MERCURY

Cyber Incident Management

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Cyber Incident Management

Introduction

Cyber Incident Management is a structured discipline focused on detecting, analyzing, responding to, and recovering from cybersecurity incidents across digital environments. It equips professionals to handle threats such as data breaches, malware attacks, and unauthorized access. The course builds a strong foundation in modern cybersecurity incident response practices aligned with global security standards. Participants will understand how security incidents impact business continuity and organizational resilience. The program emphasizes both proactive and reactive strategies for managing cyber risks effectively. It prepares learners to coordinate across technical and operational teams during cyber crises.

Targeted Groups

This Cyber Incident Management training targets professionals seeking knowledge and skills:

- SOC analysts handle daily security alerts.
- IT administrators managing enterprise systems.
- Cybersecurity officers in organizations.
- Network engineers securing infrastructure.
- Risk and compliance professionals.
- Incident response team members.
- Digital forensics beginners.
- Security consultants and auditors.

Course Objectives

Participants will achieve the following objectives by completing the Cyber Incident Management course:

- Develop a clear understanding of cyber incident management frameworks and response methodologies.
- Identify and classify cybersecurity incidents across different environments.
- Apply threat detection and response techniques in line with modern SOC practices.
- Build structured incident response plans for organizational resilience.
- Manage escalation procedures during active security breaches.
- Analyze malware, ransomware, and advanced persistent threats.
- Coordinate communication during cyber crisis management scenarios.
- Strengthen decision-making under pressure in real-time incidents.
- Enhance recovery strategies to efficiently restore systems and services.
- Improve overall cybersecurity posture through continuous learning and incident feedback loops.

Targeted Competencies

Participants will gain the following competencies during the Cyber Incident Management program:

- Incident detection and triage skills in SOC environments.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

- Ability to analyze cyber threats and attack patterns.
- Competence in executing cybersecurity incident handling procedures.
- Skills in digital forensics and log analysis.
- Capability to manage ransomware response scenarios.
- Understanding of cyber crisis coordination and communication.
- Proficiency in incident escalation and reporting workflows.
- Ability to implement structured response playbooks.
- Strong awareness of threat containment and system recovery techniques.

Studying Scenarios

In this Cyber Incident Management training, participants develop skills through the following scenarios:

- Handling simulated data breach incidents in enterprise systems.
- Responding to ransomware attacks affecting critical infrastructure.
- Investigating unauthorized access within corporate networks.
- Managing SOC alert escalation and threat validation cases.
- Coordinating recovery after large-scale service disruption events.

Course Content

Unit 1: Foundations of Cyber Incident Management

- Introduction to cyber incident management principles.
- Types of cybersecurity incidents and classifications.
- Overview of incident response lifecycle stages.
- Understanding threat detection and response basics.
- Role of SOC in incident handling operations.
- Security incident response plan structure.
- Importance of cybersecurity governance and policies.

Unit 2: Threat Detection and SOC Operations

- Security Operations Center SOC structure and roles.
- Real-time threat monitoring techniques.
- Log analysis and security event correlation.
- Alert triage and prioritization methods.
- Use of SIEM tools in incident detection.
- Indicators of compromise identification techniques.
- Early warning systems for cyber threats.

Unit 3: Incident Response Lifecycle and Execution

- Incident identification and classification steps.
- Containment strategies for active cyber threats.
- Eradication techniques for malicious activity.
- System recovery and restoration processes.
- Evidence preservation during incidents.
- Incident escalation and decision workflows.
- Post-incident review and reporting practices.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Unit 4: Digital Forensics and Malware Response

- Fundamentals of digital forensics in cyber incidents.
- Evidence collection and chain-of-custody handling.
- Malware behavior analysis techniques.
- Ransomware attack patterns and response.
- Memory and disk forensics fundamentals.
- Network forensics in breach investigations.
- Advanced persistent threat APT tracking.

Unit 5: Cyber Crisis Management and Governance

- Cyber crisis management frameworks and planning.
- Communication strategies during security breaches.
- Stakeholder coordination in cyber emergencies.
- Legal and regulatory incident reporting requirements.
- Business continuity and disaster recovery alignment.
- Risk management in cyber incident environments.
- Continuous improvement from incident lessons learned.

Final Insights & Key Takeaways

Cyber Incident Management strengthens organizational resilience by enabling structured detection and response to evolving cyber threats. Mastery of incident response processes ensures faster recovery, reduced impact, and a stronger cybersecurity posture.