QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1984

Security Monitoring, Detection & Response Training Course

SECURITY OPERATIONS & INCIDENT RESPONSE
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Security Monitoring, Detection & Response Training Course provides a practical framework for monitoring digital environments, identifying suspicious activity, detecting cybersecurity threats, and coordinating effective security responses. The program is designed to strengthen organizational capabilities for maintaining continuous visibility across networks, endpoints, identities, applications, cloud environments, and critical systems.

Participants will examine the security monitoring lifecycle, including log collection, event analysis, alert management, threat detection, incident triage, investigation, escalation, and response. The course emphasizes the ability to distinguish genuine security threats from normal operational activity and prioritize alerts according to severity, business impact, and potential risk.

The program also focuses on developing effective detection capabilities through security events, indicators of compromise, behavioral patterns, threat intelligence, detection rules, and correlation techniques. Participants will explore the role of centralized security monitoring platforms and security information and event management capabilities in bringing together data from multiple sources to support timely analysis and informed decision-making.

Through practical scenarios, log analysis exercises, alert investigations, detection use cases, and simulated response activities, participants will develop the ability to move from initial security signals to structured investigation and response. The course also addresses monitoring performance, detection gaps, false positives, response coordination, and continuous improvement to support a more mature and resilient cybersecurity operation.

Objectives

- By the end of the course, participants will be able to:
- Explain the principles and objectives of cybersecurity monitoring, detection, and response.
- Assess security visibility across networks, endpoints, identities, applications, and cloud environments.
- Identify relevant security events and indicators of suspicious activity.
- Analyze security logs and alerts to determine potential threats.
- Apply structured approaches to alert triage and prioritization.

- Develop effective security detection use cases and monitoring scenarios.
- Apply event correlation techniques to identify patterns of malicious activity.
- Distinguish between false positives, benign activity, and genuine security threats.
- Investigate suspicious events and establish appropriate escalation paths.
- Integrate threat intelligence into security monitoring and detection processes.
- Strengthen coordination between monitoring, incident response, IT, and risk teams.
- Evaluate detection coverage and identify monitoring gaps.
- Improve alert quality and reduce unnecessary security notifications.
- Establish meaningful metrics for monitoring and detection performance.
- Develop practical procedures for continuous monitoring improvement.
- Strengthen organizational readiness to detect and respond to emerging cyber threats.

Who Should Attend

This course is designed for cybersecurity professionals, security operations specialists, security monitoring analysts, security analysts, incident response professionals, threat detection specialists, security engineers, and IT professionals responsible for monitoring organizational technology environments.

It is also suitable for cybersecurity managers, information security managers, threat intelligence professionals, vulnerability management specialists, network and systems administrators, cloud security professionals, risk and compliance teams, and technology leaders who need to understand or oversee security monitoring and detection capabilities.

The program is particularly relevant to government entities, ministries, banks and financial institutions, oil and gas organizations, telecommunications companies, critical infrastructure operators, technology companies, multinational corporations, and large enterprises seeking to strengthen security visibility, threat detection, monitoring effectiveness, and operational cybersecurity resilience.

Learning Outcomes

- Upon completion of the course, participants will be able to:
- Establish a structured approach to security monitoring across critical technology environments.
- Identify the most relevant data sources for cybersecurity monitoring.
- Interpret security logs and events to identify suspicious behavior.
- Triage and prioritize security alerts according to risk and business impact.
- Investigate potential security incidents using structured analytical methods.
- Develop detection scenarios based on organizational threats and risks.
- Correlate events from multiple systems to identify attack patterns.
- Recognize indicators of compromise and suspicious behavioral activity.
- Distinguish malicious activity from legitimate or expected system behavior.
- Integrate threat intelligence into monitoring and detection activities.
- Identify weaknesses in existing detection coverage and monitoring processes.
- Improve alert accuracy and reduce excessive false positives.
- Establish escalation and handoff procedures between security teams.
- Measure monitoring and detection performance using relevant indicators.
- Develop recommendations for strengthening security monitoring capabilities.
- Create a practical roadmap for improving detection and response maturity.

