CIH: Certified Incident Handler

Course ID #: 1275-245-ZZ-W

Hours: 21

Course Content

Course Description:

In this course, you will cover the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and various laws and policy related to incident handling.

Course Objectives:

Upon successful completion of this course, students will be able to:

- Create incident handling and response policies.
- Deal with various types of computer security
- Be proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats.

Prerequisites:

In order to increase your chances of success, it is recommended that you have at least 1 year of experience in the cybersecurity domain.

Target Audience:

- Penetration Testers
- Vulnerability Assessment Auditors
- Risk Assessment Administrators
- Network Administrators
- Application Security Engineers
- Cyber Forensic Investigators/ Analyst and SOC Analyst
- System Administrators/Engineers
- Firewall Administrators and Network Managers/IT Managers
- Mid-level to High-level Cybersecurity Professionals

CIH: Certified Incident Handler

Course ID #: 1275-245-ZZ-W

Hours: 21

Topics:

Module 01: Introduction to Incident Handling and Response

Lesson 1: Overview of Information Security Concepts

- Elements of Information Security
- Information as Business Asset
- Securing Information: Defense-in-Depth
- Information Security Policies
  - Types of Security Policies
  - Examples of Security Policies

Lesson 2: Understanding Information Security Threats and Attack Vectors

- Motives, Goals, and Objectives of Information Security Attacks
- Top Information Security Attack Vectors
- Information Security Threat Categories
- Threat and Threat Actors
  - Types of Threat Actors
- Impact of Information Security Attacks
- Information Warfare

Lesson 3: Understanding Information Security Incident

- Information Security Incidents
- Signs of an Incident
- Cost of an Incident

Lesson 4: Overview of Incident Management

- Incident Management
- Incident Handling and Response
- Advantages of Incident Handling and Response

Lesson 5: Overview of Vulnerability Management

- What Is Vulnerability?
- Common Areas of Vulnerabilities
- Vulnerability Research
- Vulnerability Classification
- Vulnerability Assessment
- Types of Vulnerability Assessment
- Vulnerability Management Life Cycle
  - Pre-Assessment Phase: Creating a Baseline
  - Vulnerability Assessment Phase
  - Post-Assessment Phase

Lesson 6: Overview of Threat Assessment

- What Is Threat Assessment?
- Threat Targets and Assets
- Common Targeted Assets
- Threat Intelligence
- Threat Contextualization
- Threat Correlation
- Threat Attribution

Lesson 7: Understanding Risk Management

- What Is Risk?
- Risk Management
- Risk Assessment Process
  - Step 1: System Characterization
  - Step 2: Threat Identification
  - Step 3: Vulnerability Identification
  - Step 4: Control Analysis
  - Step 5: Likelihood Analysis
  - Step 6: Impact Analysis
  - Step 7: Risk Determination
    - Risk Levels
    - Risk Matrix
  - Step 8: Control Recommendation
  - Step 9: Risk Assessment Report
- Risk Mitigation
- Control the Risks
- Risk Management Plan Evaluation and Update
- NIST Risk Management Framework
- Risk Assessment and Management Tools

Lesson 8: Understanding Incident Response Automation and Orchestration

- Incident Response Automation
- Incident Response Orchestration
- Working of Incident Response Orchestration
- Advantages of Incident Response Orchestration

Lesson 9: Incident Handling and Response Best Practices

- OWASP
- ENISA
- GPG18 and Forensic readiness planning (SPF)

Lesson 10: Overview of Standards

- ISO/IEC 27000 Series
- ISO/IEC 27001:2013
- ISO/IEC 27002
- ISO/IEC 27035
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Information Processing Standards (FIPS) 200
- NIST Special Publication 800 Series
- Standard of Good Practice from Information Security Forum (ISF)
- NERC 1300 Cyber Security
- RFC 2196

Lesson 11: Overview of Cybersecurity Frameworks

- CIS Critical Security Controls
- COBIT Framework
- NIST Special Publication 800-61

Lesson 12: Importance of Laws in Incident Handling ▪Role of Laws in Incident Handling

- Legal and Jurisdictional Issues when Dealing with an Incident

Lesson 13: Incident Handling and Legal Compliance

- Sarbanes–Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- Gramm–Leach–Bliley Act (GLBA)
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- The Digital Millennium Copyright Act (DMCA)
- Cyber Laws that May Influence Incident Handling

