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

Updated on 09/02/2026

Sign Up

Certified Security Operations Manager Training and Certification

5 days (35 hours)

Overview

The Certified Security Operations Manager (CSOM) Certification Training prepares experienced professionals to lead a modern SOC, structure its defense capabilities, and pass the official Certified Security Operations Manager (CSOM) certification exam.

This advanced training course enables you to go beyond alert handling to master the strategic, operational, and human challenges of a Security Operations Center. You will learn how to align security activities with business objectives, risks, and compliance requirements.

You will study the design of a SOC operational model, team organization, the management of detection tools, case management, and the standardization of incident response processes.

The program also covers threat intelligence, vulnerability management, threat hunting, incident response, forensics, and the continuous improvement of defensive capabilities.

Upon completion of the course, you will be able to effectively prepare for the Certified Security Operations Manager (CSOM) exam, apply a SOC maturity framework, and justify operational decisions in practical certification scenarios.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Design and manage a SOC aligned with business risks and priorities.
- Structure processes for incident detection, investigation, and response.
- Assess the maturity of SOC capabilities and define a roadmap for improvement.
- Implement relevant metrics for management and executive communication.
- Prepare for the written and practical exams for the Certified Security Operations Manager (CSOM) certification.

Target Audience

- SOC Manager
- Senior SOC Analyst
- Cybersecurity Manager
- Incident Response Manager
- Cybersecurity Consultant

Requirements

- Two or more years of experience in defensive cybersecurity operations.
- Proficiency in incident response and SOC investigation processes.
- Operational knowledge of security logs, alerts, and SIEM use cases.
- Understanding of Windows, Linux, and network environments.

Technical Requirements

- Workstation with a quad-core processor, 16 GB of RAM, and at least 20 GB of available disk space.
- Windows 11, macOS 13, or a recent Linux distribution.
- Google Chrome, Mozilla Firefox, or Microsoft Edge browser in a supported version.
- Stable Internet connection without filtering that blocks lab platforms and remote access.
- Ability to use a virtual machine or an isolated lab environment.

Certified Security Operations Manager Training Program

[Day 1 - Morning]

Foundations of SOC Governance

- Strategic positioning of a SOC within cybersecurity governance.
- Alignment between business objectives, risks, regulatory requirements, and security services.
- Analysis of internal, outsourced, and hybrid operational models.
- Defining a SOC charter, responsibilities, and interfaces with stakeholders.

- Hands-on workshop: Developing a SOC charter and service catalog for a multi-site organization.

[Day 1 – Afternoon]

Operations Architecture and Organization

- Designing an architecture for event collection, correlation, and enrichment.
- Roles, support levels, skills, and escalation procedures within SOC teams.
- Sizing resources based on coverage, operating hours, volumes, and risk level.
- Governance of SIEM, SOAR, and EDR tools, and case management.
- Hands-on workshop: Defining the target organization, the RACI matrix, and the coverage model for a 24/7 SOC.

[Day 2 – Morning]

Threat modeling and defensive prioritization

- Identifying critical assets, sensitive processes, and threat scenarios.
- Applying threat modeling to the design of monitoring capabilities.
- Prioritizing log sources based on detection value, cost, and risks covered.
- Translating threats into detection requirements and operational use cases.
- Hands-on workshop: creating a threat model and a log prioritization matrix for a critical service.

[Day 2 - Afternoon]

Detection engineering and case management

- The lifecycle of detection rules, from business request to production deployment.
- Designing detections based on MITRE ATT&CK, behaviors, and indicators.
- Reducing false positives, analytical validation, and exception handling.
- Structuring investigation files, from case qualification to case closure.
- Hands-on workshop: Design a detection use case, its triage criteria, and its processing workflow.

[Day 3 – Morning]

Incident Response and Crisis Management

- Coordination between SOC procedures, incident response plans, and crisis management.
- Decision-making roles, escalation criteria, and coordination of technical and business teams.

- Designing playbooks tailored to high-priority incident scenarios.
- Post-incident lessons learned, corrective actions, and operational feedback.
- Hands-on Workshop: Managing a Response to a Security Breach, Including Decision-Making, Communication, and an Action Plan.

[Day 3 - Afternoon]

Specialized Defensive Capabilities

- Organizing threat intelligence activities and integrating them into SOC operations.
- Managing vulnerability management and coordinating it with detection and remediation.
- The role of threat hunting, forensics, and malware analysis.
- Selecting skills, tools, and deliverables for each specialized capability.
- Hands-on workshop: Developing a capability development roadmap for a mature SOC.

[Day 4 - Morning]

Maturity and Continuous Improvement

- Principles of SOC maturity models and criteria for evaluating capabilities.
- Assessment of the people, processes, technologies, data, and governance dimensions.
- Analysis of gaps between the current state, the target maturity level, and residual risks.
- Development of a prioritized, costed roadmap that can be justified to senior management.
- Hands-on workshop: Conduct a SOC maturity assessment and propose a 12-month transformation plan.

[Day 4 – Afternoon]

Metrics and Executive Communication

- Selection of KPIs, KRIs, and performance metrics tailored to security operations.
- Measuring detection coverage, response times, quality, and analytical workload.
- Building dashboards for operational teams, management, and internal clients
  .
- Assessment of the value, cost, and return on investment of SOC capabilities.
- Hands-on workshop: Design a SOC management dashboard and present recommendations to an executive committee.

[Day 5 - Morning]

Systematic preparation for the

- Mapping of the competency areas assessed by the Certified Security Operations Manager (CSOM) exam.
- Review of concepts related to governance, SOC design, defensive capabilities, and maturity.
- Strategies for reading scenarios, analyzing constraints, and justifying decisions.
- Preparation for the theoretical exam and practical certification scenarios.
- Hands-on workshop: solving a mock certification case study focused on creating and prioritizing a SOC program.

[Day 5 – Afternoon]

Certification simulation and action plan

- Analysis of cross-functional scenarios involving governance, detection, response, and metrics.
- Analysis of design choices, operational trade-offs, and implementation risks.
- Review of common errors in theoretical questions and practical deliverables.
- Development of an individual study plan and exam preparation strategy.
- Hands-on workshop: Conduct a final certification simulation with a detailed presentation of a SOC maturity plan.

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired

of the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.