Security Information and Event Management (SIEM) Administration 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 Information and Event Management (SIEM) Administration Training Course is designed to provide IT security professionals with the knowledge, skills, and best practices needed to effectively deploy, manage, and optimize SIEM systems. Participants will learn how to collect, correlate, and analyze security event data from multiple sources to identify potential threats, detect anomalies, and respond to incidents proactively. The course emphasizes the integration of SIEM with broader cybersecurity strategies, focusing on improving threat intelligence, compliance, and overall organizational resilience.

Through hands-on exercises, real-world examples, and scenario-based learning, participants will understand how to configure alerts, create dashboards, generate reports, and fine-tune detection rules for various IT environments. The course also addresses log management, regulatory compliance, incident response, and the role of automation in enhancing operational efficiency. By the end of the training, learners will be capable of administering SIEM solutions that strengthen network security, reduce risk, and improve situational awareness across the organization.

Programme Curriculum

Security Information and Event Management (SIEM) Administration Training Course

Introduction

Security Information and Event Management (SIEM) Administration Training Course is designed to provide IT security professionals with the knowledge, skills, and best practices needed to effectively deploy, manage, and optimize SIEM systems. Participants will learn how to collect, correlate, and analyze security event data from multiple sources to identify potential threats, detect anomalies, and respond to incidents proactively. The course emphasizes the integration of SIEM with broader cybersecurity strategies, focusing on improving threat intelligence, compliance, and overall organizational resilience.

Through hands-on exercises, real-world examples, and scenario-based learning, participants will understand how to configure alerts, create dashboards, generate reports, and fine-tune detection rules for various IT environments. The course also addresses log management, regulatory compliance, incident response, and the role of automation in enhancing operational efficiency. By the end of the training, learners will be capable of administering SIEM solutions that strengthen network security, reduce risk, and improve situational awareness across the organization.

Course Objectives

1. Understand the core principles and architecture of SIEM systems.
2. Implement log collection and normalization from diverse IT and network sources.
3. Configure correlation rules and real-time alerts for threat detection.
4. Develop dashboards, visualizations, and reporting mechanisms.
5. Perform incident detection, analysis, and response using SIEM tools.
6. Integrate threat intelligence feeds to enhance detection accuracy.
7. Apply best practices in log management and data retention policies.
8. Conduct risk assessment and compliance monitoring through SIEM.
9. Troubleshoot and optimize SIEM performance for operational efficiency.
10. Deploy automation and orchestration to streamline security operations.
11. Ensure alignment with cybersecurity frameworks and regulatory requirements.
12. Monitor insider threats and anomalous user behavior using SIEM analytics.
13. Evaluate emerging SIEM technologies and future trends in cybersecurity monitoring.

Organizational Benefits

- Enhanced threat detection and response capabilities
- Improved visibility of security events across the IT environment
- Reduced risk of data breaches and cyber incidents
- Strengthened compliance with industry and regulatory standards
- Efficient monitoring of network, endpoints, and applications
- Optimized operational performance of SIEM systems
- Better incident management and faster mitigation of threats
- Integration of threat intelligence for proactive security measures
- Reduced downtime and operational disruption from security incidents
- Improved reporting and executive-level visibility on security posture

Target Audiences

- IT security administrators and analysts
- Network and systems engineers
- SOC (Security Operations Center) personnel
- IT compliance and risk management professionals
- Incident response teams
- IT auditors and cybersecurity consultants
- IT managers and infrastructure teams
- Students and professionals aspiring to specialize in SIEM administration

Course Duration: 5 days

Course Modules

Module 1: Introduction to SIEM

- Overview of SIEM systems and architecture
- Benefits of SIEM in modern IT environments
- Key components and deployment models
- Use cases and operational challenges
- Aligning SIEM with cybersecurity frameworks
- Case Study: Successful SIEM deployment in a financial institution

Module 2: Log Collection & Normalization

- Configuring log sources from servers, applications, and network devices
- Log parsing and normalization techniques
- Importance of accurate time synchronization
- Ensuring data integrity and completeness
- Troubleshooting common log collection issues
- Case Study: Addressing log discrepancies during SIEM implementation

Module 3: Correlation Rules & Alerts

- Designing effective correlation rules for threat detection
- Setting alert thresholds and priorities
- Reducing false positives in SIEM alerts
- Leveraging use-case based rule development
- Continuous tuning of rules for operational effectiveness
- Case Study: Identifying ransomware activity using correlation rules

Module 4: Dashboards, Visualization & Reporting

- Creating dashboards for SOC visibility
- Key metrics and KPIs for SIEM monitoring
- Designing reports for technical teams and executives
- Customizing visualizations for rapid incident assessment
- Automated report generation and scheduling
- Case Study: Building a SOC dashboard to monitor critical assets

Module 5: Incident Detection & Response

- Real-time incident identification and prioritization
- Analyzing SIEM alerts and event patterns
- Integrating SIEM with incident response workflows
- Escalation procedures for security incidents
- Documentation and post-incident analysis
- Case Study: Response to a simulated phishing attack using SIEM

Module 6: Threat Intelligence Integration

- Sourcing and integrating external threat intelligence feeds
- Using threat data to enhance correlation rules
- Tracking emerging threats and vulnerabilities
- Aligning threat intelligence with organizational risk profile
- Continuous improvement of detection capabilities

- Case Study: Leveraging threat feeds to detect advanced persistent threats

Module 7: SIEM Optimization & Troubleshooting

- Performance monitoring and system health checks
- Common SIEM issues and resolution techniques
- Storage management and data retention optimization
- Continuous tuning for efficiency and accuracy
- Conducting system audits and compliance checks
- Case Study: Troubleshooting high-volume alert scenarios

Module 8: Automation & Orchestration in SIEM

- Introduction to security automation and SOAR integration
- Streamlining repetitive monitoring tasks
- Automated response workflows and playbooks
- Reducing manual intervention while maintaining control
- Evaluating automation tools for SIEM integration
- Case Study: Automating phishing response with SIEM orchestration

Training Methodology

- Instructor-led lectures with real-world examples
- Hands-on exercises on SIEM configuration, monitoring, and incident response
- Group discussions and problem-solving workshops
- Scenario-based exercises simulating attacks and threats
- Case study analysis to reinforce best practices
- Practical exercises with templates, dashboards, and alert tuning

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