Module 02: Incident Handling and Response Process

Lesson 1: Overview of Incident Handling and Response (IH&R) Process

- Introduction to Incident Handling and Response (IH&R) Process
- Importance of IH&R Process
- Overview of IH&R Process Flow

Lesson 2: Step 1 - Preparation for Incident Handling and Response

- Process Flow of Preparation for IH&R
- Determine the Need for IH&R Processes
- Define IH&R Vision and Mission
- Management Approvals and Funding
- Develop IH&R Plan
- Develop IH&R Policy
- Develop IH&R Procedures
- Define Incident Handling Criteria
- Build IH&R Team
  - Roles and Responsibilities of IH&R Team
  - IH&R Team Placement in an Organization
  - IH&R Team Models and Staffing
  - IH&R Team Selection Factors
  - Training and Preparing IH&R Personnel
- Develop Incident Readiness Procedures
  - Build Incident Response Toolkit
  - Incident Responder Toolkit Requirements
  - Setting Up a Computer Forensics Lab
  - Establish Reporting Facilities
  - Establish Structured Record Keeping Facilities
- Evaluate the Current Security Posture
  - Implement Security Policy, Procedures, and Awareness
  - Implement Security Control
  - Implement Successful Backup Strategy
  - Cyber Insurance
  - Implementing Security Policies using GPMC

Lesson 2: Step 2 - Incident Recording and Assignment

- Process Flow of Incident Recording and Assignment
- Define Incident Escalation Procedures for Employees
  - Role of IT Support and Help Desk
  - Ticketing System

Lesson 3: Step 3 - Incident Triage

- Process Flow of Incident Triage
- Incident Analysis and Validation
- Incident Classification
- Incident Prioritization
  - Incident Prioritization Approaches
  - Incident Prioritization Categories
  - Best Practices
- Tools for Incident Analysis and Validation

Lesson 4: Step4 - Notification

- Process Flow of Notification
- Point of Contact
- Details to Notify
- Internal Communication Methods
- Incident Notification Form

Lesson 5: Step 5 - Containment

- Process Flow of Incident Containment
- Incident Containment
- Guidelines for Incident Containment

Lesson 6: Step 6 - Evidence Gathering and Forensics Analysis

- Process Flow of Evidence Gathering and Forensics Analysis
- Evidence Gathering and Forensics Analysis
- Evidence Handling

Lesson 7: Step 7 - Eradication

- Process Flow of Eradication
- Eradication
- Tools for Detecting Missing Security Patches

Lesson 8: Step 8 - Recovery

- Process Flow of Recovery
- Systems Recovery

Lesson 9: Step 9 - Post-Incident Activities

- Process Flow of Post-Incident Activities
- Incident Documentation
- Report Writing Tools
- Incident Impact Assessment
- Review and Revise Policies
- Close the Investigation
- Incident Disclosure
  - Incident Disclosure Procedure

Module 3: Forensic Readiness and First Response

Lesson 1: Introduction to Computer Forensics

- Computer Forensics
- Role of Computer Forensics in Incident Handling
- Phases Involved in the Computer Forensics Investigation Process
  - Pre-investigation Phase
  - Investigation Phase
  - Post-investigation Phase

Lesson 2: Overview of Forensic Readiness

- Forensic Readiness
- Forensic Readiness and Business Continuity
- Forensic Readiness Planning
- Forensic Readiness Procedures
  - Forensic Policy
  - Forensics in the Information System Life Cycle
  - Creating Investigation Team
  - Maintaining an Inventory
  - Host Monitoring
  - Network Monitoring

Lesson 3: Overview of First Response

- First Responder
- Roles of First Responder
- First Response Basics
- Incident Response: Different Situations
- First Responder Common Mistakes
- Health and Safety Issues
- Securing the Crime Scene
- Collecting Incident Information
- Documenting the Electronic Crime Scene

Lesson 4: Overview of Digital Evidence

- Digital Evidence
- Types of Digital Evidence
- Characteristics of Digital Evidence
- Roles of Digital Evidence
- Types of Evidence

Lesson 5: Understanding the Principles of Digital Evidence Collection

- ACPO Principles of Digital Evidence
- Scientific Working Group on Digital Evidence (SWGDE)

Lesson 6: Collecting the Evidence

- Collecting and Preserving Evidence
- Collecting Physical Evidence
- Dealing with Powered On Computers
- Dealing with Powered Off Computers
- Dealing with Networked Computers
- Dealing with Open Files and Startup Files
- Operating System Shutdown Procedure
- Collecting Evidence from Social Networks

