Training Course on Building a Security Incident and Event Management (SIEM) Strategy

Professional Development Training Course Outline

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

Course Introduction

In today's digital-first world, cybersecurity threats are evolving at an alarming rate, making it crucial for organizations to adopt a proactive and intelligent approach to security operations. A Security Incident and Event Management (SIEM) strategy is a vital pillar of any modern cybersecurity infrastructure. It combines real-time monitoring, advanced threat detection, automated responses, and centralized log management to identify and mitigate potential security threats before they cause damage.

Training Course on Building a Security Incident and Event Management (SIEM) Strategy is designed to empower IT professionals, SOC analysts, and cybersecurity leaders with the knowledge and hands-on skills required to build, implement, and optimize a robust SIEM strategy. With deep insights into real-world SIEM architectures, log correlation, threat intelligence integration, and incident triaging, participants will gain practical experience that aligns with today's cybersecurity standards and compliance requirements. Whether you're deploying SIEM for the first time or optimizing existing systems, this course ensures you're equipped for modern-day challenges.

Programme Curriculum

Training Course on Building a Security Incident and Event Management (SIEM) Strategy

Introduction

In today's digital-first world, cybersecurity threats are evolving at an alarming rate, making it crucial for organizations to adopt a proactive and intelligent approach to security operations. A Security Incident and Event Management (SIEM) strategy is a vital pillar of any modern cybersecurity infrastructure. It combines real-time monitoring, advanced threat detection, automated responses, and centralized log management to identify and mitigate potential security threats before they cause damage.

Training Course on Building a Security Incident and Event Management (SIEM) Strategy is designed to empower IT professionals, SOC analysts, and cybersecurity leaders with the knowledge and hands-on skills required to build, implement, and optimize a robust SIEM strategy. With deep insights into real-world SIEM architectures, log correlation, threat intelligence integration, and incident triaging, participants will gain practical experience that aligns with today's cybersecurity standards and compliance requirements. Whether you're deploying SIEM for the first time or optimizing existing systems, this course ensures you're equipped for modern-day challenges.

Course Objectives

1. Understand SIEM architecture and its role in modern cybersecurity operations
2. Learn to collect and normalize log data from multiple sources
3. Implement real-time threat detection using rule-based and ML-driven correlation
4. Explore cloud-based SIEM tools and hybrid deployment models
5. Integrate threat intelligence feeds with SIEM platforms
6. Design incident response workflows within SIEM environments
7. Build dashboards and visualizations for security monitoring
8. Apply compliance frameworks (e.g., GDPR, HIPAA, ISO 27001) using SIEM tools
9. Conduct root cause analysis and post-incident reviews
10. Automate alerting and ticketing systems for efficient response
11. Develop SIEM optimization strategies for performance and scalability
12. Evaluate and compare leading SIEM solutions (Splunk, QRadar, LogRhythm, Sentinel)
13. Use MITRE ATT&CK framework for mapping SIEM detection rules

Target Audience

1. Security Operations Center (SOC) Analysts
2. IT Security Managers
3. System Administrators
4. Network Engineers
5. Incident Response Teams
6. Compliance Officers
7. Cloud Security Engineers
8. Penetration Testers and Ethical Hackers

Course Duration: 5 days

Course Modules

Module 1: Introduction to SIEM and Cybersecurity Landscape

- Understanding the cybersecurity threat landscape
- Evolution and importance of SIEM in modern IT environments
- Core components of a SIEM system
- Key SIEM features and functionalities
- Benefits of SIEM for enterprise security
- **Case Study:** Implementation of SIEM in a healthcare organization for HIPAA compliance

Module 2: Log Collection, Normalization & Parsing

- Identifying critical log sources (firewalls, servers, endpoints)
- Log normalization standards and parsing rules
- Using syslog, agents, and APIs for log collection
- Time synchronization and log integrity
- Parsing log data for correlation readiness

- **Case Study:** Centralized log collection in a retail environment to detect card-skimming

Module 3: Threat Detection and Rule Correlation

- Types of correlation rules (rule-based, behavior-based, ML-driven)
- Customizing detection use cases
- Signature-based vs anomaly-based detection
- Building efficient and low-noise detection rules
- Use of MITRE ATT&CK for correlation
- **Case Study:** Detecting insider threats using behavioral analytics in a financial institution

Module 4: Incident Response and Automation

- Incident triage and escalation processes
- Automated alerting, ticketing, and containment
- Integration with SOAR platforms
- Playbooks for repeatable response actions
- Best practices for reducing mean time to respond (MTTR)
- **Case Study:** Automated ransomware response with integrated SOAR in an enterprise network

Module 5: SIEM in the Cloud and Hybrid Environments

- Comparing on-premise vs cloud SIEM solutions
- Challenges in cloud log visibility and management
- Cloud-native SIEM tools (e.g., Azure Sentinel, AWS CloudTrail)
- Multi-cloud and hybrid deployment considerations
- Cloud compliance and security frameworks
- **Case Study:** Migrating to Azure Sentinel for a distributed logistics company

Module 6: Threat Intelligence Integration

- Understanding threat feeds (STIX, TAXII, OpenIOC)
- Incorporating threat intelligence into SIEM
- Use of commercial vs open-source threat intelligence
- Enriching alerts with threat context
- Mapping indicators of compromise (IOCs) to detection rules
- **Case Study:** Preventing phishing campaigns using TI feeds in an educational institution

Module 7: Compliance, Auditing & Reporting

- Mapping SIEM outputs to compliance mandates (e.g., PCI-DSS, GDPR)
- Creating audit-ready reports and dashboards
- Log retention policies and legal considerations
- Alerting on non-compliant activity
- Role of SIEM in audit investigations
- **Case Study:** Achieving GDPR audit success using SIEM in an e-commerce company

Module 8: SIEM Optimization, Maintenance & Evaluation

- Regular tuning and suppression of false positives
- Performance benchmarking of SIEM tools
- Data ingestion vs storage costs management
- Evaluating and comparing SIEM vendors
- Future-proofing SIEM with modularity and integration
- **Case Study:** Optimizing Splunk Enterprise SIEM in a manufacturing enterprise

Training Methodology

- Interactive lectures with industry-relevant content
- Real-world lab simulations using tools like Splunk, QRadar, and Sentinel
- Group activities and guided workshops for skill-building
- Live case study walkthroughs with SME facilitation
- Post-module assessments and project-based evaluations

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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