Cybersecurity Impact "Bootcamp" in Addis Ababa

The objective of this program is to equip beginners and career changers with practical cybersecurity skills required to transition into entry-level cybersecurity roles. The bootcamp provides hands-on training in cybersecurity fundamentals, network and application security, incident handling, ethical hacking, forensics, risk management, and threat intelligence through real-world scenarios and guided practice.

24 WEEKS | <DATE> | FULLY ONLINE

- The program focuses on building strong cybersecurity foundations aligned with real-world industry requirements.
- Designed to take learners from beginner level to job-ready cybersecurity professionals within an accelerated timeframe.
- Hands-on learning through real-world scenarios, labs, and simulated cyberattack environments.
- Covers cybersecurity operations, network and application security, incident response, ethical hacking, and forensics.
- Aligned with the NICE / NIST Cybersecurity Workforce Framework and CertNexus CFR learning objectives.
- Delivered through flexible, self-paced online learning with instructor guidance and career-focused support.
- Ideal for individuals seeking to start a cybersecurity career or organizations developing cybersecurity talent.

TARGET AUDIENCE

- Beginners with no prior cybersecurity background
- Career changers entering the cybersecurity field
- IT professionals transitioning into security roles
- SOC analyst entry-level aspirants
- Cybersecurity operations and incident response beginners
- Students and graduates seeking hands-on cybersecurity training
- Anyone preparing for an entry-level cybersecurity career

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.

ECS Ethiopia

MODULE 01
INTRO TO CYBER
In just 30 hours, learn the cybersecurity basics, from malware and the OWASP Top 10 to risk management and career paths. Understand attackers and tools like SIEM & firewalls, and learn about the potential career paths in this booming field.

Topics Covered
- The Cybersecurity World and Crime
- Attackers and APTS
- Mitigating Risk and Taking Control

MODULE 02
BOOTCAMP INTRODUCTION
The Bootcamp Introduction will give you the tools you need to make the program an efficient and fulfilling learning experience. During this course, you will learn how the program is structured alongside the basics of computers.

Topics Covered
- Overview of the Bootcamp and Cybersecurity Industry
- Cybersecurity Career Paths

MODULE 03
NETWORK ADMINISTRATION
This course focuses on designing, configuring, and troubleshooting networks so you can acquire the necessary skills for running and monitoring a network with confidence.

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

Tools: Cisco Packet Tracer, Nmap, Windows PowerShell

MODULE 04
CYBERSECURITY FUNDAMENTALS
The next stage of the bootcamp defines cybersecurity and how organizations utilize it. This is when you will acquire knowledge about vulnerabilities, exploits, and threats, then dive into different types of attackers, their motivations, capabilities, strategies, and the kinds of malware used to target their victims.

Topics Covered
- Most Common Vulnerabilities, Risks, and Threats
- The Main Concepts in Cybersecurity
- Types of Malware and Attackers
- NIST & International Cybersecurity Framework
- Most Common Cyberattacks
- Famous Cyber Incidents

MODULE 05
NETWORK AND APPLICATION SECURITY
Here you will learn about network and application security defense methodologies and construction of secure network architectures. When this course is over, you will understand how to detect and eventually block malicious actors from carrying out cyberattacks and crimes.

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

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

MODULE 06
INCIDENT HANDLING
In this course, you will dive into the world of cyberattacks and learn how they work, their impact, and how to detect them. Next, you will practice detection and analysis of incidents in security applications, then roleplay as a real-world cybersecurity analyst.

Topics Covered
- Types of Attacks in the Web, Domain, & Malware Areas
- Practicing the Role of the SOC Analyst
- Analyzing Malicious Indicators
- Group and Individual Incident Report Writing

Tools: Splunk, In-House SIEM, Wazuh, VirusTotal, PowerShell, Wireshark

MODULE 07
FORENSICS
Access digital forensic processes for analyzing threats in digital devices, including identification, recovery, investigation, and validation of digital evidence.

Topics Covered
- Computer Memory Forensics and Memory Dump Analysis
- Digital Evidence Acquisition Methodologies
- Registry Forensics and Timeline Analysis
- Network Forensics, Anti-Forensics, and Steganography

Tools: Volatility Framework, FTK Imager, Autopsy, NetworkMiner, Wireshark, OpenStego, Magnet RAM Capture, Redline

MODULE 08
MALWARE ANALYSIS
This course will teach you how to use multiple malware analysis methods, such as reverse engineering, binary analysis, and obfuscation detection to analyze real-world malware samples.

Topics Covered
- Dynamic Malware Analysis and Reverse Engineering
- Fileless Malware Analysis
- Containment, Eradication, and Recovery
- Analysis Using Sysinternals

Tools: Procmon, Autoruns, TCPView, ExeInfo PE, ProcDOT, HashCalc, FileAlyzer, PDFStreamDumper, HxD, Wireshark, UPX

MODULE 09
ETHICAL HACKING AND INCIDENT RESPONSE
Here you will dive into the world of hacking by performing cyberattacks and practicing relevant response methodologies.

Topics Covered
- Ethical Hacking and Penetration Testing Frameworks
- Network Hacking and Web Application Hacking (OWASP Top 10)
- Post-Incident Activities
- Capture the Flag (CTF) Challenge

Tools: Metasploit, SQLMap, Nmap

MODULE 10
SECURE DESIGN PRINCIPLES
This course helps you understand trend analysis and cybersecurity design best practices.

Topics Covered
- Trend Analysis
- Artificial Intelligence in Cybersecurity
- Zero-Trust Policy
- Best Detection Methodologies
- Incident Impact Mitigation

MODULE 11
RISK MANAGEMENT
Study risk management and related methodologies to effectively manage cybersecurity risks.

Topics Covered
- Risk Management Processes
- Risk Analysis and Prioritization
- Policies, Procedures, Standards, and Guidelines
- Security Models

Module 12
Threat Intelligence
Discover methods, techniques, and tools used to gather intelligence about cyber threats.

Topics Covered
- Threat Intelligence Cycle
- Dark Web and Dark Market Investigation
- Online Anonymity Techniques
- Trend and Data Analysis

Tools: ThriveDX Security Awareness Training

Module 13
Final Scenarios and Assessment
This is where it all comes together through real-life cybersecurity scenarios and a cumulative final exam.

Topics Covered
- Practical Incident Scenarios
- Attack Detection and Analysis
- Incident Reporting
- Final Examination and Interview Preparation