E|CIH
EC-Council Certified Incident Handler

EC-Council
Building A Culture Of Security

EC-Council Certified Incident Handler

COURSE OUTLINE

EC-Council Official Curricula

EC-Council Certified Incident Handler

Course Outline

(Version 3)

Module 01: Introduction to Incident Handling and Response

Understand Information Security Threats and Attack Vectors

- Elements of Information Security
- Motives, Goals, and Objectives of Information Security Attacks
- Threat and Threat Actors
  - Threats Sources
  - Types of Threat Actors
  - Attributes of Threat Actors
- Information Security Attack Vectors
- Classification of Attacks
- Impact of Information Security Attacks
- Vulnerability Classification

Explain Various Attack and Defense Frameworks

- EC-council's Hacking Methodology
  - Footprinting
  - Scanning
  - Enumeration
  - Vulnerability Analysis
  - System Hacking
    - Gaining Access
    - Escalating Privileges

        - Maintaining Access
        - Clearing Logs
    - Cyber Kill Chain Methodology
    - MITRE ATT&CK Framework
    - MITRE D3FEND
    - RE&CT Framework
    - Tactics, Techniques, and Procedures (TTPs)
        - Tactics
        - Techniques
        - Procedures
    - Indicators of Compromise
        - Categories of Indicators of Compromise

Understand Information Security Concepts

- Vulnerability Assessment
- Risk Management
- NIST Risk Management Framework
- Cyber Threat Intelligence
    - Types of Threat Intelligence
- Threat Modeling
    - Threat Modeling Process
- Threat Hunting
    - Threat Hunting Steps

Understand Information Security Incidents

- Information Security Incidents
- Signs of an Incident
    - Sources of Precursors and Indicators
- Cost of an Incident

Understand the Incident Management Process

- Incident Management
- Incident Handling and Response (IH&R)
- Advantages of Incident Handling and Response

- OODA Loops in Incident Response
- Importance of ChatGPT in Incident Response

Understand Incident Response Automation and Orchestration

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

Describe Various Incident Handling and Response Best Practices

- Best Practices
  - OWASP
  - ENISA
  - FTC

Explain Various Standards Related to Incident Handling and Response

- ISO/IEC 27000 Series
- ISO/IEC 27001
- Other ISO Standards
  - ISO/IEC 27002
  - ISO/IEC 27035
  - ISO/IEC 27037
  - ISO/IEC 27041
  - ISO/IEC 27042
  - ISO/IEC 27043
  - ISO/IEC 27050
  - ISO 22320:2018
- FFIEC
- Payment Card Industry Data Security Standard (PCI DSS)
- NERC 1300 Cyber Security
  - NERC 1307: Incident Reporting and Response Planning

Explain Various Cybersecurity Frameworks

- NIST Special Publication 800-61
- ITIL Incident Management

- COBIT Framework
- CIS Critical Security Controls

Understand Incident Handling Laws and Legal Compliance

- Role of Laws in Incident Handling
- Legal and Jurisdictional Issues When Dealing with an Incident
- Sarbanes–Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- Gramm–Leach–Bliley Act (GLBA)
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- The Digital Millennium Copyright Act (DMCA)
- CAN-SPAM Act
- Cyber Laws That May Influence Incident Handling

Module 02: Incident Handling and Response Process

Understand 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
- The Golden Hour of Incident Response

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 an IH&R Plan
- Develop IH&R Policy
- Develop IH&R Procedures
- Build IH&R Team
    - Roles and Responsibilities of an 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 Response Readiness Procedures
  - Role of Computer Forensics in Incident Handling
  - Establish Forensic Readiness
    - Forensic Readiness and Business Continuity
    - Forensic Readiness Planning
    - Forensic Readiness Procedures
      - ✓ Forensic Policy
      - ✓ Forensics in the Information System Life Cycle
      - ✓ Creating an Investigation Team
      - ✓ Maintaining an Inventory
      - ✓ Host Monitoring
      - ✓ Network Monitoring
  - Build Incident Response Toolkit
  - Incident Responder Toolkit Requirements
  - Establish Reporting Facilities
    - Incident Reporting Template
  - Establish Structured Record Keeping Facilities
  - Establish Playbooks and Runbooks for Incident Response
    - Playbooks
    - Runbooks
  - Establish Communication Procedures for Internal Teams and External Groups
    - Develop a Communication Plan
    - Communication with External Reporting Bodies
  - Establish Incident Response Metrics
    - Key Performance Indicators (KPIs)
    - Key Result Indicators (KRIs)
    - Key Control Indicators (KCIs)

