



Cybersecurity “Bootcamp” for IT Professionals in Addis Ababa

The objective of this program is to enable IT professionals to transition into cybersecurity roles by developing practical, job-ready skills in cyber defense, network and application security, incident handling, forensics, ethical hacking, and risk management. The bootcamp delivers hands-on, scenario-based training aligned with real-world cybersecurity operations.

280 HOURS | <DATE> | FULLY ONLINE

- The program is designed for IT professionals seeking a fast and structured transition into cybersecurity careers.
- Focused on practical cybersecurity skills required for analyst-level roles.
- Hands-on learning through labs, tools, and real-world attack scenarios.
- Covers defensive and offensive security, incident response, and risk management.
- Delivered using an accelerated learning methodology inspired by military-style bootcamps.
- Ideal for professionals targeting entry- to mid-level cybersecurity positions.

TARGET AUDIENCE

- IT Support and Helpdesk Professionals
- Network and System Administrators
- SOC and Security Operations Aspirants
- Infrastructure and Operations Engineers
- IT Professionals transitioning into Cybersecurity
- Organizations upskilling existing IT teams

THE INSTRUCTOR

Delivered by highly experienced instructors with over 10 years of expertise in cybersecurity, ICT systems, and information security. Our instructors combine hands-on operational experience with a proven track record in delivering professional training.

Training is designed to emphasize practical, scenario-based learning and hands-on labs to ensure that participants gain real-world skills applicable to their work environments.

ABOUT ECS ETHIOPIA

ECS Ethiopia is a technology-driven company working with government bodies, municipalities, and large corporations to bring advanced global solutions to Ethiopia. As part of the ECS Group (UK), we help finance and execute major projects while fostering strong partnerships and innovation across the country.

GLOBAL TRAINING PARTNERSHIPS

Our training programs and learning platform were developed in close collaboration with leading international training organisations. Thousands of professionals worldwide have successfully completed these programs using this training content and learning system.



MODULE 01 NETWORK ADMINISTRATION

Prior to the start of the Bootcamp, learners are required to complete the online self-paced Pework module Network Administration, whose objective is to refresh topics for bootcampers as well as provide an opportunity to familiarize themselves with the platform. The module focuses on designing, configuring, and troubleshooting networks. The Pework can take anywhere from 10–40 hours depending on the learner's technical background.

Topics Covered:

- Network Configuration – LAN, WAN
- Segmentations, VLANs and Subnetting
- Network Mapping Tools
- Troubleshooting and Monitoring Networks
- Network Devices – Switches, Routers
- Telecommunication
- System Administration

Tools: Cisco Packet Tracer, Nmap, Windows PowerShell

MODULE 02 CYBERSECURITY FUNDAMENTALS

This module is designed to teach how organizations implement cybersecurity and introduce the different roles in the industry. Additionally, bootcampers will get to know the history of famous hackers from the 1950s until today. The module then explores modern hackers and their motives, capabilities, and techniques, as well as the different types of malware they use to attack their victims.

Topics Covered:

- NIST Framework
- Malware Types
- Social Engineering
- Vulnerabilities, Risks, and Exploits
- Famous Cyber-Attacks

MODULE 03 NETWORK AND APPLICATION SECURITY

In this module, bootcampers learn about network and application security defense methodologies. They will be able to identify which tools are required based on the network and the needs of the organization. It also covers construction of secure network architectures. For each method, bootcampers learn how to detect and eventually block malicious actors from carrying out cyber-attacks and crimes.

Topics Covered:

- Cryptography – Symmetric vs Asymmetric Keys
- Encryption/Decryption, Hash Functions
- Security Architecture
- Security Tools – Firewalls, Antivirus, IDS/IPS, SIEM
- Access Control Methods, Multi-factor Authentication, Authentication Protocols
- Honeypots and Cyber Traps

Tools: Kali Linux, Splunk, Snort IDS, Active Directory, Nmap, OpenVPN, Windows Firewall, Linux iptables

MODULE 04 INCIDENT HANDLING

In this module, bootcampers learn about the most common types of cybersecurity attacks. They will practice detection and analysis of incidents as a Cybersecurity Analyst would in real life. They will also analyze different attack vectors and their attributes and identify false-positive cases.

Topics Covered:

- Detection and Analysis of Cyber-Attacks – DDoS/DoS, Brute-Force
- OWASP Top 10 Attacks – SQL Injection, Cross-Site Scripting
- Group and Individual Incident Report Writing

Tools: Splunk

MODULE 05 FORENSICS

In this module, bootcampers learn digital forensic processes for analyzing threats in digital devices. This includes identification, recovery, investigation, and validation of digital evidence in computers and other media devices.

Topics Covered:

- Computer Memory Forensics, Memory Dump Analysis
- FTK Imager, Autopsy, Redline and RAM Capturing
- Digital Evidence Acquisition Methodologies
- Registry Forensics
- Windows Timeline Analysis and Data Recovery
- Network Forensics, Anti-Forensics and Steganography

Tools: Volatility Framework, FTK Imager, Autopsy, NetworkMiner, Wireshark, OpenStego, ShellBags Explorer, winmd5free, Magnet RAM Capture, Redline, HxD

MODULE 06 ETHICAL HACKING AND INCIDENT RESPONSE

As future Cybersecurity Analysts, it is essential for bootcampers to understand offensive methodologies in cyber warfare. In Ethical Hacking, they will learn how to perform cyber-attacks, which will provide them with insights on cyber defense best practices, vulnerability assessments, forensics, and incident response processes. In Incident Response, bootcampers will learn the relevant response methodologies used once an attack has occurred.

Topics Covered:

- Ethical Hacking Processes and Methodologies
- Network Hacking, Reconnaissance, Google Hacking and Locating Attack Vectors
- Exploitation Techniques
- Web Application Hacking, OWASP Top 10 – XSS, SQL Injection, Manual and Automated Attacks
- Post Incident Activity

Tools: Metasploit, SQLMap, Nmap



MODULE 07

RISK MANAGEMENT

In this module, bootcampers will learn about risk management and dive into the cybersecurity aspects involved. They will learn methodologies and processes to analyze, prioritize, and manage risks effectively.

Topics Covered:

- Risk Management Processes
- Analyzing, Prioritizing, Evaluating and Monitoring Severity of Internal and External Risks
- Risk Management Policies, Procedures, Standards, and Guidelines
- Security Models

MODULE 08

FINAL SCENARIOS

The final module includes real-life scenarios of cybersecurity incidents and a cumulative final exam covering all the content learned throughout the Bootcamp. This ensures bootcampers have gained the technical knowledge and practical skills required to begin their cybersecurity career.