Lesson 7: Securing the Evidence

- Evidence Management
- Chain of Custody
  - Simple Format of the Chain of Custody Document
  - Chain of Custody Form
- Evidence Bag Contents List
- Packaging, Transporting, and Storing Electronic Evidence

Lesson 8: Overview of Data Acquisition

- Data Acquisition
- Duplicate the Data (Imaging)
- Data Imaging Tools
- Verify Image Integrity

Lesson 9: Understanding the Volatile Evidence Collection

- Why Volatile Data Important?
- Order of Volatility
- Volatile Data Collection Methodology
- Collecting Volatile Information
  - System Information
  - Current System Date and Time/Command History
  - Current System Uptime
  - Running Processes
  - Open Files, Clipboard Data, Service/Driver Information
  - Logged-On Users
  - DLLs or Shared Libraries
  - Network Information
  - Network Connections
- Tools for Collecting Volatile Evidence

Lesson 10: Understanding the Static Evidence Collection

- Static Data Acquisition
- Static Data Collection Process
- Tools for Collecting Static Evidence

Lesson 11: Performing Evidence Analysis

- Evidence Analysis: Preparations
- Forensic Analysis Tools
  - Forensic Explorer
  - Forensic Toolkit (FTK)
  - Event Log Explorer
  - OSForensics
  - Helix3
  - Autopsy
  - EnCase Forensics
  - Foremost
- Forensics Reports

Lesson 12: Overview of Anti-Forensics

- What is Anti-Forensics?
- Anti-Forensics Techniques
  - Golden ticket
  - Data/File Deletion
  - Password Protection
  - Steganography
  - Program Packers
  - Virtual Machine
  - Artifact Wiping
  - Memory Residents
  - Alternate Data Stream (ADS)
- Other Anti-Forensics Techniques
  - Data Hiding in File System Structures
  - Trail Obfuscation
  - Overwriting Data/Metadata
  - Encryption
  - Encrypted Network Protocols
  - Rootkits
  - Buffer Overflow against Forensic Tools
  - Detecting Forensics Tool Activities

Module 04: Handling and Responding to Malware Incidents

Lesson 1: Overview of Malware Incident Response

- Introduction to Malware
- Components of Malware
- Methods of Malware Propagation
- Common Techniques Attackers Use to Distribute Malware on the Web
- Need for Malware Incident Response
- Case Study

Lesson 2: Preparation for Handling Malware Incidents

- Preparing Malware Incident Response Team
- Importance of Safely Handling Malware
- Preparing Malware Testbed
- Malware Analysis Tools

Lesson 3: Detecting Malware Incidents

- Indications of Malware Incidents
- Malware Detection Techniques
  - Live System/Dynamic Analysis
    - Port Monitoring
    - Process Monitoring
    - Registry Monitoring
    - Windows Service Monitoring
    - Startup Programs Monitoring
    - Event Logs Monitoring
    - Installation Monitoring
    - Files and Folders Monitoring
    - Device Drivers Monitoring
    - Network Traffic Monitoring
    - DNS Monitoring/Resolution
    - API Calls Monitoring
    - Scheduled Task Monitoring
    - Browser Activity Monitoring
  - Memory Dump/Static Analysis
    - File Fingerprinting
    - Local and Online Malware Scanning
    - Performing String Search
    - Identifying Packing/ Obfuscations Methods
    - Finding the Portable Executables (PE) Information
    - Identifying File Dependencies
    - Malware Disassembly
    - Memory Dump Analysis using Volatility Framework
  - Intrusion Analysis
    - Detecting Malware by its Covert Storage/Hiding Techniques
    - Detecting Malware by its Covert Communication Techniques

Lesson 4: Containment of Malware Incidents

Lesson 5: Eradication of Malware Incidents

- Antivirus Tools

Lesson 6: Recovery after Malware Incidents

Lesson 7: Guidelines for Preventing Malware Incidents

Module 05: Handling and Responding to Email Security Incidents

Lesson 1: Overview of Email Security Incidents

- Introduction to Email Security Incidents
- Types of Email Security Incidents
  - Crimes Committed by Sending Emails
    - Spamming
    - Phishing
      - Examples of Phishing Emails
      - Types of Phishing
    - Mail Bombing
    - Mail Storming
    - Malware Distribution
  - Crimes Supported by Emails
    - Identity Theft
      - Types of Identity Theft
      - Common Techniques Attackers Use to Perform Identity Theft
    - Cyberstalking
    - Child Pornography
    - Child Abduction