- Service Level Agreements (SLAs)

- Evaluate the Current Security Posture
  - Implement Security Policy, Procedures, and Awareness
  - Implement Security Controls
    - Administrative Security Controls
    - Physical Security Controls
    - Technical Security Controls
  - Implement a Robust Backup Strategy
  - Choosing a Good Cyber Insurance Policy
    - Why Do Organizations Need Cyber Insurance?

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
    - SolarWinds Web Help Desk (WHD)
    - AlienVault OSSIM

Step 3: Incident Triage

- Process Flow of Incident Triage
- Incident Analysis and Validation
- Incident Classification
- Incident Prioritization
  - Incident Prioritization Categories
    - Functional Impact of the Incident
    - Information Impact of the Incident
    - Recoverability Effort Categories
- Tools for Incident Triage

Step 4: Notification

- Notification Process Flow
- Point of Contact
- Notification Details

- Internal Communication
  - Considerations for Internal Incident Communication
- External Communication
  - External Bodies to Communicate During an Incident
  - Develop or Prepare for Media Queries
- Incident Notification Form
- Tools for Incident Notification

Step 5: Containment

- Process Flow of Incident Containment
- Incident Containment
  - Criteria for selecting appropriate containment procedure
- Guidelines for Incident Containment

Step 6: Evidence Gathering and Forensic Analysis

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

Step 7: Eradication

- Process Flow of Eradication
- Eradication

Step 8: Recovery

- Recovery Process Flow
- Systems Recovery
  - Determine the Course of Action
  - Monitor and Validate the Systems

Step 9: Post-Incident Activities

- Process Flow of Post-Incident Activities
- Incident Postmortem
- After-Action Report (AAR)
  - Building the Appropriate After-Action Report (AAR)
    - Recap
    - Review

        - Analysis
        - Areas of Improvement
    - Lessons Learned
    - Incident Documentation
        - Concise and Clear
        - Written in a Standard Format
        - Reviewed by Editors
    - Report Writing Tools
    - Incident Impact Assessment
    - Review and Revise Policies
        - Employee Training and Awareness
    - Close the Investigation
    - Incident Disclosure
        - Incident Disclosure Procedure

Information Sharing Activities

- Establish Information Sharing Capabilities
    - Team-to-Team Information Sharing
    - Team-to-Coordinating Team Information Sharing
    - Coordinating Team-to-Coordinating Team Information Sharing
- Information Sharing Techniques
    - Ad hoc
    - Partially automated
    - Security considerations while sharing incident information
- Granular Information Sharing
    - Business Impact Information
    - Technical Information
- NIST Information Sharing Recommendations

Module 03: First Response

Explain the Concept of First Response

- First Response

- First Responder
  - Roles of First Responder
- First Response Basics
- First Response: Different Situations
  - First Response by Non-forensics Staff
  - First Response by System/Network Administrators
  - First Response by Laboratory Forensics Staff
    - Documenting the Electronic Crime Scene
    - Collecting Incident Information
    - Planning the Search and Seizure
    - Identifying and Collecting Electronic Evidence
    - Packaging Electronic Evidence
    - Transporting Electronic Evidence
- First Responder Common Mistakes
- Health and Safety Issues

Understand the Process of Securing and Documenting the Crime Scene

- Documenting the Electronic Crime Scene
  - Photographing and Sketching the Scene
- Planning the Search and Seizure
- Collecting Incident Information
  - Conducting Preliminary Interviews
- Initial Search of the Scene
- Securing and Evaluating the Crime Scene
- Seizing Evidence at the Crime Scene

Understand the Process of Collecting Evidence at the Crime Scene

- Collecting the 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

- Windows OS
- macOS
- UNIX/Linux OS

- Dealing with Smartphones or Other Handheld Devices

Explain the Process for Preserving, Packaging, and Transporting Evidence

- Preserving Evidence
- Chain of Custody
  - Simple Format of the Chain of Custody Document
  - Chain of Custody Form
- Evidence Bag Contents List
- Packaging Evidence
- Exhibit Numbering
- Determining the Location for Evidence Examination
- Transporting and Storing Evidence

