Certified Security Operations Manager (CSOM)

Course Duration: 4 Days
Exam Reference: CSOM

Course Overview

This Security Operations Management training is designed for leaders, focusing on how to plan, build, and mature security operations teams within an enterprise. You will gain the strategic and managerial knowledge required to effectively lead functions like Incident Response, Threat Hunting, and SIEM. The course emphasizes governance, metrics, and managing people and processes to mature the entire security operations capability.

Prerequisites

2+ Years Sec Operations experience.

Course Objectives

Upon completion, you will be able to:

- Perform threat modeling to strategically identify and prioritize threats to the organization.
- Understand the core security operations functions, the services they provide, and their business value.
- Learn how to build a SOC, including staffing, technology stack selection, and process definition.
- Conduct maturity assessments for key security teams (SOC, IR, Hunting, and CTI).
- Master the use of metrics for effective reporting and problem identification at the managerial level.

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

Certified Security Operations Manager (CSOM)

Course Outline

Module 1: Modern Security Operations

- Business Objectives, Legal Enablers, and Considerations (Aligning SOC with Governance)
- Security Operations Team (Roles, Structure, and Collaboration Models)

Module 2: Building a Security Operations Team

- Threat Modelling (Techniques and methodologies for identifying organizational threats)
- Building Your Team (Staffing, Training, and Organizational Placement)
- SIEM & Detection Engineering (Strategic planning and selection of detection technologies)
- Case Management (Process, standardization, and tooling)
- Other Tooling & Administration (Vulnerability Scanners, Endpoint tools, etc.)
- Processes and Documentation (Playbooks, Runbooks, SOPs)

Module 3: Capability Development
Incident Response (Building the full lifecycle capability)

- Threat Intelligence (Integration into SOC workflows and strategic decision-making)
- Vulnerability Management (Process ownership and cross-functional remediation)
- Digital Forensics (Establishing forensic readiness and collection capabilities)
- Malware Analysis (Integrating analysis output into detection)
- Threat Hunting (Establishing a hunting program and team structure)

Module 4: Metrics, Maturity, and Measuring Success

- Maturity Models (Using frameworks to assess and advance SOC capability)
- Operationalizing MITRE ATT&CK (Mapping detections and controls to adversary tactics)
- Cyber Deception (Implementing deception techniques like honeypots)
- Security Orchestration, Automation, and Response (SOAR) (Strategy and implementation)
- Reporting and Metrics (KPIs, KRIs, Executive Reporting, and Dashboards)
- Security Research & Presentation (Staying current and communicating risk to leadership)
- Retaining Talent (Strategies for team morale and skill development)