

Certified Security Operations Manager (CSOM)

Proposed instructor-led schedule: 5 days |

Course Overview

Certified Security Operations Manager (CSOM) is designed for established or aspiring security operations managers and focuses on developing high-performing security operations teams. The published syllabus is organised around Modern Security Operations; Building a Security Operations Centre; Capability Development; and Metrics, Maturity, and Measuring Success, followed by exam preparation. This proposed five-day instructor-led schedule groups the published domains for delivery and is not an official provider-issued timetable.

Day-wise Breakdown

Day 1: Modern Security Operations

- Introduction to modern security operations
- Business objectives, legal enablers, and operational considerations
- Security operations teams and responsibilities
- Operational environments and service models
- Cyber threat hunting: purpose and operational integration
- Aligning security operations priorities with business needs

Day 2: Building a Security Operations Centre

- SOC design, scope, operating model, and service structure
- Threat modelling to inform monitoring and response priorities
- Building the team: roles, staffing, skills, and development
- SIEM and detection engineering
- Case management and incident workflow
- Security tooling, administration, processes, and policies

Day 3: Capability Development

- Incident response capability and operational coordination
- Threat intelligence: collection, analysis, and operational use
- Vulnerability management and remediation prioritisation
- Digital forensics and evidence handling
- Malware analysis capability and investigative support
- Threat-hunting programme and team structure

Day 4: Metrics, Maturity, and Measuring Success

- SOC maturity models and capability assessment
- Operationalising MITRE ATT&CK to assess detection and control coverage
- Purple-team engagements and validation of defensive effectiveness
- Deception and active defence
- Security orchestration, automation, and response (SOAR)
- Reporting, KPIs, risk indicators, dashboards, and executive communication

Day 5: Sustaining Performance and Exam Preparation

- Security research and presentation of operational findings
- Retaining talent, developing skills, and supporting team effectiveness
- Additional operational improvement activities
- Review of SOC capability development and management decisions
- CSOM theory exam format and preparation approach
- CSOM practical assessment format and scenario-based preparation