Security Operations Center (SOC) Tier 1 Analyst Training Course

Professional Development Training Course Outline

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

Course Introduction

Security Operations Center (SOC) Tier 1 Analyst Training Course provides participants with the foundational knowledge and practical skills needed to detect, respond, and escalate cybersecurity threats in real-time. This course emphasizes key SOC functions, including log monitoring, threat analysis, incident response, security alert triage, and the use of Security Information and Event Management (SIEM) tools. Participants gain insights into threat intelligence, attack vectors, and the workflow of a SOC, preparing them to act decisively in fast-paced cybersecurity environments.

With increasing cyber threats targeting enterprises globally, organizations require highly skilled Tier 1 SOC analysts to monitor, identify, and respond to incidents efficiently. This course combines theoretical knowledge with hands-on exercises, enabling participants to interpret security logs, detect anomalies, manage alerts, and escalate incidents to Tier 2 and Tier 3 teams. Learners also explore best practices in documentation, reporting, and communication within SOC frameworks, ensuring operational efficiency, regulatory compliance, and proactive threat management.

Programme Curriculum

Security Operations Center (SOC) Tier 1 Analyst Training Course

Introduction

Security Operations Center (SOC) Tier 1 Analyst Training Course provides participants with the foundational knowledge and practical skills needed to detect, respond, and escalate cybersecurity threats in real-time. This course emphasizes key SOC functions, including log monitoring, threat analysis, incident response, security alert triage, and the use of Security Information and Event Management (SIEM) tools. Participants gain insights into threat intelligence, attack vectors, and the workflow of a SOC, preparing them to act decisively in fast-paced cybersecurity environments.

With increasing cyber threats targeting enterprises globally, organizations require highly skilled Tier 1 SOC analysts to monitor, identify, and respond to incidents efficiently. This course combines theoretical knowledge with hands-on exercises, enabling participants to interpret security logs, detect anomalies, manage alerts, and escalate incidents to Tier 2 and Tier 3 teams. Learners also explore best practices in documentation, reporting, and communication within SOC frameworks, ensuring operational efficiency, regulatory compliance, and proactive threat management.

Course Objectives

1. Understand the role and responsibilities of a Tier 1 SOC analyst in a cybersecurity framework.
2. Develop skills to monitor and analyze security alerts and events using SIEM tools.
3. Recognize common attack vectors, malware behavior, and intrusion techniques.
4. Perform effective log analysis across network, system, and application layers.
5. Triage and escalate security incidents based on severity and impact.
6. Apply threat intelligence to identify potential risks proactively.
7. Document and report security incidents following best practices.
8. Understand SOC workflow processes, standard operating procedures, and escalation paths.
9. Analyze alerts for false positives and refine detection rules.
10. Apply basic digital forensics principles during incident investigation.
11. Maintain operational readiness through continuous monitoring and performance evaluation.
12. Collaborate effectively with Tier 2/3 analysts and other IT teams.
13. Ensure compliance with internal security policies and external regulatory requirements.

Organizational Benefits

- Strengthened early threat detection and rapid incident response
- Improved operational efficiency within the SOC
- Reduced business risk from cyber attacks and security breaches
- Increased accuracy in identifying genuine security incidents
- Better collaboration between SOC tiers and IT teams
- Enhanced regulatory compliance and audit readiness
- Consistent incident documentation and reporting practices
- Optimized use of SIEM and other security monitoring tools
- Improved staff competency and readiness for evolving threats
- Stronger organizational cybersecurity posture and resilience

Target Audiences

- Junior SOC analysts and entry-level cybersecurity professionals
- IT security officers and network administrators
- Security monitoring staff in enterprises and service providers
- Cybersecurity interns and students seeking SOC roles
- IT support and operations staff with cybersecurity responsibilities
- Threat intelligence and incident response teams
- Compliance and risk management personnel
- Consultants and trainers in cybersecurity operations

Course Duration: 5 days

Course Modules

Module 1: Introduction to SOC Operations

- Overview of Security Operations Centers and analyst roles
- Key functions of a Tier 1 SOC analyst
- SOC workflow, processes, and communication channels
- Overview of SIEM tools and monitoring platforms
- Understanding threat landscapes and attack surfaces
- Case Study: SOC setup and workflow at a multinational enterprise

Module 2: Log Analysis and Monitoring

- Fundamentals of log collection and correlation
- Network, server, and application log analysis
- Identifying anomalies and suspicious activities
- Filtering and prioritizing alerts
- Understanding baseline behavior for effective monitoring
- Case Study: Detecting unauthorized access through log analysis

Module 3: Security Alerts Triage

- Classification of security alerts by severity
- Differentiating between false positives and real threats
- Escalation procedures to Tier 2 and Tier 3 analysts
- Tracking incident life cycles and maintaining incident tickets
- Communication protocols during alert triage
- Case Study: Handling multiple concurrent security alerts

Module 4: Threat Intelligence Basics

- Introduction to threat intelligence concepts and sources
- Identifying emerging threats and attack patterns
- Using indicators of compromise (IoCs) in SOC operations
- Applying threat intelligence to enhance detection
- Correlating threat feeds with SIEM alerts
- Case Study: Using threat intelligence to prevent a phishing campaign

Module 5: Malware and Intrusion Awareness

- Overview of malware types and behaviors
- Recognizing signs of system compromise
- Understanding intrusion detection and prevention systems (IDS/IPS)
- Malware containment and initial response procedures
- Using SIEM to detect malware activity
- Case Study: Investigation of a ransomware attack incident

Module 6: Incident Documentation & Reporting

- Proper documentation of security incidents
- Incident reporting templates and standard practices
- Communicating findings to management and stakeholders
- Recording mitigation actions and resolutions
- Maintaining evidence integrity for audits or investigations

- Case Study: Documentation and reporting of a detected insider threat

Module 7: Digital Forensics Fundamentals

- Basics of digital forensics in SOC environments
- Collecting and preserving digital evidence
- Understanding file systems, memory, and network captures
- Preliminary analysis for Tier 1 investigators
- Reporting findings for escalation or further investigation
- Case Study: Forensic investigation of compromised user credentials

Module 8: SOC Best Practices & Operational Efficiency

- Standard operating procedures for effective SOC operations
- Performance metrics and KPIs for Tier 1 analysts
- Team collaboration and knowledge sharing techniques
- Maintaining continuous monitoring and readiness
- Optimizing SIEM and security tools for efficiency
- Case Study: Improving SOC efficiency through workflow optimization

Training Methodology

- Instructor-led presentations and demonstrations
- Hands-on exercises in SIEM platforms and log monitoring
- Scenario-based simulations of security incidents
- Group discussions and peer-to-peer problem solving
- Case study analysis with real-world examples
- Continuous feedback and practical evaluation exercises

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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