Course Outline

DAY 01

Foundations of Security Monitoring and Threat Visibility

- Principles of cybersecurity monitoring.
- The role of monitoring in organizational security.
- Security visibility and its relationship to risk management.
- Networks, endpoints, identities, applications, and cloud environments.
- Security logs, events, and telemetry.
- Sources of security monitoring data.
- Log collection and normalization.

DAY 01 — CONTINUED

- Understanding normal versus abnormal activity.
- Security event classification and prioritization.
- Monitoring critical assets and high-risk environments.
- Common monitoring challenges and visibility gaps.
- Establishing a security monitoring framework.

PRACTICAL APPLICATION

Map the critical assets and security data sources of a selected organization and identify priority monitoring requirements.

DAY 02

Security Detection, Alerting and Analysis

- Principles of cybersecurity threat detection.
- Detection methods and security indicators.
- Indicators of compromise and indicators of suspicious behavior.
- Detection rules and monitoring scenarios.
- Event correlation and contextual analysis.
- Behavioral and anomaly-based detection.
- Alert generation and classification.
- Alert severity and prioritization.
- Managing false positives and false negatives.
- Detection coverage and monitoring gaps.
- Developing effective detection use cases.
- Improving the quality and relevance of security alerts.

PRACTICAL APPLICATION

Analyze a series of security alerts, classify their severity, identify potential threats, and determine appropriate investigation priorities.

DAY 03

Security Information, Event Analysis and Investigation

- Centralized security monitoring concepts.
- Security information and event management capabilities.
- Integrating logs from multiple technology sources.
- Searching and analyzing security events.
- Building event timelines.
- Investigating suspicious authentication activity.
- Detecting endpoint and network anomalies.
- Investigating malicious or unusual user behavior.
- Correlating events across systems.
- Identifying attack patterns and indicators.
- Documenting investigation findings.
- Escalation from detection to incident response.

> **PRACTICAL APPLICATION**
>
> Conduct a simulated security investigation using multiple event sources to reconstruct an attack sequence and determine the appropriate escalation path.

DAY 04

Detection Engineering, Threat Intelligence and Response Coordination

- Building threat-driven detection strategies.
- Using threat intelligence to improve detection.
- Mapping threats, techniques, and attack behaviors.
- Developing and maintaining detection use cases.
- Prioritizing detection based on organizational risk.
- Coordinating monitoring and incident response teams.
- Alert escalation and incident handoff.
- Response actions following confirmed detection.

DAY 04 — CONTINUED

- Monitoring emerging and evolving threats.
- Testing detection effectiveness.
- Managing detection changes and operational requirements.
- Continuous improvement of detection capabilities.

PRACTICAL APPLICATION

Develop a threat-driven detection use case, including data sources, detection logic, alert criteria, investigation steps, escalation requirements, and response actions.

DAY 05

Security Operations Performance and Continuous Improvement

- Measuring security monitoring effectiveness.
- Key performance and operational indicators.
- Alert volumes, response times, and investigation quality.
- Detection coverage and control effectiveness.
- Measuring false-positive rates and alert efficiency.
- Identifying recurring monitoring weaknesses.
- Security monitoring governance and accountability.
- Reporting security monitoring results to management.
- Improving operational workflows and team coordination.
- Reviewing detection capabilities against changing threats.
- Building a continuous improvement process.
- Developing a security monitoring maturity roadmap.

FINAL WORKSHOP

Develop an integrated Security Monitoring, Detection & Response framework for a selected organization, covering monitoring sources, detection use cases, alert prioritization, investigation, threat intelligence, escalation, response coordination, performance measurement, governance, and continuous improvement.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/security-monitoring-detection-response-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440