Lesson 2: Preparation for Handling Email Security Incidents

- Preparation

Lesson 3: Detection and Containment of Email Security Incidents

- Indications of Email Attack
- Indications of Identity Theft
- Detecting Phishing/Spam Mails
  - Tools for Detecting Phishing/Spam Mails
- Containing Emails Incidents
- Analyzing Email Headers
  - Example of Email Header Analysis
  - Sender Policy Framework (SPF)
  - Domain Keys Identified Mail (DKIM)
  - Steps to Analyze Email in Gmail
  - Steps to Analyze Email in Yahoo Mail
  - Tools for Analyzing Email Headers
- Checking the Email Validity
- Examining the Originating IP Address
- Tracing the Email Origin
- Tracing Back Web-based Email
- Email Tracking Tools
- Analyzing Email Logs
- Analyzing SMTP Logs

Lesson 4: Eradication of Email Security Incidents

- Eradicating Email Attacks
- Reporting Phishing and Spam Email to Email Service Provider
- Guidelines against Spam
- Guidelines against Phishing
- Guidelines against Identity Theft Recovery after Email Security Incidents
- Recovery Steps to Follow after Email Incidents
- Recovery of Deleted Emails
- Email Recovery Tool: Recover My Email
- Anti-phishing Tool: Gophish
- Anti-spamming Tool: SPAMfighter
- Email Security Checklist
- Email Security Tools

Module 06: Handling and Responding to Network Security Incidents

Lesson 1: Overview of Network Security Incidents

- Introduction to Network Security Incidents
- Common Network Security Incidents
- Need for Network Security Incident Handling and Response

Lesson 2: Preparation for Handling Network Security Incidents

- Preparation Steps for Handling Network Security Incidents
- Preparation of Network Security Incident Handling Toolkit
  - Windows-based Tools to Analyze Incidents
  - Linux-based Tools to Analyze Incidents
  - Vulnerability Analysis Tools to Analyze Incidents

Lesson 3: Detection and Validation of Network Security Incidents

- General Indications of Network Security Incidents
- Detection and Validation of Suspicious Network Events
- Tools for Detection and Validation of Suspicious Network Events

Lesson 4: Handling Unauthorized Access Incidents

- Introduction to Unauthorized Access Incidents
- Indications of Unauthorized Access Incidents
- Detecting Reconnaissance Attacks
  - PING Sweep Attempts
  - Port Scanning Attempts
    - Half Open/Stealth Scan Attempts
    - Full Connect Scan Attempt
    - Null Scan Attempts
    - Xmas Scan Attempts
  - Detecting Social Engineering Attempts
- Detecting Sniffing and Spoofing Attacks
  - Mac Flooding Attempts
  - ARP Poisoning Attempts
  - Other Sniffing Detection Techniques
- Detecting Firewall and IDS Evasion Attempts
  - General Indications of Intrusions
  - Intrusion Detection Using Snort
  - Reviewing Firewalls/IDS Logs
- Detecting Brute Forcing Attempts
- Containment of Unauthorized Access Incidents
- Eradication of Unauthorized Access Incidents
  - Physical Security Measures
  - Authentication and Authorization Measures
  - Host Security Measures
  - Network Security Measures
- Recovery after Unauthorized Access Incidents

Lesson 5: Handling Inappropriate Usage Incidents

- Introduction to Inappropriate Usage Incidents
- Indications of Inappropriate Usage Incidents
  - Detecting Inappropriate Usage Incidents
  - Detecting High Resource Utilization
  - Accessing Malware in the Network
  - Reviewing Log Entries of Application Logins
  - Analyzing Network Security Device Logs
- Containment of Inappropriate Usage Incidents
- Eradication of Inappropriate Usage Incident
- Recovery after Inappropriate Usage Incident

