QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1985

Security Information & Event Management (SIEM) Training Course

SECURITY OPERATIONS & INCIDENT RESPONSE
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Security Information & Event Management (SIEM) Training Course provides a comprehensive practical framework for understanding, implementing, operating, and optimizing security information and event management capabilities within modern cybersecurity environments. The program focuses on how organizations can centralize security data, correlate events, identify suspicious activity, investigate threats, and support timely security response.

Participants will explore the core architecture and operating principles of SIEM solutions, including log collection, data ingestion, normalization, parsing, correlation, indexing, alert generation, dashboards, reporting, and security monitoring. The course emphasizes the importance of selecting appropriate data sources and establishing reliable visibility across networks, endpoints, applications, identities, cloud environments, and critical infrastructure.

The program develops practical capabilities in SIEM-based threat detection and investigation. Participants will learn how to build security use cases, develop correlation rules, analyze alerts, investigate event sequences, identify indicators of compromise, reduce false positives, and use contextual information to distinguish genuine threats from normal operational activity.

The course also addresses SIEM governance, operational performance, threat intelligence integration, incident response, compliance reporting, and continuous optimization. Through hands-on exercises, log analysis, detection scenarios, investigation cases, and simulated security operations, participants will develop the skills required to maximize the value of SIEM capabilities and strengthen organizational security monitoring and response.

Objectives

- By the end of the course, participants will be able to:
- Explain the architecture, components, and operating principles of SIEM solutions.
- Assess organizational requirements for centralized security event management.
- Identify and prioritize appropriate log and event data sources.
- Design effective SIEM data collection and ingestion processes.
- Apply techniques for log normalization, parsing, indexing, and enrichment.

- Develop security monitoring and detection use cases.
- Create correlation rules for identifying suspicious activity.
- Analyze SIEM alerts and prioritize them according to risk and severity.
- Investigate security events and reconstruct potential attack timelines.
- Integrate threat intelligence into SIEM monitoring and detection.
- Reduce false positives and improve alert quality.
- Strengthen SIEM integration with incident response processes.
- Develop security dashboards and management reports.
- Evaluate SIEM performance, data quality, and detection coverage.
- Establish effective SIEM governance and operational procedures.
- Develop a roadmap for continuous SIEM optimization and maturity improvement.

Who Should Attend

This course is designed for cybersecurity professionals, security operations analysts, SIEM administrators, security monitoring specialists, incident response professionals, threat detection analysts, security engineers, and information security professionals responsible for monitoring and analyzing security events.

It is also suitable for cybersecurity managers, security operations center leaders, IT administrators, network and systems professionals, threat intelligence specialists, vulnerability management professionals, risk and compliance teams, internal auditors, and technology leaders responsible for overseeing security monitoring and reporting.

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 strengthen centralized security monitoring, threat detection, incident investigation, and cybersecurity governance.

Learning Outcomes

- Upon completion of the course, participants will be able to:
- Describe the functional architecture of a SIEM environment.
- Determine which organizational data sources should be integrated into a SIEM.
- Configure and evaluate security log collection requirements.
- Assess the quality, completeness, and reliability of collected security data.
- Apply appropriate approaches to data parsing, normalization, and enrichment.
- Develop SIEM use cases aligned with organizational threats and risks.
- Create and refine correlation logic for security event detection.
- Analyze alerts and determine appropriate investigation priorities.
- Correlate events from multiple sources to identify potential attack patterns.
- Reconstruct security incidents using SIEM event data and timelines.
- Apply threat intelligence to improve detection and investigation.
- Identify and reduce false positives without weakening meaningful detection.
- Develop operational dashboards and security monitoring reports.
- Measure SIEM performance and detection coverage using relevant indicators.
- Integrate SIEM workflows with incident response and escalation processes.
- Develop a practical roadmap for improving SIEM effectiveness and maturity.

Course Outline

DAY 01

SIEM Fundamentals, Architecture and Security Data

- Introduction to security information and event management.
- The role of SIEM within modern cybersecurity operations.
- SIEM architecture and core components.
- Security event collection and data ingestion.
- Log sources and security telemetry.
- Network, endpoint, application, identity, and cloud data.
- Log collection methods and data pipelines.

DAY 01 — CONTINUED

- Data parsing and normalization.
- Indexing, storage, retention, and search.
- Data quality and completeness.
- Security visibility and monitoring requirements.
- SIEM deployment and operational considerations.

PRACTICAL APPLICATION

Design a high-level SIEM architecture for a selected organization and identify the priority systems and data sources that should be integrated.

DAY 02

SIEM Configuration, Correlation and Detection Use Cases

- SIEM data onboarding and source management.
- Developing effective security monitoring requirements.
- Security detection use cases.
- Correlation concepts and event relationships.
- Rule logic and detection conditions.
- Authentication and access monitoring.
- Endpoint and malware detection.
- Network security event monitoring.
- Suspicious user behavior detection.
- Privilege escalation and account compromise scenarios.
- Data access and exfiltration indicators.
- Threat-based SIEM use-case development.
- Testing and refining detection rules.

PRACTICAL APPLICATION

Develop a set of SIEM detection use cases and correlation rules for selected cybersecurity scenarios.

DAY 03

Alert Analysis, Threat Detection and Investigation

- SIEM alert generation and management.
- Alert classification and severity.
- Security alert triage and prioritization.
- Distinguishing legitimate activity from suspicious behavior.
- False positives and false negatives.
- Event correlation and contextual analysis.
- Building security event timelines.
- Investigating compromised accounts.
- Investigating malware and endpoint activity.
- Investigating suspicious network behavior.
- Identifying indicators of compromise.
- Documenting investigation findings.
- Escalating confirmed security incidents.

> **PRACTICAL APPLICATION**
>
> Investigate a simulated security incident using SIEM events from multiple sources and reconstruct the attack sequence.

DAY 04

Threat Intelligence, Incident Response and SIEM Operations

- Integrating threat intelligence with SIEM.
- Indicators of compromise and threat context.
- Enriching security events with external and internal intelligence.
- Connecting SIEM with incident response workflows.
- Alert escalation and case management.
- Coordinating SIEM analysts with incident response teams.
- Supporting containment and response activities.
- SIEM dashboards and operational visibility.

DAY 04 — CONTINUED

- Executive and management security reporting.
- Compliance and audit reporting.
- SIEM access control and operational governance.
- Managing SIEM performance and operational challenges.

PRACTICAL APPLICATION

Build an integrated SIEM response workflow connecting threat intelligence, alert investigation, escalation, incident response, reporting, and management notification.

DAY 05

SIEM Optimization, Performance and Continuous Improvement

- Measuring SIEM effectiveness and operational performance.
- Detection coverage and use-case effectiveness.
- Data quality and source reliability.
- Alert volume and analyst workload.
- Reducing unnecessary alerts and improving detection efficiency.
- Monitoring investigation and response performance.
- SIEM governance and accountability.
- Reviewing detection gaps against evolving threats.
- Maintaining and updating SIEM use cases.
- Continuous tuning and optimization.
- SIEM maturity assessment.
- Developing a strategic SIEM improvement roadmap.

FINAL WORKSHOP

Develop an integrated SIEM operating framework for a selected organization covering architecture, data sources, onboarding, detection use cases, correlation, alert management, investigation, threat intelligence, incident response, reporting, governance, performance measurement, and continuous optimization.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/security-information-event-management-siem-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440