Certified Cybersecurity Analyst Program

The objective of this program is to provide learners with practical skills in cybersecurity operations, including threat detection, incident response, malware analysis, and security monitoring, preparing them for Cybersecurity Analyst, Cybersecurity Operations Technician, and Tier 1 SOC Analyst roles.

100 HOURS | <DATE> | FULLY ONLINE

- Provides practical training for professionals preparing for cybersecurity operations roles.
- Builds hands-on skills in network security, cloud security, SIEM, and incident response.
- Includes applied labs, case studies, and certification assessments.
- Covers malware analysis, digital forensics, Splunk, AWS, and AI-powered security operations.
- Delivered through an online learning platform with guided instruction and practical exercises.
- Designed for professionals seeking Cybersecurity Analyst and Tier 1 SOC Analyst roles.

TARGET AUDIENCE

- Professionals with basic IT or networking knowledge
- IT and security staff seeking practical cybersecurity skills
- Professionals preparing for cybersecurity operations roles
- Individuals progressing from foundational cybersecurity training
- Anyone looking to build hands-on cybersecurity analysis skills

THE INSTRUCTOR

This program is delivered through a dedicated learning platform and supported by experienced instructors with strong backgrounds in cybersecurity, IT systems, and digital technologies.

The training combines guided instruction, hands-on labs, case studies, and applied assessments to help participants build practical skills and prepare for certification.

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.

FUNDAMENTALS COURSE

This course provides a practical foundation in cybersecurity defense covering network security, operating system protection and SOC operations. You will explore how modern organizations detect and respond to threats using industry frameworks, secure architectures and endpoint defense.

MODULE 1

CYBERSECURITY AND SOC OPERATIONS BASICS

This module introduces learners to the essential principles of cybersecurity operations and the role of a Security Operations Center (SOC). Learners will explore the structure and function of SOC teams, the frameworks that guide defensive operations, and the strategies used to identify, prevent, and respond to cyber threats. Emphasis is placed on understanding how frameworks such as NIST, MITRE ATT&CK, and the Cyber Kill Chain support organized and effective defense.

Topics Covered:

- Understanding Cybersecurity
- Defensive Strategies
- Cybersecurity Teams
- Framework Fundamentals
- NIST Framework
- MITRE Frameworks
- Cyber Kill Chain

MODULE 2

NETWORKING AND SECURITY FUNDAMENTALS

This module provides a foundational understanding of networking concepts and how they intersect with cybersecurity defense. Learners will study how data moves through networks, how secure network architectures are designed, and how monitoring tools identify and mitigate potential threats.

Topics Covered:

- Network Basics
- Network Security Introduction
- Network Monitoring
- Network Segmentation
- Secure Network Design
- Network Security Scenarios
- Email Security

MODULE 3

OPERATING SYSTEM SECURITY

This module focuses on securing modern operating systems, emphasizing the configuration and protection of endpoints across Windows and Linux environments. Learners will explore operating system security fundamentals, host protection, and endpoint detection and response (EDR) tools.

Topics Covered:

- Overview of Operating Systems
- OS Security Fundamentals
- Introduction to Host Security
- Endpoint Protection
- Endpoint Detection and Response (EDR)
- Windows Security Foundations
- Windows Security Tools
- Linux Security Foundations
- Linux Security Tools

MODULE 04

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Cyber Kill Chain
- Log Me Out
- Blocking ICMP Traffic with Windows Firewall
- Wazuh FIM and Active Response
- BitLocker
- ClamAV Malware Scan

CASE STUDY

- NOC Case Study: Resolving a Network Outage
- SOC Case Study: Mitigating a Ransomware Attack
- Case Study: Detecting a DoS Attack
- Case Study: Mitigating a MITM Attack
- Case Study: OS Security Breach

ESSENTIALS COURSE

This course introduces core monitoring and detection practices in cybersecurity, focusing on SIEM operations, network defense and cloud security. You will learn how to analyze logs, secure network traffic and monitor cloud environments.

MODULE 1
NETWORK SECURITY

This module introduces the core principles and tools used to secure modern networks. Learners will explore VPNs, firewalls, and intrusion detection and prevention systems (IDS/IPS), developing the skills to configure, monitor, and protect network environments.