Lesson 6: Handling Denial-of-Service Incidents

- Introduction to Denial-of-Service Incidents
- Introduction to Distributed Denial-of-Service Incidents
- Types of DoS/DDoS Incidents
  - Volumetric Attacks
  - Protocol Attacks
  - Application Layer Attacks
  - Permanent Denial-of-Service Attack
  - Distributed Reflection Denial of Service (DRDoS)
- DoS/DDoS Attack Tools
- Indications of DoS/DDoS Incidents
- Detecting DoS/DDoS Incidents
  - Activity Profiling
  - Sequential Change-point Detection
  - Wavelet-based Signal Analysis
  - Detection by Analyzing Network Connections
  - Detection by Analyzing Non-Responding Applications
  - Other Detection Techniques
  - Tools for Detecting DoS/DDoS Incidents
- Containment of DoS/DDoS Incidents
- Post-Attack Forensics
- Eradicating DoS/DDoS Incidents
  - Blocking Potential Attacks
  - Disabling Botnets
  - Neutralizing Handlers
- Recovery after DoS/DDoS Incidents
- DoS/DDoS Recommendations
  - Protect Secondary Victims
  - Enable DoS/DDoS Protection at ISP Level
- DoS/DDoS Protection Tools

Lesson 7: Handling Wireless Network Security Incidents

- Introduction to Wireless Network Security Incidents
- Types of Wireless Network Security Incidents
  - Access Control Attacks
  - Integrity Attacks
  - Confidentiality Attacks
  - Availability Attacks
  - Authentication Attacks
- Preparation for Handling Wireless Network Security Incidents
- Indications of Wireless Network Security Incidents
- Detecting Wireless Network Security Incidents
- Containment of Wireless Network Security Incidents
- Eradication of Wireless Network Security Incidents
- Recovery after Wireless Network Security Incidents

Module 07: Handling and Responding to Web Application Security Incidents

Lesson 1: Overview of Web Application Incident Handling

- Introduction to Web Applications
- Web Application Architecture
- Introduction to Web Application Incident Handling

Lesson 2: Web Application Security Threats and Attacks

- OWASP Top 10 Application Security Risks – 2017
  - A1 -Injection Flaws
    - SQL Injection Attacks
    - Command Injection Attacks
    - File Injection Attack
    - LDAP Injection Attacks
  - A2 -Broken Authentication
  - A3 -Sensitive Data Exposure
  - A4 -XML External Entity (XXE)
  - A5 -Broken Access Control
  - A6 -Security Misconfiguration
  - A7 -Cross-Site Scripting (XSS) Attacks
  - A8 -Insecure Deserialization
  - A9 -Using Components with Known Vulnerabilities
  - A10 -Insufficient Logging and Monitoring
- Other Web Application Threats
  - Directory Traversal
  - Unvalidated Redirects and Forwards
  - Watering Hole Attack
  - Cross-Site Request Forgery (CSRF) Attack
  - Cookie/Session Poisoning
  - Web Services Foot printing Attack
  - XML Poisoning Attack
  - Hidden Field Manipulation Attack
  - Attacks Using Single and Double Encoding

Lesson 3: Preparation to Handle Web Application Security Incidents

- Steps to Handle Web Application Security Incidents
- Deploying a WAF
- Deploying SIEM Solutions

Lesson 4: Detecting and Analyzing Web Application Security Incidents

- Indicators of Web Application Security Incidents
- Detecting Web Incidents
  - Automated Detection
  - Manual Detection
    - SQL Injection
    - Using Regex -SQL Injection
    - XSS Attacks
    - Regex -XSS Attacks
    - Directory Traversal Attacks
    - Regex -Directory Traversal Attacks
    - Dictionary Attacks
    - Stored Cross Site Script Attacks
    - DoS/DDoS attacks
    - Potentially Malicious Elements within HTML
    - Malicious Elements in Common Web File Types
    - RFI Attacks
    - LFI Attacks
    - Watering Hole Attacks
- Analyzing Web Server Content
- Log Analysis Tools

Lesson 5: Containment of Web Application Security Incidents

- Containment of Web Application Security Incidents
- Containment Methods
  - Whitelisting/Blacklisting
  - Web Content Filtering
  - Proxy Servers
- Containment Tools
  - Whitelisting/Blacklisting Tools
  - Web Content Filtering Tools
  - Web Proxy Tools

Lesson 6: Eradication of Web Application Security Incidents

- How to Eradicate Web Application Security Incidents
- Eradicating Injection Attacks
- Eradicating Broken Authentication and Session Management Attacks
- Eradicating Sensitive Data Exposure Attacks
- Eradicating XML External Entity Attacks
- Eradicating Broken Access Control Attacks
- Eradicating Security Misconfiguration Attacks
- Eradicating XSS Attacks
- Eradicating Insecure Deserialization Attacks
- Eradicating Attacks due to Known Vulnerabilities in Components
- Eradicating Insufficient Logging & Monitoring Attacks
- Eradicating DoS/DDoS Attacks
- Eradicating Web Services Attacks
- Eradicating CAPTCHA Attacks
- Eradicating other Web Application Attacks
  - Directory Traversal Attacks
  - Unvalidated Redirect and Forward Attacks
  - Watering Hole Attacks
  - Cross-Site Request Forgery Attacks
  - Cookie/Session Poisoning Attacks
- Implement Encoding Schemes
  - Eradicate XSS Attacks using HTML Encoding
  - Eradicate SQL Injection Attacks using Hex Encoding

