

CompTIA Security+ 'Bootcamp' in Addis Ababa

The objective of this course is to equip participants with essential cybersecurity knowledge required to secure systems, networks, and organizational assets against evolving threats. The training offers hands-on experience in risk management, network defense, identity access management, cryptography, incident response, and compliance practices aligned with the CompTIA Security+ (SY0-701) global certification track.

5 FULL DAYS | <DATE - TBD> | TRAINING FACILITIES AT <LOCATION>

- The course follows the official CompTIA Security+ (SY0-701) objectives.
- Focus on real-world cyber threats, vulnerabilities, attack vectors, and mitigation strategies.
- Hands-on lab experience for network security, access controls, encryption, monitoring & incident handling.
- Covers both cloud and on-premises security models including modern security tools & frameworks.
- Participants learn to identify risks, configure defenses, and maintain security posture effectively.
- Ideal for beginners entering cybersecurity or those progressing toward global Security+ certification.
- **Course prerequisites:** Basic understanding of computer networks and operating systems; familiarity with IT terminology; recommended prior experience in IT support or networking.

TARGET AUDIENCE

- Junior / Entry-level Cybersecurity Professionals
- IT Support & Network Administrators
- SOC / Blue Team Beginners
- System Engineers & Helpdesk Technicians
- Students transitioning into Cybersecurity
- Anyone preparing for CompTIA Security+ (SY0-701) Certification

THE INSTRUCTOR

Delivered by senior instructors with 10+ years of experience in cybersecurity and ICT systems, with strong hands-on and professional training expertise. Practical, scenario-based learning and hands-on labs are emphasized.

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

INTRODUCTION TO CYBERSECURITY CONCEPTS

Understand the fundamentals of information security, including confidentiality, integrity, and availability (CIA triad). Learn about security principles, best practices, and the evolving cyber threat landscape.

MODULE 02

THREATS, ATTACKS, AND VULNERABILITIES

Study various attack vectors such as malware, phishing, social engineering, insider threats, and advanced persistent threats (APTs). Learn vulnerability scanning, patch management, and mitigation techniques.

MODULE 03

RISK MANAGEMENT AND GOVERNANCE

Explore enterprise risk management frameworks, threat modeling, and business impact analysis. Learn to apply security policies, standards, and procedures aligned with regulatory requirements.

MODULE 04

NETWORK SECURITY FUNDAMENTALS

Learn about network design and defense strategies. Study firewalls, routers, switches, VPNs, VLANs, and intrusion detection/prevention systems. Understand segmentation, zero trust principles, and secure protocols.

MODULE 05

SECURE SYSTEM AND APPLICATION DESIGN

Understand secure configuration of operating systems, applications, and services. Learn software development lifecycle (SDLC) concepts, secure coding principles, and patch management.

MODULE 06

IDENTITY AND ACCESS MANAGEMENT (IAM)

Explore authentication, authorization, and accounting (AAA) principles. Learn about SSO, MFA, access control models (RBAC, ABAC, MAC), and directory services such as Active Directory and LDAP.

MODULE 07

CRYPTOGRAPHY AND PKI

Study encryption algorithms, digital certificates, hashing, and digital signatures. Learn about Public Key Infrastructure (PKI) and its role in securing communication and verifying authenticity.

MODULE 08

SECURITY OPERATIONS AND MONITORING

Examine SOC operations, event monitoring, and log analysis. Learn about SIEM, endpoint detection and response (EDR), and threat intelligence. Understand how to identify and prioritize security alerts.

MODULE 09

INCIDENT RESPONSE AND FORENSICS

Learn incident response phases: preparation, detection, containment, eradication, and recovery. Study forensic procedures, evidence handling, and post-incident review for organizational improvement.

MODULE 10

CLOUD AND VIRTUALIZATION SECURITY

Understand security challenges in cloud computing. Study cloud service models (IaaS, PaaS, SaaS), shared responsibility models, and virtualization risks. Learn about secure container deployment and resource isolation.

MODULE 11

MOBILE AND IOT SECURITY

Explore mobile device management (MDM), application control, and endpoint protection strategies. Understand IoT device vulnerabilities, firmware attacks, and methods to secure embedded systems.

MODULE 12

PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS

Study physical access controls, surveillance systems, hardware locks, and secure facility design. Learn about environmental risks, power management, and protection against physical tampering.

MODULE 13

SECURITY AWARENESS AND HUMAN FACTORS

Understand the human element of cybersecurity. Learn about user awareness training, insider threats, social engineering prevention, and promoting a security-aware organizational culture.

MODULE 14

BUSINESS CONTINUITY AND DISASTER RECOVERY

Learn to plan and maintain business continuity. Study backup strategies, redundancy, failover, and disaster recovery plans. Understand metrics such as RTO and RPO.

MODULE 15

LEGAL, ETHICS, AND COMPLIANCE

Understand global compliance frameworks (GDPR, HIPAA, PCI-DSS, ISO 27001). Learn about privacy principles, data governance, and legal considerations in incident handling and digital forensics.

MODULE 16

SECURITY POLICIES AND PROCEDURES

Study the role of administrative controls in maintaining organizational security. Learn about acceptable use policies, change management, auditing, and continuous improvement cycles.

MODULE 17

EMERGING TECHNOLOGIES AND TRENDS

Explore security implications of AI, machine learning, quantum computing, and blockchain. Understand new attack surfaces and evolving defensive technologies shaping modern cybersecurity.

MODULE 18

SECURITY ASSESSMENTS AND TESTING

Learn vulnerability assessment, penetration testing fundamentals, and security validation methods. Understand scanning, remediation verification, and communicating test results effectively.

MODULE 19

SECURE DEPLOYMENT AND AUTOMATION

Study Infrastructure as Code (IaC), configuration management, and automated security enforcement. Learn how DevOps and automation tools support consistent and secure deployment processes.

MODULE 20

MAINTAINING ORGANIZATIONAL SECURITY POSTURE

Integrate all course concepts to build, assess, and maintain a proactive organizational security program. Learn about continuous improvement, metrics, and communication with stakeholders.