Topics Covered:

- Understanding VPNs
- Implementing and Securing VPNs
- Firewall Foundations
- Creating Firewall Rules
- pfSense
- Introduction to IDS/IPS
- Configuring and Mitigating with IDS/IPS

MODULE 2
CLOUD SECURITY

This module provides a practical introduction to securing cloud environments and services. Learners will gain experience with virtualization, cloud service models, and Amazon Web Services (AWS), while learning to apply security measures that protect cloud-based infrastructure.

Topics Covered

- Virtualization Fundamentals
- Cloud Computing Fundamentals
- Amazon Web Services (AWS)
- Cloud Monitoring
- Cloud Security
- Serverless Computing Fundamentals
- Serverless Site Hosting
- Containerization Computing Fundamentals
- Container Management
- Container Orchestration

MODULE 3
SIEM AND LOG ANALYSIS

This module focuses on the use of Security Information and Event Management (SIEM) systems for real-time monitoring, detection, and response. Learners will analyze logs, correlate events, and identify anomalies using tools such as Splunk.

Topics Covered:

- Log Fundamentals
- Log Collection and Management
- SIEM Fundamentals
- SIEM Architecture and Deployment
- SIEM in Cybersecurity Operations
- Introduction to Splunk
- Searching and Reporting in Splunk
- Splunk for Security
- Log Management in SIEM
- Alert Management
- Correlation in SIEM
- Real-World SIEM Applications

MODULE 04
CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- OpenVPN Configuration
- Windows Firewall Rules Configuration
- Configuring Chain Rules in iptables
- pfSense Rules Configuration
- Ruling Snort
- Ubuntu Instance and Shell Commands
- Monitoring Lambda Functions
- SPA Creation
- ECS Fargate Container Creation
- SIEM Dashboard
- Analyzing Logs and Events Using Splunk
- Dashboards
- SIEM Integration with Apache Logs

CASE STUDY

SIEM in Action

ANALYSIS COURSE

This course provides a practical foundation in threat investigation and response, covering malware analysis, digital forensics, incident handling and AI-powered security operations. You will explore tools and techniques for detecting threats, investigating security events and using AI to enhance analysis.

MODULE 1

MALWARE ANALYSIS AND FORENSICS FUNDAMENTALS

This module introduces learners to the foundations of malware analysis and digital forensics, focusing on identifying, dissecting, and understanding malicious software.

Topics Covered:

- Introduction to Malware
- Malware Types
- Spotting Malware
- Static Analysis – Scenarios
- Forensics Fundamentals
- Basic Forensic Tools
- Sysinternals Tools
- Malware in Investigations
- Forensics in Action
- Threat Intelligence Platforms (TIPs)
- OSINT

MODULE 2

INCIDENT RESPONSE

This module provides a practical framework for responding to cybersecurity incidents from detection to recovery.

Topics Covered:

- Introduction to Incident Response
- Incident Response Lifecycle
- Organizational Plans
- Foundations of IOCs
- Investigating IOCs
- Documentation and Reporting

MODULE 3

GENAI FOR SOC ANALYSTS

This module examines how generative AI and large language models (LLMs) are transforming security operations and helping analysts automate investigations and improve threat detection.

Topics Covered:

- AI & Machine Learning
- GenAI Landscape
- Fundamentals of LLMs
- Automated Security Analysis
- Threat Intelligence & Investigation
- Phishing Detection
- GenAI-Assisted IR Workflows
- Responsible AI and Ethical Implications
- LLM Vulnerabilities
- Mitigating Risks and Challenges
- Future Directions of GenAI
- AI Scams Examples

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

CASE STUDY

- Hybrid Analysis Malware Investigation
- Dynamic Analysis with Sysinternals
- Dynamic and Static Malware Analysis
- Searching Shodan
- LLM Chat Configurations
- Advanced LLM-Powered Log Analysis
- VirusTotal & Code Insight
- Analyzing Phishing Emails
- LLM01:2025 – Prompt Injection
- LLM02:2025 – Sensitive Information Disclosure