Security Operations Management and Metrics Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the age of Cloud Security, AI-driven threats, and rapid digital transformation, traditional Security Operations Centers are struggling with alert fatigue, the global cybersecurity skills gap, and overwhelming threat intelligence volumes. Security Operations Management and Metrics Training Course moves beyond basic incident response to equip leaders and analysts with the advanced knowledge required for a proactive defense posture. The focus is on implementing a data-driven security strategy by establishing clear Security KPIs and Metrics such as MTTD, MTTR, and Security ROI. Mastering these concepts is no longer just a technical requirement, but a critical business mandate for achieving organizational cyber resilience and aligning SecOps efficacy with core enterprise risk management goals.

This intensive training is designed to transform security professionals into strategic operators capable of managing a modern, agile SOC. You will learn to implement Security Orchestration, Automation, and Response (SOAR) platforms, leverage UEBA for advanced threat hunting, and map your operational effectiveness to industry-standard frameworks like NIST CSF and MITRE ATT&CK. Through practical real-world case studies and hands-on labs, you will gain the expertise to optimize workflow, prioritize vulnerabilities, and effectively communicate complex cyber risk to executive leadership. Invest in this course to build a High-Fidelity SOC that not only detects and responds to threats faster but also demonstrates quantifiable Return on Security Investment

Programme Curriculum

Security Operations Management and Metrics Training Course

Introduction

In the age of Cloud Security, AI-driven threats, and rapid digital transformation, traditional Security Operations Centers are struggling with alert fatigue, the global cybersecurity skills gap, and overwhelming threat

intelligence volumes. Security Operations Management and Metrics Training Course moves beyond basic incident response to equip leaders and analysts with the advanced knowledge required for a proactive defense posture. The focus is on implementing a data-driven security strategy by establishing clear Security KPIs and Metrics such as MTTD, MTTR, and Security ROI. Mastering these concepts is no longer just a technical requirement, but a critical business mandate for achieving organizational cyber resilience and aligning SecOps efficacy with core enterprise risk management goals.

This intensive training is designed to transform security professionals into strategic operators capable of managing a modern, agile SOC. You will learn to implement Security Orchestration, Automation, and Response (SOAR) platforms, leverage UEBA for advanced threat hunting, and map your operational effectiveness to industry-standard frameworks like NIST CSF and MITRE ATT&CK. Through practical real-world case studies and hands-on labs, you will gain the expertise to optimize workflow, prioritize vulnerabilities, and effectively communicate complex cyber risk to executive leadership. Invest in this course to build a High-Fidelity SOC that not only detects and responds to threats faster but also demonstrates quantifiable Return on Security Investment

Course Duration

5 days

Course Objectives

1. Strategically design and staff a modern High-Fidelity SOC model.
2. Implement and manage the SOC maturity model across all core functions.
3. Define, calculate, and benchmark critical Security KPIs like MTTD, MTTR, and MTTC.
4. Master the integration and workflow automation using SOAR platforms.
5. Develop an advanced Threat Hunting program utilizing the MITRE ATT&CK framework.
6. Build effective, context-rich dashboards and reports for Executive Risk Communication.
7. Apply Zero Trust Architecture (ZTA) principles to daily security operations.
8. Operationalize Cloud Security Posture Management (CSPM) in a multi-cloud environment.
9. Reduce Alert Fatigue through effective triage, tuning, and behavioral analytics.
10. Conduct Vulnerability Prioritization and Remediation based on business impact and exploitability.
11. Link security metrics directly to quantifiable Return on Security Investment (ROSI).
12. Establish a continuous Compliance Monitoring and audit process
13. Lead and execute full End-to-End Incident Response and forensics processes.

Target Audience

1. SOC Managers and Team Leads.
2. Senior Security Analysts.
3. CISO/VP of Security.
4. IT/Security Architects.
5. Risk & Compliance Officers.
6. Incident Response and Forensics Specialists.
7. DevSecOps Engineers.
8. Technical Program Managers.

Course Modules

Module 1: The Strategic SOC and Maturity Model

- SOC Design and Operating Models.
- Defining the SOC Maturity Model stages and self-assessment.
- Budgeting and staffing a modern SOC.
- Aligning the SOC mission with enterprise Business Resilience objectives.
- Case Study: Transitioning from a reactive, log-review SOC to a proactive, Threat Hunting organization.

Module 2: Foundational Security Metrics & KPIs

- Mean Time to Detect.
- Mean Time to Respond & Contain.
- The business value of Dwell Time reduction and its impact on breach cost.
- Measuring Security Control Efficacy against simulated attacks.
- Case Study: A financial firm reducing MTTD by 40% using advanced SIEM correlation rules.

Module 3: Advanced Threat Hunting and Intelligence

- Operationalizing Threat Intelligence.
- Applying the MITRE ATT&CK Framework for defense gap analysis and threat simulation.
- Developing and executing a structured Threat Hunting methodology.
- Leveraging User and Entity Behavior Analytics for detecting insider threats.
- Case Study: Using CTI to proactively hunt for a specific APT group's TTPs within the network logs.

Module 4: Security Orchestration, Automation, and Response (SOAR)

- Introduction to SOAR and the concept of Security Playbooks.
- Designing and implementing a tiered Incident Response automation strategy.
- Practical hands-on lab: Building a Phishing Triage and Containment Playbook.
- Integrating SOAR with third-party tools.
- Case Study: Automating 70% of low-fidelity alerts to significantly reduce Analyst Alert Fatigue.

Module 5: Vulnerability and Patch Management Metrics

- Moving beyond CVSS.
- Calculating and improving the Vulnerability Remediation Rate and Patch Latency.
- Metrics for measuring the effectiveness of your Asset Inventory program.
- Integrating vulnerability scanners with ticketing and patch management systems.
- Case Study: Prioritizing the top 10% of vulnerabilities that pose 90% of the actual risk

Module 6: Cloud and Hybrid Security Operations

- SecOps challenges in Multi-Cloud and hybrid environments.
- Implementing Cloud Security Posture Management metrics and tools.
- Monitoring cloud workloads and serverless environments for security anomalies.
- Establishing Zero Trust operational policies and measuring compliance.
- Case Study: Incident response in a public cloud environment involving a misconfigured S3 bucket or equivalent Cloud Native exploit.

Module 7: Executive Reporting and Return on Security Investment (ROSI)

- Translating technical metrics into Executive Risk Language.

- Creating a C-Suite Dashboard focused on governance and strategic risk posture.
- Calculating and demonstrating Return on Security Investment for a security tool or project.
- Mapping operational metrics to compliance frameworks.
- Case Study: Presenting a compelling ROSI case to secure funding for a new SOAR platform.

Module 8: Incident Response Leadership and Post-Incident Analysis

- Leading the Incident Response Team through a major security breach.
- Legal, PR, and regulatory considerations during an active security incident.
- Performing structured Root Cause Analysis and post-incident reviews.
- Implementing a continuous feedback loop for process and tool refinement.
- Case Study: Simulating a major Ransomware Attack and evaluating the team?ÇÖs effectiveness using a Tabletop Exercise scorecard.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com