Certified SOC Analyst Program

The objective of this program is to provide learners with practical skills in Security Operations Center (SOC) activities, including threat monitoring, log analysis, incident response, and vulnerability management, preparing them for Tier 2 SOC Analyst roles and the Certified SOC Analyst certification.

100 HOURS | <DATE> | FULLY ONLINE

- Provides practical training for professionals preparing for Security Operations Center (SOC) roles.
- Builds hands-on skills in threat monitoring, log analysis, and incident response.
- Includes applied labs, case studies, and certification assessments.
- Covers SIEM, SOAR, digital forensics, vulnerability management, and AI-driven defense.
- Delivered through an online learning platform with guided instruction and practical exercises.
- Designed for professionals seeking Tier 2 SOC Analyst and Cyber Defense Analyst roles.

TARGET AUDIENCE

- Professionals with foundational cybersecurity knowledge
- SOC analysts seeking to advance their skills
- IT and security staff involved in monitoring and response
- Cybersecurity professionals preparing for Tier 2 SOC roles
- Anyone with practical cybersecurity experience looking to specialize in SOC operations

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.

SOC OPERATIONS AND THREAT MONITORING COURSE

This course provides a practical foundation in SOC operations and threat monitoring, covering security operations concepts, network security monitoring, and intrusion detection and prevention strategies. You will learn to identify malicious activity, monitor traffic, and apply defenses to strengthen detection and response.

MODULE 1

SECURITY OPERATIONS CONCEPTS

This module explores the structure, workflows, and responsibilities within a modern Security Operations Center (SOC). Learners will understand SOC tiers, escalation paths, and quality assurance practices while developing the ability to write clear and effective incident reports.

Topics Covered:

- SOC Tiers and Escalation Paths
- SOC Metrics and Quality Assurance
- Writing Clear and Effective Incident Reports

MODULE 2

NETWORK SECURITY MONITORING

This module provides hands-on experience with the tools and techniques used to monitor network activity and detect malicious behavior. Learners will collect and inspect network traffic using Wireshark, Zeek, and other monitoring tools to build visibility across infrastructure and support proactive SOC operations.

Topics Covered:

- Advanced Network Traffic Collection and Inspection
- Foundations of Network Telemetry in the SOC
- SNMP for Device and Infrastructure Monitoring
- Zeek for Protocol-Level Network Visibility
- Infrastructure Monitoring with Nagios
- Application and Network Monitoring with Zabbix

MODULE 3

INTRUSION DETECTION AND PREVENTION STRATEGIES

This module builds essential computer literacy skills by introducing learners to digital systems, core components, and the interaction between software and hardware. Topics include data, operating systems, and command-line interfaces.

Topics Covered:

- Living in a Digital Age
- Computer Components
- Operating Systems

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Sigma to SIEM
- Incident Report Analysis
- Trace Ann's Activities on the Network
- Traffic Analysis
- Extracting Files – Wireshark & NetworkMiner
- SNMP Configuration on Cisco
- Zeek It
- Install and Configure Nagios
- Zabbix Resource Monitoring
- Suricata Installation on pfSense
- Anomaly Detection
- Writing and Testing Suricata Rules with PCAP

CASE STUDY

The Olympics Cyber-Attack

THREAT DETECTION AND LOG ANALYSIS COURSE

This course provides a practical foundation in threat detection and log analysis, covering SIEM tuning and alert operations, SOAR fundamentals, and advanced Windows and Linux log analysis. You will learn to optimize detection rules, automate response workflows, and analyze system logs to uncover threats and support faster incident response.

MODULE 1

SIEM TUNING AND ALERT OPERATIONS

This module introduces the full lifecycle of security alert management, from event triage to SIEM optimization. Learners explore incident analysis techniques, alert classification, and false positive reduction strategies to improve detection accuracy and efficiency.

Topics Covered:

- Foundations of Incident Analysis
- Working with Security Alerts
- SIEM Tuning and Alert Optimization
- Access Management Attacks
- HTTP – The Main Protocol Behind the Web
- Web Attacks

MODULE 2

INTRODUCTION TO SOAR

Learners are introduced to Security Orchestration, Automation, and Response (SOAR) technologies and their role in modern SOC operations. The module covers key SOAR components, playbook automation, and incident management workflows using Splunk SOAR.

Topics Covered:

- SOAR Foundations
- SOAR Key Features
- Splunk SOAR
- SOAR Advanced Integrations
- Serverless Computing Fundamentals

MODULE 3

ADVANCED WINDOWS AND LINUX LOG ANALYSIS

This module develops advanced skills in cross-platform log analysis for security monitoring and threat detection. Learners analyze Windows and Linux event data to identify authentication anomalies, privilege escalation, and lateral movement.

Topics Covered:

- Critical Windows Event IDs for Security Analysis
- Linux System Logs and Authentication Monitoring
- Cross-System Event Correlation for Investigation
- Detecting Privilege Escalation and Lateral Movement in Logs

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Tune and Test a SIEM Rule
- Domain Breach Investigation
- Detecting with Splunk
- SQL Injection Investigation
- Web Injection
- Implementing Splunk SOAR Playbook
- Windows Log Correlation and Analysis in Splunk

CASE STUDY

- Zoom and the Cost of Weak Access Controls
- Heartland Payment Systems
- How SOAR Improved Incident Response at a SOC

INCIDENT RESPONSE AND VULNERABILITY MANAGEMENT COURSE

This course provides practical training in incident response and vulnerability management, covering digital evidence acquisition, response processes, and purple teaming with AI-driven defense. You will learn to collect and preserve evidence, coordinate effective responses, and apply advanced techniques to strengthen organizational resilience.

MODULE 1

DIGITAL EVIDENCE ACQUISITION

This module provides a practical introduction to digital forensics and evidence handling in cybersecurity investigations. Learners explore how to identify, collect, and preserve digital evidence while maintaining chain of custody and forensic integrity.

Topics Covered:

- Digital Forensics
- Digital Evidence
- Digital Investigation
- Forensics Workstations
- Computerized System & Memory
- Cryptography and Digital Forensics
- Memory Dump Analysis
- Non-Volatile Data Acquisition

MODULE 2

INCIDENT RESPONSE

Learners develop the foundational skills required to manage and respond to security incidents effectively. This module covers incident response teams, the NIST incident response model, and best practices for preparation, detection, containment, and recovery.

Topics Covered:

- Introduction to Incident Response
- Notable Security Incidents
- Incident Response Plan
- Incident Response Scenarios
- Phishing Email Investigations

MODULE 3

PURPLE TEAMING AND AI-DRIVEN DEFENSE

This module bridges offensive and defensive security practices through collaborative purple teaming. Learners explore AI agents and how they can be used in SOC operations to improve detection, analysis, and response.

Topics Covered:

- Foundations of AI Agents
- Agent Safety, Evaluation & Limits
- The Blue Role in Purple Teaming
- Simulation of Attack

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Forensic Imaging Using FTK Imager
- MemorizeMe
- Process Investigation
- Memory Acquisition
- Autopsy Walkthrough
- Phishing Attachment Analysis
- Your First Agent

CASE STUDY

- Equifax Breach (2017)
- National Public Data Breach
- 2024 CDK Global Cyberattack
- Red Scenario Analysis and Rule Tuning – Part 1
- Red Scenario Analysis and Rule Tuning – Part 2