students will get the opportunity to experience real-world scenarios by becoming the systems administrator for the fictional GlobeX Corporation. They will learn about network design, troubleshooting, VPN tunneling, firewall configuration and server deployment, alongside user identity management, scripting, automation and system health monitoring.

The program concludes with a deep dive into cybersecurity operations (SecOps Foundations), where students will explore cyber frameworks, data encryption, cloud security, network security, threat modeling and incident response. They will also acquire ethical hacker skills in penetration testing, culminating in two major projects to showcase their newfound skills.

What's included?

- ✓ 26-week immersive program (up to 640 hours of total immersion!)
- ✓ 240 hours of live instruction
- ✓ Interactive hands-on labs
- ✓ Career Coaching
- ✓ Security+ exam voucher
- ✓ 6 weeks post-program Skills Validation Badge activities
- ✓ Knowledge Retention Assurance

Prerequisites

This program has been designed for beginners, whether you are at the beginning of your career or switching into the cybersecurity industry. We do recommend that you have a general understanding of Windows client operating system as well as experience with Microsoft products and technologies.

What you'll learn

- Windows troubleshooting
- CompTIA troubleshooting methodology
- ITIL service management
- Network Design
- Troubleshooting
- VPN tunneling
- Firewall Configuration
- Server Deployment
- Cyber Frameworks
- Data Encryption
- Cloud Security
- Network Security
- Threat Modeling
- Incident Response

Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

Course agenda

Weeks 1–2 (estimated) Self-paced pre-work	Cybersecurity Foundations 101: Modern Computing Technologies and Operating Systems Cybersecurity Foundations 102: Introduction to Cybersecurity	Learn about modern computer technologies and different operating systems then explore the field of cybersecurity and its core concepts and many career pathways.
Weeks 3–8 Cohort begins	Cybersecurity Foundations 201: Foundations of Computer Operations	Learn strategies and skills to help you identify and troubleshoot common system issues or challenges.
Weeks 9–14	Cybersecurity Foundations 301: Networking & System Administration	Learn how to build, configure, secure, and manage modern networks and systems.
Weeks 15–20	Cybersecurity Foundations 401a: Cybersecurity Governance & Operations	Learn how to manage security operation efforts to support effective security governance, risk management, and compliance.
Weeks 21–26	Cybersecurity Foundations 401b: Threat Management and Penetration Testing	Learn about the various tools, tactics, and methods cyber attackers use and how these can be leveraged to bolster and guide organizational security efforts.
Weeks 27-32 (Optional)	Cybersecurity Foundations 501: AI in Cybersecurity	Culminate your learning experience with a capstone project that challenges you to design and implement a generative AI solution to a pressing cybersecurity problem.

Topics included

Cybersecurity Foundations 101: Modern Computing Technologies and Operating Systems

- Common Computer Hardware
- Operating Systems (Windows, Linux, Mac)
- Intro to Command Line and Terminal
- Basic Computing Concepts and Functions

Cybersecurity Foundations 102: Introduction to Cybersecurity

- Intro to Cybersecurity Careers
- Cybersecurity Principles and Core Concepts
- Intro to Basic Networking & Cloud Technologies
- Common Security Frameworks and Polices
- Command Line and Terminal

Cybersecurity Foundations 201: Foundations of Computer Operations

- Linux Diagnostics and IT Service Delivery
- Windows Diagnostics
- Software, Networking, Virtualization & Cloud Computing

Cybersecurity Foundations 301: Networking & System Administration

- Server Administration and Management
- Network Infrastructure and Design
- Network Security

Cybersecurity Foundations 401a: Cybersecurity Governance & Operations

- Governance, Risk, and Compliance (GRC)
- Data Security
- Security Operations 1
- Cloud Security

Cybersecurity Foundations 401b: Threat Management and Penetration Testing

- Threat Modeling and Analysis
- Threat Hunting
- Web Application Security
- Penetration Testing

(Optional) Cybersecurity Foundations 501: AI in Cybersecurity

- Leverage AI technologies
- Integrate generative AI modules

Career Coaching Services

Students will have access to our Career Coaching services and a digital career services platform for 30 days, which will provide you with further assistance to kickstart your career in cybersecurity.

Knowledge Retention Assurance

Students will continue to have access to Infosec Skills for six months. 1,400+ hands-on cybersecurity courses and cyber ranges to keep their skills sharp while starting their cybersecurity career.

Verified Skills Validation Badge

Students will have the opportunity to take one of our Skills Validation Badges. Each badge offers a two-week intensive, hands-on simulation where students must perform real-world tasks.

After your boot camp

After this Immersive Boot Camp, students will have access to career coaches. These experts will help create a stand-out resume and prep for interviews. While they search for jobs, they can keep their skills fresh with extended access the 1,400+ cyber ranges and courses available on Infosec Skills.

In addition, students are strongly encouraged to gain Skills Validation Badges after the initial course. There are three badges, each gained after a two-week intensive. Those that complete these assessments will receive an Infosec badge and a transcript to prove their mastery of the skill.

Skill Assessment 1: Penetration Testing 2 Weeks	Optional Assessment Activities for the Infosec Verified in Penetration Testing Badge	Demonstrate your skills and knowledge in the area of penetration testing and ethical hacking.
Skill Assessment 2: Threat Hunting 2 Weeks	Optional Assessment Activities for the Infosec Verified in Threat Hunting Badge	Demonstrate your skills and knowledge in the area of cyber threat hunting
Skill Assessment 3: Incident Response 2 Weeks	Optional Assessment Activities for the Infosec Verified in Incident Response Badge	Demonstrate your skills and knowledge in the area of Incident Response.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

©2024 Infosec, Inc. All rights reserved.

INFOSEC