Module 04: Handling and Responding to Malware Incidents

Understand the Handling of Malware Incidents

- Introduction to Malware Incident Handling
- Malware Propagation Techniques
- Common Techniques Attackers Use to Distribute Malware on the Web

Explain Preparation for Handling Malware Incidents

- Preparing Malware Incident Response Team
- Importance of Safely Handling Malware
  - Steps to Handle Malware Safely

Understand Detection of Malware Incidents

- Indicators of Malware Incidents
- Indicators of Trojan Incidents
- Indicators of Virus Incidents
- Indicators of Fileless Malware Incidents
- Detecting Malware Intrusion using YARA Rules
- Detecting Fileless Malware Incidents using SentinelOne

- Tools for Detecting Remote Access Trojans (RATs)
- Tools for Detecting Malware in Encrypted Network Traffic
- Tools for Detecting Fileless Malware

Explain Containment of Malware Incidents

- Containment of Malware Incidents
- Tools for Containment of Malware Incidents

Describe How to Perform Malware Analysis

- Preparing Malware Testbed
- Malware Analysis Tools
  - Hardware Tools
  - Software Tools
- Malware Analysis Techniques
  - Live-System/Dynamic Analysis
    - Port Monitoring
    - Process Monitoring
    - Registry Monitoring
    - Windows Services Monitoring
    - Startup Programs Monitoring
    - Event Logs Monitoring/Analysis
    - Installation Monitoring
    - Files and Folders Monitoring
    - Device Drivers Monitoring
    - Network Traffic Monitoring /Analysis
    - DNS Monitoring/Resolution
    - API Calls Monitoring
    - System Calls Monitoring
    - Scheduled Tasks Monitoring
    - Browser Activity Monitoring
    - Identifying Remote Access Trojans (RATs)
    - Analyzing Linux-based Fileless Malware using Command Line Utilities
  - Memory Dump/Static Analysis

- File Fingerprinting
- Local and Online Malware Scanning
- Performing Strings Search
- Identifying Packing/Obfuscation Methods
- Finding the Portable Executables (PE) Information
- Identifying File Dependencies
- Malware Disassembly
- Analyzing ELF Executable Files
- Analyzing Mach Object (Mach-O) Executable Files
  - ✓ Malicious Mach-O Binaries
  - ✓ Reverse Engineering Mach-O Binaries
- Analyzing Malicious MS Office Documents
  - ✓ Finding Suspicious Components
  - ✓ Finding Macro Streams
  - ✓ Dumping Macro Streams
  - ✓ Identifying Suspicious VBA Keywords
- Memory Dump Analysis using Volatility Framework

o Intrusion Analysis

- Detecting Malware via its Covert Storage/Hiding Techniques
- Detecting Malware via its Covert Communication Techniques
- Analyzing Malware Alerts using Microsoft 365 Defender

Understand Eradication of Malware Incidents

- Eradication of Malware Incidents
  - o Eradicating Trojan Incidents
  - o Eradicating Virus and Worm Incidents
  - o Eradicating Ransomware Incidents
- Antivirus Tools
- Anti-Trojan Software

Explain Recovery after Malware Incidents

- Recovery after Malware Incidents
- Tools for Recovery after Malware Incidents

Understand the Handling of Malware Incidents - Case Study

- Handling Prestige Ransomware Incident

Describe Best Practices against Malware Incidents

- Best Practices against Malware Incidents
- Best Practices against Fileless Malware Incidents
- Fileless Malware Protection Tools

Module 05: Handling and Responding to Email Security Incidents

Understand 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 Used by Attackers to Obtain Personal Information for Identity Theft
    - Cyberstalking

Explain Preparation Steps for Handling Email Security Incidents

- Preparation for Handling Email Security Incidents
- Email Filtering Tools
- Email Monitoring Tools
- Email Log Analysis Tools

Understand Detection and Containment of Email Security Incidents

- Indicators of Email Attack
- Indicators of Identity Theft
- Detecting Phishing/Spam Mails
  - Detecting Spear Phishing Attacks
  - Tools for Detecting Spear Phishing Attacks
    - Barracuda Impersonation Protection
- Containment of Email Security Incidents

