QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1986

Cybersecurity Incident Response & Management Training Course

SECURITY OPERATIONS & INCIDENT RESPONSE
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Cybersecurity Incident Response & Management Training Course provides a practical and structured framework for identifying, analyzing, containing, managing, and recovering from cybersecurity incidents. The program focuses on developing the organizational capabilities required to respond to security incidents efficiently while minimizing operational disruption, financial exposure, data loss, and reputational impact.

Participants will examine the complete incident response lifecycle, beginning with preparation and incident identification and progressing through triage, analysis, containment, eradication, recovery, and post-incident review. The course emphasizes structured decision-making, clear responsibilities, effective escalation, evidence handling, incident documentation, and coordination between technical teams and business stakeholders.

The program also addresses the management dimension of cybersecurity incidents, including incident classification, severity assessment, response priorities, communication, crisis escalation, business continuity, regulatory considerations, and executive involvement. Participants will learn how to coordinate cybersecurity, IT, risk, compliance, legal, communications, and management functions during complex incidents.

Through realistic scenarios, investigation exercises, incident simulations, and practical response planning, participants will develop the ability to manage incidents from initial detection through resolution and lessons learned. The course also emphasizes continuous improvement, helping organizations strengthen incident response procedures, identify recurring weaknesses, improve readiness, and build greater cyber resilience.

Objectives

- By the end of the course, participants will be able to:
- Explain the principles, phases, and objectives of cybersecurity incident response.
- Establish effective incident response processes aligned with organizational risks.
- Identify and classify cybersecurity incidents according to severity and impact.
- Apply structured techniques for incident triage and initial assessment.
- Analyze security incidents and determine appropriate response priorities.

- Coordinate containment, eradication, and recovery activities.
- Establish clear roles, responsibilities, and escalation procedures.
- Apply appropriate practices for evidence preservation and incident documentation.
- Manage communication between technical teams and business stakeholders.
- Assess operational, financial, regulatory, and reputational impacts of cybersecurity incidents.
- Coordinate incident response with business continuity and disaster recovery.
- Manage high-impact incidents requiring executive and crisis-level intervention.
- Evaluate incident response effectiveness through exercises and post-incident reviews.
- Identify root causes and recurring weaknesses following security incidents.
- Develop corrective and preventive actions to reduce future incident risks.
- Strengthen organizational incident response maturity and cyber resilience.

Who Should Attend

This course is designed for cybersecurity managers, incident response professionals, security analysts, security operations specialists, information security professionals, threat detection specialists, security engineers, and IT professionals responsible for identifying or responding to cybersecurity incidents.

It is also suitable for risk and compliance professionals, business continuity specialists, internal control teams, legal and privacy professionals, crisis management teams, technology managers, communications professionals, and executives who participate in cybersecurity incident management or organizational crisis response.

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 cybersecurity incident management and organizational resilience.

Learning Outcomes

- Upon completion of the course, participants will be able to:
- Assess an organization's readiness to manage cybersecurity incidents.
- Establish structured processes for incident identification, assessment, and escalation.
- Classify incidents based on severity, business impact, and urgency.
- Conduct initial incident triage and determine appropriate response actions.
- Analyze technical and contextual information to understand incident scope.
- Develop incident timelines and document key response decisions.
- Coordinate containment and eradication activities across relevant teams.
- Support secure recovery and restoration of affected systems and services.
- Preserve relevant evidence and maintain accurate incident records.
- Communicate incident status effectively to technical, operational, and executive stakeholders.
- Assess business, regulatory, financial, and reputational consequences.
- Coordinate cybersecurity response with continuity and recovery requirements.
- Manage complex incidents involving multiple teams and competing priorities.
- Conduct post-incident reviews and identify improvement opportunities.
- Develop corrective actions based on root causes and lessons learned.
- Create an actionable roadmap for improving incident response capability.

Course Outline

DAY 01

Foundations of Cybersecurity Incident Response

- Principles and objectives of incident response.
- Cybersecurity incidents and common attack scenarios.
- The incident response lifecycle.
- Incident preparedness and organizational readiness.
- Incident identification and initial reporting.
- Incident classification and severity levels.
- Assessing scope, impact, and urgency.

DAY 01 — CONTINUED

- Incident response roles and responsibilities.
- Security operations and incident response coordination.
- Escalation criteria and response priorities.
- Incident response policies and procedures.
- Integration with organizational risk management.

> **PRACTICAL APPLICATION**
>
> Assess a series of cybersecurity scenarios, classify the incidents, determine their severity, and establish appropriate escalation priorities.

DAY 02

Incident Triage, Analysis and Investigation

- Initial incident assessment and triage.
- Collecting and validating incident information.
- Establishing incident timelines.
- Analyzing security alerts and available evidence.
- Identifying indicators of compromise.
- Determining incident scope and affected assets.
- Investigating compromised accounts and credentials.
- Analyzing endpoint, network, and application activity.
- Evidence preservation and documentation.
- Developing investigation hypotheses.
- Coordinating technical investigation activities.
- Determining when an event becomes a confirmed incident.

> **PRACTICAL APPLICATION**
>
> Investigate a simulated cybersecurity incident, establish its timeline, identify affected assets, analyze available evidence, and determine the required response.

DAY 03

Containment, Eradication and Recovery

- Principles of incident containment.
- Short-term and long-term containment strategies.
- Isolating affected systems and accounts.
- Managing compromised credentials and access.
- Removing malicious components and persistence mechanisms.
- Addressing vulnerabilities and root causes.
- Secure system restoration.
- Recovery validation and monitoring.
- Coordinating technical and business recovery.
- Managing dependencies and critical services.
- Returning systems to normal operations.
- Post-recovery security verification.

> **PRACTICAL APPLICATION**
>
> Develop and execute a response plan for a simulated compromise, covering containment, eradication, recovery, validation, and restoration of business services.

DAY 04

Incident Management, Communication and Cyber Crisis Response

- Managing cybersecurity incidents at the organizational level.
- Incident management structures and responsibilities.
- Coordination between cybersecurity, IT, risk, legal, compliance, and communications.
- Executive escalation and decision-making.
- Business impact assessment.
- Protecting critical business services.
- Internal and external incident communications.
- Stakeholder and customer communication considerations.

DAY 04 — CONTINUED

- Regulatory and privacy considerations.
- Managing reputational and operational risks.
- Crisis escalation and executive briefings.
- Maintaining decision and incident management records.

PRACTICAL APPLICATION

Conduct a cyber incident management simulation involving operational disruption, sensitive information exposure, executive escalation, stakeholder communication, and competing response priorities.

DAY 05

Post-Incident Management, Exercises and Continuous Improvement

- Post-incident review principles.
- Root cause analysis and lessons learned.
- Evaluating incident response performance.
- Identifying gaps in people, processes, technology, and governance.
- Corrective and preventive actions.
- Updating incident response policies and procedures.
- Testing incident response capabilities.
- Designing tabletop and simulation exercises.
- Measuring response readiness and maturity.
- Incident response performance indicators.
- Building a continuous improvement framework.
- Developing a cybersecurity incident response maturity roadmap.

FINAL WORKSHOP

Conduct an end-to-end cybersecurity incident response simulation from initial detection and triage through investigation, containment, eradication, recovery, executive communication, and post-incident review, followed by the development of a prioritized incident response improvement roadmap.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/cybersecurity-incident-response-management-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440