+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 22/08/2025

Sign up

SOC Analyst Training

8 days (56 hours)

Presentation

Today, cybersecurity is at the heart of the strategic challenges faced by organizations faced with intensifying threats and increasingly sophisticated attacks. The SOC plays a central role in detecting, analyzing and responding to incidents. This "SOC (Security Operations Center) Analyst" training course is designed for professionals who want to understand the mechanisms of defensive cybersecurity, master SOC tools and methodologies, and develop the skills needed to effectively protect information systems.

During this training course, you will learn to master the fundamentals of defensive cybersecurity and understand the role and missions of the SOC analyst within an organization. You'll learn about the threat ecosystem, attack techniques (phishing, ransomware, APT, data exfiltration) and detection and monitoring methodologies.

You will be trained in the use of key SOC tools (SIEM, SOAR, EDR, IDS/IPS, Threat Intelligence), in the analysis and correlation of security events, and in desktop and network investigation. You will also learn to manage incidents according to international standards (NIST, ISO 27035), from detection to remediation, and to produce usable technical reports for CISOs, IT teams and management.

Finally, you will consolidate your skills through case studies and practical workshops.
You'll learn all about the SIEM system: triaging alerts in a SIEM, analyzing malicious traffic, forensic investigation, crisis management in the face of ransomware and simulating a first day in a SOC.

On completion of this course, you will be able to detect, analyze and respond effectively to security incidents.

Objectives

- Understand the role and missions of an SOC analyst
- Master the fundamentals of defensive cybersecurity

- Use SOC tools and technologies
- Analyze and correlate security events
- Manage security incidents
- Write technical reports
- Coordinate with other cybersecurity teams
- Monitor cyber threats and attack techniques

Target audience

- Systems and network technicians and administrators
- IT managers
- Security consultants
- Engineers
- technical managers
- network architects
- project managers

Prerequisites

- Knowledge of networks.
- Completion of the introductory cybersecurity course or equivalent knowledge.

SOC ANALYST TRAINING PROGRAM

[Day 1 - Morning]

Introduction to defensive cybersecurity

- Learning objectives and target skills
- Fundamentals of defensive cybersecurity: principles of protection, detection and response
- Overview of defensive cybersecurity
- Assets, threats and attack surfaces (CIA, MITRE ATT&CK)
- Organization of cyber professions & role of the SOC
- Practical workshop: Mapping IS threats with MITRE ATT&CK.

[Day 1 - Afternoon] SOC analyst

fundamentals

- SOC analyst missions (L1, L2, L3)
- SOC value chain: monitoring, detection, investigation, reporting
- Coordination with other teams (CERT, CSIRT, Blue Team, Red Team)
- Role of the SOC analyst in the defense chain and incident lifecycle management
- Overview of SOC tools (SIEM, SOAR, EDR, Threat Intel)

- Practical workshop: Simulation of alert triage in a SIEM.

[Day 2 - Morning]

Overview of cyber threats

- Attack typology (phishing, ransomware, DDoS, APT)
- Exploitation of vulnerabilities (CVE, CVSS)
- Social engineering and hybrid attacks
- Workshop: Analysis of a suspicious email (phishing).

[Day 2 - Afternoon] Cyber

watch

- Introduction to cyber intelligence (CERT-FR, OSINT, Threat Intel feeds)
- Integrating intelligence into the day-to-day work of a SOC analyst
- Notions of Threat Intelligence (IoC: hash, IP, domain)
- Practical workshop: Building a cyber intelligence mini-dashboard.

[Day 3 - Morning]

SIEM

- SIEM architecture and principles (Splunk, ELK, QRadar)
- Log sources: systems, networks, applications, cloud
- Event parsing and normalization
- Practical workshop: Log collection and visualization via ELK.

[Day 3 - Afternoon] Log

collection

- Log correlation to detect simple patterns
- Basic SIEM investigation (suspicious authentication, brute force)
- Analyze and correlate security events to identify potential incidents
- Practical workshop: Correlating network and system events in a SIEM.

[Day 4 - Morning]

Endpoint Detection & Response (EDR)

- Endpoint detection and response (EDR)
- Signatures vs. behavioral detection
- Investigating a compromised workstation
- Practical workshop: Analysis of an infected workstation using an EDR.

[Day 4 - Afternoon]

Networks and real-time monitoring

- Capture and analysis of network traffic (Wireshark, Zeek)
- IDS/IPS signatures (Snort, Suricata)
- Netflow monitoring
- Network anomaly detection and data exfiltration
- Practical workshop: Analysis of malicious traffic with Wireshark.

[Day 5 - Morning]

SOC investigation methodology

- Detection process ? analysis ? qualification
- False positives, confirmed incidents
- Introduction to technical reporting (writing an incident qualification)
- Practical workshop: Qualifying a raw alert as a confirmed incident.

[Day 5 - Afternoon]

Incident management process

- Incident management (NIST SP 800-61, ISO 27035 - simplified)
- Stages: preparation, containment, eradication, feedback
- Managing security incidents throughout their lifecycle
- Internal and external incident communication
- Practical workshop: Table-top exercise on a ransomware attack.

[Day 6 - Morning]

Investigation and forensics

- Introduction to forensics: acquiring and preserving evidence
- System, disk and memory logs
- Presentation of tools (Volatility, Autopsy, FTK Imager - demonstration)
- Practical workshop: extracting evidence from a compromised machine.

[Day 6 - Afternoon]

Scripts and task automation

- Good hardening practices (systems & networks)
- Vulnerability management (scanners, patch management)
- Application security as seen by the SOC (simplified OWASP Top 10)
- Practical workshop: Detecting SQL injection in application logs.

[Day 7 - Morning]

SOC automation and orchestration (SOAR)

- SOC automation: SOAR (principles, simple playbooks)
- Useful scripts (Python/PowerShell - accessible level)
- Practical workshop: Simple Python script to extract IoCs from logs.

[Day 7 - Afternoon] Reporting

& communication

- SOC technical reporting (post-incident reports, MTTD/MTTR indicators)
- Communication to CISO, CIO, COMEX
- Capitalization and RETEX (SOC knowledge base)
- Writing clear, usable technical reports to document security incidents
- Practical workshop: Writing an incident report + summary presentation to COMEX.

[Day 8 - Morning]

Case study

- Comprehensive case study: IS compromise
- Initial log analysis and detection
- Multi-source investigation (SIEM, EDR, network)
- Containment and remediation
- Practical workshop: Complete end-to-end practical exercise.

[Day 8 - Afternoon]

Preparing to take up the position of SOC Analyst

- Proactive threat hunting (basics)
- Anticipation of emerging threats (IoT, supply chain, AI - popularized)

- Preparing for the position of SOC Analyst
- Ethics and legal aspects of cyber surveillance
- Certifications and prospects (CEH, CompTIA Security+, SOC Analyst)
- Situational workshop: Simulation of a first day as a SOC.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level on different types of technology, as well as his or her expectations and personal objectives with regard to the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.