Understand Analysis of Email Security Incidents

- Analyzing Phishing Emails Using ThePhish
- Tools for Analyzing Phishing/Spam Mails
- 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 Outlook
  - Tools for Analyzing Email Headers
- Checking Email Validity
- Examining Originating IP Address
- Tracing Email Origin
- Tracing Back Web-based Email
- Email Tracking Tools
- Analyzing Email Logs
  - Examining System Logs
  - Examining Network Equipment Logs
  - Examining Microsoft Exchange Email Server Logs
  - Examining Linux Email Server Logs
  - Analyzing Email Logs using EventLog Analyzer
- Analyzing SMTP Logs

Explain Eradication of Email Security Incidents

- Eradicating Email Security Incidents
- Reporting Phishing and Spam Emails to Email Service Providers

Understand the Process of Recovery after Email Security Incidents

- Recovery after Email Security Incident
- Recovery of Deleted Emails
  - Gmail
  - Outlook PST
- Email Recovery Tools

Understand the Handling of Email Security Incidents - Case Study

- Handing DigitalOcean Mailchimp Security Incident

Explain Best Practices against Email Security Incidents

- Email Security Checklist
- Guidelines against Spam Emails
- Guidelines against Phishing Emails
- Guidelines against Identity Theft
- Guidelines against Mail Bombing
- Guidelines against Cyberstalking
- Audit Organization's Security for Phishing Attacks using OhPhish
- Anti-spamming Tools
- Email Security Tools

Module 06: Handling and Responding to Network Security Incidents

Understand the Handling of Network Security Incidents

- Introduction to Handling Network Security Incidents
- Common Network Security Incidents
  - Unauthorized Access Incidents
  - Inappropriate Usage Incidents
  - Denial-of-Service Incidents
  - Wireless Network Incidents

Prepare to Handle Network Security Incidents

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

Understand Detection and Validation of Network Security Incidents

- General Indicators of Network Security Incidents
  - Indicators of Windows-based Network Incidents
  - Indicators of Linux-based Network Incidents
- Detection and Validation of Suspicious Network Events
- Tools for Detecting and Validating Suspicious Network Events
- Detecting and Analyzing Network Security Incidents using Flowmon ADS
- Network Log Analysis Tools

Understand the Handling of Unauthorized Access Incidents

- Indicators of Unauthorized Access Incidents
  - Physical Intrusion
  - Changes in System Configuration
  - Changes in Network
  - Changes in Administrator Settings
  - Unauthorized Data Modification
  - Unauthorized Usage of Standard User Account
  - Unauthorized Data Access
  - High Resource Utilization
- Detecting Reconnaissance Attacks
  - Ping Sweep Attempts
  - Port Scanning Attempts
    - Half Open/Stealth Scan Attempts
    - Full Connect Scan Attempts
    - Null Scan Attempts
    - XMAS Scan Attempts

- Social Engineering Attempts
- Detecting Sniffing and Spoofing Attacks
  - MAC Flooding Attempts
  - ARP Poisoning Attempts
  - Other Sniffing Detection Techniques
    - Check Devices Running in Promiscuous Mode
    - Run IDS
    - Network Tools
    - Ping Method
    - DNS Method
    - ARP Method
    - Using Promiscuous Detection Tools
- Detecting Firewall and IDS Evasion Attempts
  - Intrusion Detection Using Snort
  - Reviewing Firewalls/IDS Logs
- Detecting Brute-force Attempts
- Detecting SMB Attacks against Windows
- Detecting Password Spray Attack 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

Understand the Handling of Inappropriate Usage Incidents

- Indicators of Inappropriate Usage Incidents
  - Indicators of Unauthorized Service Usage
  - Indicators of Access to Inappropriate Materials
  - Indicators of Inappropriate Resource Usage
  - Indicators of Inappropriate System and Network Activities