Lesson 7: Recovery from Web Application Security Incidents

- Recovery from Web Application Incidents
- Tools to Recover from Web Application Incidents

Lesson 8: Best Practices for Securing Web Applications

- Best Web Application Coding Practices
- Web Application Fuzz Testing
- Source Code Review
- Web Application Security Testing Tools

Module 08: Handling and Responding to Cloud Security Incidents

Lesson 1: Cloud Computing Concepts

- Introduction to Cloud Computing
- Types of Cloud Computing Services
- Separation of Responsibilities in Cloud
- Cloud Deployment Models
- NIST Cloud Deployment Reference Architecture

Lesson 2: Overview of Handling Cloud Security Incidents

- Handling Cloud Security Incidents
- Incident Handling Responsibilities in Cloud
- Challenges in Cloud Incident Handling and Response
  - Architecture and Identification
  - Data Collection
  - Logs
  - Analysis
  - Legal
- Challenges in Cloud Forensics
- Organizational Issues in Cloud Incident Handling

Lesson 3: Cloud Security Threats and Attacks

- Cloud Computing Threats
- Cloud Computing Attacks

Lesson 4: Preparation for Handling Cloud Security Incidents

- Preparation Steps to Handle Cloud Security Incidents
  - Preparation Steps for Cloud Service Provider (CSP)
  - Preparation Steps for Cloud Consumer (CC)

Lesson 5: Detecting and Analyzing Cloud Security Incidents

- Indicators of Cloud Security Incidents
- Detecting Cloud Security Incidents
  - Network Related Incidents
  - Storage Related Incidents
  - Servers Related Incidents
  - Virtualization Related Incidents
  - Application Related Incidents
- Evidence Data Concerns
- Cloud-based Log Analysis Tools

Lesson 6: Containment of Cloud Security Incidents

- Containment of Cloud Security Incidents
- Containment Tools for Cloud Security Incidents

Lesson 7: Eradication of Cloud Security Incidents

- Eradicating Cloud Security Incidents
- MITC Attack Detection Tool: Tripwire

Lesson 8: Recovering from Cloud Security Incidents

Lesson 9: Best Practices Against Cloud-based Incidents

- Best Practices Against Cloud Security Incidents
- Cloud Security is the Responsibility of both Cloud Provider and Consumer
- Cloud Security Tools

CIH: Certified Incident Handler

Course ID #: 1275-245-ZZ-W
Hours: 21

Module 09: Handling and Responding to Insider Threats

Lesson 1: Introduction to Insider Threats
- Insider Threats
- Types of Insider Threats
- Driving Force Behind Insider Attacks
- Common Attacks Carried Out by Insiders
- Importance of Handling Insider Attacks
- Case Study

Lesson 2: Preparation for Handling Insider Threats
- Preparation Steps to Handle Insider Threats

Lesson 3: Detecting and Analyzing Insider Threats
- Indicators of Insider Threats
- Detecting Insider Threats
  - Mole Detection
  - Profiling
  - Behavioral Analysis
- Log Analysis
- Network Analysis
  - Detecting Malicious Telnet Connections
  - Detecting Malicious FTP Connections
  - Detecting Data Exfiltration
- System Analysis
  - Look for Removable Media
  - Look for Browser Data
- Database Analysis
  - Examine Microsoft SQL Server Logs
  - Collecting Volatile Database Data
  - Using DBCC LOG Command
- Physical Security Analysis
- Insider Threat Detection Tools

Lesson 4: Containment of Insider Threats

Lesson 5: Eradication of Insider Threats
- Eradicating Insider Threats
  - Human Resources
  - Network Security
  - Access Controls
  - Privileged Users
  - Audit Trails and Log Monitoring
  - Physical Security

Lesson 6: Recovery after Insider Attacks
- Recovering from Insider Attacks

Lesson 7: Best Practices Against Insider Threats
- Best Practices Against Insider Threats
- Insider Threat Prevention Tools