QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1987

Security Operations Center (SOC) Management & Operations Training Course

SECURITY OPERATIONS & INCIDENT RESPONSE
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Security Operations Center (SOC) Management & Operations Training Course provides a comprehensive practical framework for designing, managing, operating, and continuously improving a modern Security Operations Center. The program focuses on establishing effective security operations capabilities that provide continuous visibility, threat monitoring, detection, analysis, incident response, and cybersecurity risk management.

Participants will explore the organizational, operational, and technical components of a SOC, including operating models, team structures, roles and responsibilities, workflows, escalation procedures, monitoring processes, alert management, incident handling, threat intelligence, and performance measurement. The course emphasizes how these components work together to create an efficient and risk-focused security operations capability.

A major focus is placed on day-to-day SOC operations. Participants will learn how to manage security alerts, perform triage, investigate suspicious activities, coordinate incident response, maintain operational procedures, manage workloads, and improve collaboration between security analysts, incident responders, IT teams, risk functions, and management. The program also addresses the effective use of centralized security monitoring, automation, and security technologies within SOC operations.

The course further addresses SOC governance, performance management, service quality, workforce planning, operational resilience, and continuous improvement. Through practical scenarios, operational simulations, incident investigations, performance exercises, and SOC design workshops, participants will develop the capabilities required to establish a mature, measurable, and sustainable Security Operations Center.

Objectives

- By the end of the course, participants will be able to:
- Explain the strategic role and core functions of a Security Operations Center.
- Assess organizational requirements for establishing or improving SOC capabilities.
- Design appropriate SOC operating models and organizational structures.
- Define SOC roles, responsibilities, workflows, and escalation procedures.

- Establish effective security monitoring and alert management processes.
- Apply structured methods for security alert triage and investigation.
- Coordinate SOC activities with incident response and crisis management.
- Integrate threat intelligence into SOC monitoring and detection.
- Improve the use of security information and event management capabilities within SOC operations.
- Evaluate opportunities for security automation and workflow optimization.
- Establish effective SOC performance indicators and service measures.
- Manage analyst workloads, operational priorities, and shift-based operations.
- Strengthen SOC governance, documentation, and operational controls.
- Assess SOC maturity and identify operational and capability gaps.
- Develop continuous improvement initiatives for SOC effectiveness.
- Create a strategic roadmap for building or advancing SOC operations.

Who Should Attend

This course is designed for SOC managers, SOC team leaders, security operations analysts, security monitoring professionals, incident response specialists, threat detection analysts, security engineers, and information security professionals involved in security operations.

It is also suitable for cybersecurity managers, chief information security professionals, IT managers, threat intelligence specialists, vulnerability management teams, risk and compliance professionals, business continuity specialists, and technology leaders responsible for establishing, managing, or overseeing security operations.

The program is particularly relevant to government entities, ministries, banks and financial institutions, oil and gas organizations, telecommunications companies, critical infrastructure operators, technology organizations, multinational corporations, and large enterprises seeking to establish, mature, or optimize their Security Operations Center capabilities.

Learning Outcomes

- Upon completion of the course, participants will be able to:
- Assess the current maturity and operational effectiveness of a SOC.
- Select an appropriate SOC operating model based on organizational requirements.
- Define SOC organizational structures, roles, responsibilities, and reporting lines.
- Establish effective workflows for monitoring, detection, investigation, and response.
- Develop structured procedures for alert triage and escalation.
- Investigate security events and determine appropriate response actions.
- Coordinate SOC operations with incident response and other security functions.
- Integrate threat intelligence into security monitoring and operational decision-making.
- Improve the use of SIEM and related security monitoring technologies.
- Identify opportunities to automate repetitive SOC activities.
- Manage SOC workloads, priorities, shifts, and operational capacity.
- Develop meaningful SOC performance indicators and management reports.
- Identify gaps in people, processes, technology, and governance.
- Establish quality assurance and continuous improvement mechanisms.
- Strengthen operational resilience and service continuity.
- Develop a practical roadmap for SOC maturity and capability improvement.

Course Outline

DAY 01

SOC Strategy, Architecture and Operating Models

- Role and strategic importance of the Security Operations Center.
- Core SOC functions and operational responsibilities.
- SOC operating models and organizational structures.
- Internal, outsourced, and hybrid SOC models.
- SOC roles, responsibilities, and competency requirements.
- Security monitoring and visibility requirements.
- SOC processes and operational workflows.

DAY 01 — CONTINUED

- Asset and data source prioritization.
- Integration with cybersecurity governance and risk management.
- SOC policies, procedures, and documentation.
- Escalation structures and communication channels.
- Designing an effective SOC operating framework.

PRACTICAL APPLICATION

Design a high-level SOC operating model for a selected organization, including functions, roles, workflows, escalation paths, and priority monitoring requirements.

DAY 02

SOC Monitoring, Alert Management and Threat Detection

- Security monitoring principles and operational visibility.
- Security event and log management.
- SIEM capabilities within SOC operations.
- Security alert generation and management.
- Alert classification and prioritization.
- Alert triage and investigation workflows.
- Identifying indicators of compromise.
- Detecting suspicious user, endpoint, and network behavior.
- Detection use cases and correlation rules.
- False-positive management and alert tuning.
- Threat intelligence integration.
- Improving detection coverage and monitoring effectiveness.

PRACTICAL APPLICATION

Analyze a series of SOC alerts, prioritize them based on risk, conduct initial investigations, and determine appropriate escalation actions.

DAY 03

SOC Incident Response and Operational Coordination

- SOC responsibilities throughout the incident lifecycle.
- Incident identification and initial assessment.
- Security incident triage and classification.
- Investigation and evidence collection.
- Incident escalation and handoff.
- Coordination between SOC and incident response teams.
- Containment and response support.
- Managing high-severity security incidents.
- Coordination with IT, infrastructure, risk, legal, compliance, and business teams.
- Incident documentation and case management.
- Communication during security incidents.
- Post-incident review and lessons learned.

> **PRACTICAL APPLICATION**
>
> Conduct a simulated SOC incident from initial alert through investigation, escalation, response coordination, and post-incident review.

DAY 04

SOC Management, Automation and Performance

- Managing SOC analysts and operational teams.
- Shift management and 24-hour operational coverage.
- Workload distribution and prioritization.
- Analyst skills, competency development, and performance.
- Security automation and workflow orchestration.
- Automating repetitive monitoring and response tasks.
- Improving operational efficiency.
- SOC service quality and operational controls.
- Key performance and operational indicators.

DAY 04 — CONTINUED

- Measuring alert handling and response performance.
- Management dashboards and reporting.
- Managing operational risks and service continuity.

PRACTICAL APPLICATION

Develop a SOC performance framework including staffing requirements, workload management, operational indicators, service measures, automation opportunities, and management reporting.

DAY 05

SOC Governance, Maturity and Continuous Improvement

- SOC governance and accountability.
- Security operations policies and standards.
- Assessing SOC maturity and capability.
- Identifying people, process, technology, and governance gaps.
- Detection and response capability assessment.
- Quality assurance and operational reviews.
- Benchmarking SOC performance.
- Continuous improvement and optimization.
- Improving analyst effectiveness and operational workflows.
- Building resilience into SOC operations.
- Strategic SOC development and transformation.
- Developing a long-term SOC maturity roadmap.

FINAL WORKSHOP

Develop an integrated Security Operations Center management and operations framework for a selected organization, covering operating model, organizational structure, monitoring, detection, alert management, incident response, threat intelligence, automation, staffing, performance measurement, governance, maturity assessment, and continuous improvement.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/security-operations-center-soc-management-operations-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440