- Detecting Inappropriate Usage Incidents
  - Detecting High Resource Utilization
  - Accessing Malware in Network
  - Detecting and Analyzing Malware in Network using Splunk Enterprise Security
  - Reviewing Log Entries of Application Logins
  - Analyzing Failed Login Attempts in Windows
  - Analyzing Failed Login Attempts in Linux
  - Analyzing Network Security Device Logs
  - Analyzing Abnormal Activities in Windows-based Systems
    - Unusual User Accounts
    - Unusual Files
    - Unusual Processes and Services
    - Unusual Running Network Services
    - Unusual Network Activity
    - Unusual Automated Tasks
    - Unusual Log Entries
  - Analyzing Abnormal Activities in Linux-based Systems
    - Unusual User Accounts
    - Unusual Files
    - Unusual Running Network Services
    - Unusual Network Activity
    - Unusual Log Entries
    - Unusual Processes
  - Viewing and Analyzing Linux Syslog using Solarwinds Loggly
- Containment of Inappropriate Usage Incidents
- Eradication of Inappropriate Usage Incidents
- Recovery after Inappropriate Usage Incidents

Understand the Handling of Denial-of-Service Incidents

- Indicators of DoS/DDoS Incidents
  - DoS/DDoS Attacks Targeting a Host
  - DoS/DDoS Attacks Targeting Operating Systems

- DoS/DDoS Attacks Targeting Network Services
- DoS/DDoS Attacks Targeting System Applications

- 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
  - Detection by Analyzing Network Traffic using Wireshark
  - Other Detection Techniques
  - Tools for Detecting DoS/DDoS Incidents
- Containment of DoS/DDoS Incidents
  - Absorb Attacks
  - Divert Traffic
  - Degrade Services
  - Block Attacks
  - Shutdown Services
  - Load Balancing
  - Throttling
  - Drop Requests
- Post-attack Forensics
  - Traffic Pattern Analysis
  - Packet Traceback
  - Event Log Analysis
- Eradicating DoS/DDoS Incidents
  - Blocking Potential Attacks
    - Egress Filtering
    - Ingress Filtering
    - TCP Intercept
    - Rate Limiting
  - Disabling Botnets

- RFC 3704 Filtering
- Black-hole Filtering
- DDoS Prevention Offerings from ISP or DDoS Service

o Neutralizing Handlers

- Network Traffic Analysis
- Neutralize Botnet Handlers
- Spoofed Source Address

- Recovery after DoS/DDoS Incidents

Understand the Handling of Wireless Network Security Incidents

- Preparation for Handling Wireless Network Security Incidents
- Indicators of Wireless Network Security Incidents
- Detecting Wireless Network Security Incidents
  - Access Point Monitoring
  - Wireless Client Monitoring
  - General Wireless Traffic Monitoring
- Containment of Wireless Network Security Incidents
- Eradication of Wireless Network Security Incidents
- Recovery after Wireless Network Security Incidents

Understand the Handling of Network Security Incidents - Case Study

- Handling DDoS Attacks on Google Cloud

Describe Best Practices against Network Security Incidents

- Best Practices against Network Security Incidents
- Best Practices against DoS/DDoS Incidents
  - DoS/DDoS Recommendations
    - Protect Secondary Victims
      - ✓ Individual Users
      - ✓ Network Service Providers
- Best Practices against Wireless Network Security Incidents
- Tools for Detecting Missing Security Patches
- DoS/DDoS Protection Tools
- Network Security Tools

Module 07: Handling and Responding to Web Application Security Incidents

Understand the Handling of Web Application Incidents

- Introduction to Web Application Incident Handling
- OWASP Top 10 Application Security Risks – 2021

Explain Preparation for Handling Web Application Security Incidents

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

Understand Detection and Containment of Web Application Security Incidents

- Indicators of Web Application Security Incidents
- Detecting Web Incidents
- Tools for Detecting 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

Explain Analysis of Web Application Security Incidents

- Analyzing Web Incidents
  - Manual Analysis
    - SQL Injection
    - Using Regex - SQL Injection
    - XSS Attacks
    - Using Regex - XSS Attacks
    - Directory Traversal Attacks
    - Using 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
  - ✓ Using URLs Containing IP Addresses
  - ✓ Using PHP Functions
  - ✓ Using URLs with an Appended Question Mark(s)
  - ✓ Using Off-site URLs
- LFI Attacks
- Watering Hole Attacks

