Security Incident Management & Investigation

SEC020

Course Description

This course provides professionals with the knowledge and skills required to manage and investigate security incidents effectively. It covers the entire lifecycle of security incidents, from identification and response to investigation and resolution. Participants will learn how to apply best practices in incident detection, manage incident response teams, conduct thorough investigations, and ensure compliance with legal and regulatory requirements. The course also focuses on improving the overall security posture by learning from past incidents and implementing corrective measures.

Course Objectives

By the end of this course, participants will be able to:

- Understand the principles of security incident management and the key phases involved.
- Detect and classify security incidents accurately, determining the appropriate response.
- Lead or participate in the incident response process, including containment, eradication, and recovery.
- Conduct effective security incident investigations, including gathering and preserving evidence.
- Develop and implement strategies for preventing future incidents based on lessons learned.
- Ensure compliance with legal, regulatory, and organizational requirements during investigations.
- Communicate effectively with stakeholders and report incident findings and actions.

Who Should Attend

- Security professionals, incident response teams, and IT personnel responsible for handling security incidents.
- Investigators, compliance officers, and risk managers involved in security event analysis.
- Managers and directors overseeing security operations and response planning.
- Anyone seeking to improve their ability to manage, respond to, and investigate security incidents.

Course Duration

5 Working Days

Course Outlines

1. Introduction to Security Incident Management
    - Overview of security incident management and its importance in maintaining security.
    - Key phases of incident management: detection, response, investigation, and resolution.
    - Types of security incidents: cyber-attacks, data breaches, physical security events, and insider threats.
2. Incident Detection and Classification
    - Techniques for detecting security incidents: monitoring, alerts, and threat intelligence.
    - Classifying incidents: severity levels, impact assessment, and escalation protocols.
    - Tools and technologies used in incident detection and classification.
3. Incident Response Planning and Execution
    - Developing an incident response plan: roles, responsibilities, and procedures.
    - Incident containment, eradication, and recovery methods.
    - Communicating with stakeholders and managing internal and external notifications.
    - Coordinating with law enforcement and regulatory bodies when necessary.
4. Evidence Gathering and Preservation
    - Best practices for collecting and preserving evidence during a security incident.
    - Chain of custody and legal considerations in handling evidence.
    - Techniques for forensic analysis and documenting findings for legal purposes.
5. Investigation Techniques and Methodology
    - Steps in conducting a thorough security incident investigation.
    - Analyzing logs, network traffic, and system data to determine the cause and impact.
    - Interviewing suspects and witnesses as part of the investigation process.
    - Identifying the root cause of incidents and how to trace back to the origin.
6. Legal, Regulatory, and Compliance Considerations
    - Understanding legal obligations during security incident management and investigation.
    - Compliance with data protection laws (e.g., GDPR, HIPAA) and industry regulations.
    - Reporting requirements and documentation during investigations.
    - The role of incident management in compliance and risk mitigation.

7. Post-Incident Analysis and Reporting
    - Documenting the incident timeline, actions taken, and outcomes.
    - Conducting a post-mortem analysis to identify weaknesses and lessons learned.
    - Creating detailed incident reports for internal stakeholders, clients, and regulators.
    - Developing and implementing corrective actions to prevent future incidents.
8. Improving Security Posture through Incident Feedback
    - Using incident data to refine security policies and response strategies.
    - Strengthening incident response capabilities through continuous improvement.
    - Training teams and preparing for future incidents using lessons learned.
    - Leveraging threat intelligence and vulnerability assessments to improve security.