- Analyzing Web Server Content
- Log Analysis Tools

Understand Eradication of Web Application Security Incidents

- Eradication of Web Application Security Incidents
- Eradicating Broken Access Control Attacks
- Eradicating Cryptographic Failures/Sensitive Data Exposure Attacks
- Eradicating Injection Attacks
  - SQL Injection Attacks
  - Command Injection Attacks
  - File Injection Attacks
- Eradicating Insecure Design Attacks
- Eradicating Security Misconfiguration Attacks
- Eradicating Attacks due to Vulnerable and Outdated Components
- Eradicating Attacks due to Identification and Authentication Failures
- Eradicating Attacks due to Software and Data Integrity Failures
- Eradicating Attacks due to Security Logging and Monitoring Failures
- Eradicating Server-side Request Forgery Attacks
- Eradicating XSS Attacks
- Eradicating Directory Traversal Attacks
- Eradicating DoS/DDoS Attacks

- Eradicating Watering Hole Attacks
- Implement Encoding Schemes
  - Types of Encoding Schemes
    - URL Encoding
    - HTML Encoding
    - Unicode Encoding
    - Base64 Encoding
    - Hex Encoding
  - Eradicate XSS Attacks using HTML Encoding
  - Eradicate SQL Injection Attacks using Hex Encoding

Explain Recovery after Web Application Security Incidents

- Recovery after Web Application Incidents
- Tools to Recover from Web Application Incidents
  - ApexSQL Log
  - CrowdStrike Falcon™ Orchestrator
  - SysTools SQL Recovery

Understand the Handling of Web Application Security Incidents - Case Study

- Handling GoDaddy Data Breach

Describe Best Practices for Securing Web Applications

- Best Web Application Coding Practices
- Web Application Fuzz Testing
  - Fuzz Testing Steps
  - Fuzz Testing Strategies
  - Fuzz Testing Scenario
  - Fuzz Testing Tools
- Source Code Review
  - Manual Code Review
  - Automated Code Review
- Web Application Security Testing Tools

Module 08: Handling and Responding to Cloud Security Incidents

Understand the Handling of Cloud Security Incidents

- Introduction to Cloud Computing
  - Characteristics of Cloud Computing
  - Limitations of cloud computing
- Separation of Responsibilities in Cloud
- Cloud Service Providers
- OWASP Top 10 Cloud Security Risks
- Handling Cloud Security Incidents
- Incident Handling Responsibilities in Cloud
- Challenges in Cloud Security Incident Handling and Response
  - Architecture and Identification
  - Data Collection
  - Logs
  - Analysis
  - Legal
- Challenges in Cloud Forensics
- Organizational Issues in Cloud Security Incident Handling

Explain Various Steps Involved in Handling Cloud Security Incidents

- Preparation Steps to Handle Cloud Security Incidents
  - Preparation Steps for CSPs
  - Preparation Steps for CCs
- Detecting and Analyzing Cloud Security Incidents
  - Indicators of Cloud Security Incidents
  - Detecting Cloud Security Incidents
    - Network-related Incidents
    - Storage-related Incidents
    - Server-related Incidents
    - Virtualization-related Incidents
    - Application-related Incidents
  - Detecting Cloud Security Incidents using Falco

- Evidence Data Concerns
- Cloud-based Log Analysis Tools
- Tools for Detecting Cloud Security Incidents

- Containment of Cloud Security Incidents
  - Containment Tools for Cloud Security Incidents
- Eradication of Cloud Security Incidents
- Recovery after Cloud Security Incidents

Understand How to Handle Azure Security Incidents

- Preparation Steps to Handle Azure Security Incidents
- Detecting and Analyzing Azure Security Incidents
  - Indicators of Azure Security Incidents
    - Indicators of Windows-based Azure Security Incidents
    - Indicators of Linux-based Azure Security Incidents
    - Indicators of Azure App Service-based Security Incidents
    - Indicators of Azure Container-based Security Incidents
    - Indicators of Azure SQL Database Security Incidents
    - Indicators of Azure Resource Manager Security Incidents
    - Indicators of Azure Storage Security Incidents
  - Detecting and Responding to Security Threats Using Microsoft Azure Sentinel
  - Investigating Incidents using Microsoft Azure Sentinel
  - Analyzing Azure Monitor Logs
  - Detecting Brute-force Attacks using Microsoft Azure Sentinel
  - Managing and Responding to Security Alerts in Microsoft Defender for Cloud
- Containment of Azure Security Incidents
- Eradication of Azure Security Incidents
- Recovery after Azure Security Incidents
- Azure Incident Response Tools
- Azure Security Tools
- Best Practices against Azure Security Incidents

Understand How to Handle AWS Security Incidents

- Preparation Steps to Handle AWS Security Incidents

- Prepare People
- Prepare Technology
- Prepare Processes

- Detecting and Analyzing AWS Security Incidents
  - Indicators of AWS Security Incidents
  - Forensic Disk Collection in AWS
  - Responding to Service and Infrastructure Domain Incidents
    - Service Domain Incidents
    - Infrastructure Domain Incidents
  - Investigating AWS CloudTrail for IAM-based Incidents
    - Using AWS Console
    - Using AWS CLI
  - Investigating Amazon VPC Flow Logs using AWS Management Console
  - Analyzing Amazon CloudWatch Logs
  - Detecting and Analyzing AWS Security Incidents using GuardDuty
  - Automating Incident Response using AWS Systems Manager Incident Manager
- Containment of AWS Security Incidents
  - Basic Containment
  - Security Group Level Containment
  - Subnet and VPC-Level Containment
- Eradication of AWS Security Incidents
- Remediating Security Incidents Discovered by GuardDuty
- Recovery after AWS Security Incidents
  - Backup and Restore
  - Pilot Light
  - Warm Standby
  - Multi-site Active/Active
- Recovery after AWS Security Incidents using CloudEndure Disaster Recovery
- Best Practices against AWS Security Incidents
  - Basic AWS Security Practices
  - AWS Infrastructure Security Practices

- AWS Financial Services Security Practices
- AWS Security Hub Practices
- AWS Security Groups Practices
- AWS Backup Data Practices

- AWS Security Tools

Understand How to Handle Google Cloud Security Incidents

- Preparation Steps to Handle Google Cloud Security Incidents
- Detecting and Analyzing Google Cloud Security Incidents
  - Indicators of Google Cloud Security Incidents
  - Investigating and Responding to Google Cloud Security Incidents
    - Detecting Access Attempts from Anonymous Proxy
    - Detecting BigQuery Data Exfiltration
    - Detecting Brute Force: SSH
    - Detecting Malware
    - Detecting Persistent Anomalous IAM Grants
  - Analyzing Google Workspace Logs using Filters
  - Analyzing Log Data using Google Cloud Log Analytics
  - Detecting and Responding to Container Security Incidents
    - Malicious Script Executed
    - Reverse Shell
  - Detecting and Responding to VM-based Security Incidents
    - Execution: Cryptocurrency Mining Hash Match
    - Execution: Cryptocurrency Mining YARA Rule
- Containment of Google Cloud Security Incidents
  - Containment of Compromised Google Cloud Credentials
- Eradication of Google Cloud Security Incidents
  - Eradicating Google Kubernetes Engine Security Incidents
- Recovery after Google Cloud Security Incidents
- Best Practices against Google Cloud Security Incidents
- Google Cloud Security Tools

Understand the Handling of Cloud Security Incidents - Case Study

- Handling Kaseya VSA Ransomware Security Incident

Explain Best Practices against Cloud Security Incidents

- Best Practices against Cloud Security Incidents
- CSA Best Practices for Cloud Security
- Cloud Security is the Responsibility of Cloud Provider and Consumer
- FedRAMP Compliance and Baseline Security Controls
- Cloud Security Tools

Module 09: Handling and Responding to Insider Threats

Understand the Handling of Insider Threats

- Insider Threats
- Types of Insider Threats
  - Malicious Insider
  - Negligent Insider
  - Professional Insider
  - Compromised Insider
  - Accidental Insider
- Driving Force behind Insider Attacks
- Common Attacks Performed by Insiders
- Importance of Handling Insider Attacks

Explain Preparation Steps for Handling Insider Threats

- Preparation Steps to Handle Insider Threats

Understand Detection and Containment of Insider Threats

- Indicators of Insider Threats
- Detecting Insider Threats
  - Mole Detection
  - Profiling
  - Behavioral Analysis
  - Behavioral Analysis Tools
  - Detecting Insider Threats Using Firewall Analyzer

- Insider Threat Detection Tools
- Containment of Insider Threats

Explain Analysis of Insider Threats

- Log Analysis
- Network Analysis
  - Detecting Malicious Telnet Connections
  - Detecting Malicious FTP Connections
  - Detecting Malicious HTTP Exfiltration
  - Detecting Data Exfiltration
- System Analysis
  - Search for Removable Media
  - Search for Browser Data
- Database Analysis
  - Examine Microsoft SQL Server Logs
  - Collect Volatile Database Data
  - Using DBCC LOG Command
  - Database Analysis Tools
- Physical Security Analysis

Understand Eradication of Insider Threats

- Eradicating Insider Threats
  - Human Resources
  - Network Security
  - Access Controls
  - Privileged Users
  - Audit Trails and Log Monitoring
  - Physical Security

Understand the Process of Recovery after Insider Attacks

- Recovery after Insider Attacks

Understand the Handling of Insider Threats - Case Study

- Case Study 1: Ubiquiti Data Breach
- Case Study 2: Stradis Healthcare Incident

Describe Best Practices against Insider Threats

- Best Practices against Insider Threats
- Insider Threat Prevention Tools

Module 10: Handling and Responding to Endpoint Security Incidents

Understand the Handling of Endpoint Security Incidents

- Introduction to Endpoint Security Incident Handling
  - Need for Endpoint Security Incident Handling
- Common Endpoint Security Incidents
  - Mobile-based Security Incidents
  - IoT-based Security Incidents
  - OT-based Security Incidents

Explain the Handling of Mobile-based Security Incidents

- Introduction to Handling Mobile-based Security Incidents
- OWASP Top 10 Mobile Risks
- Preparation Steps for Handling Mobile-based Security Incidents
  - Preparation of Mobile-based Incident Handling Toolkit
- Detecting Mobile-based Security Incidents
  - Indicators of Mobile-based Incidents
  - Investigating Mobile-based Incidents using Mobile Verification Toolkit (MVT)
  - Capturing and Analyzing Android Network Traffic using Wireshark
  - Capturing and Analyzing iOS Network Traffic using Wireshark
  - Analyzing iOS Network Traffic using Network Analyzer Pro
  - Analyzing Android Logs
  - Android-based Log Analysis Tools
  - iOS-based Log Analysis Tools
- Containment of Mobile-based Security Incidents
- Eradication of Mobile-based Security Incidents
- Recovery after Mobile-based Security Incidents
- Best Practices against Mobile-based Security Incidents
  - Best Practices for Securing Android Devices

- Best Practices for Security iOS Devices
- Android Security Tools
- iOS Security Tools

Explain the Handling of IoT-based Security Incidents

- Introduction to Handling IoT-based Security Incidents
- OWASP Top 10 IoT Threats
- Preparation Steps for Handling IoT-based Security Incidents
  - Preparation of IoT-based Incident Handling Toolkit
- Detecting IoT-based Security Incidents
  - Indicators of IoT-based Incidents
  - Detecting IoT Security Incidents using Microsoft Sentinel
  - Analyzing IoT Network Traffic using Foren6
  - IoT-based Log Analysis Tools
- Containment of IoT-based Security Incidents
- Eradication of IoT-based Security Incidents
- Recovery after IoT-based Security Incidents
- Best Practices against IoT-based Security Incidents
  - Best Practices for IoT Hardware Security
  - IoT Security Tools

Explain the Handling of OT-based Security Incidents

- Introduction to Handling OT-based Security Incidents
- Preparation Steps for Handling OT-based Incidents
  - Preparation of OT-based Incident Handling Toolkit
- Detecting OT-based Security Incidents
  - OT-based Incident Response with MITRE ATT&CK® for ICS
  - Indicators of OT-based Incidents
  - Detecting Network Traffic Anomalies in ICS Networks
  - Passive Discovery and Analysis of OT Networks with LogRhythm
  - Analyzing IIoT Traffic using NetworkMiner
  - Analyzing Modbus/TCP Traffic using Wireshark
  - Acquiring Evidence during OT Incident Response

- OT-based Log Analysis Tools
- Containment of OT-based Security Incidents
- Eradication of OT-based Security Incidents
- Recovery after OT-based Security Incidents
  - Roles Involved in Recovery Task
- Best Practices against OT-based Security Incidents
  - Best Practices for OT Hardware Security
  - OT Security Tools

Understand the Handling of Endpoint Security Incidents - Case Study

- Handling BotenaGo Malware Incident on LILIN Security Camera DVR Devices