6 Days

# ECIH v2 - [EC-Council Certified Incident Handler]

The EC-Council Certified Incident Handler training is a specialist course that exposes students and professionals to the various techniques and policies which can be deployed to combat the emerging computer security incidents. This training and certification program provides a comprehensive curriculum for participants increasing their proficiency to handle malicious code incidents, insider attack threats, and network security incidents.

After completing the training, an individual will be able to create response policies and incident handling techniques to protect the vulnerabilities attacking an information system.

This training will prepare participants for the ECIH 212-89 exam that will be conducted on the last day of training. Passing this exam is crucial to validate one's proven ability in Incident Handling.

## Course Details

## Course Outline

**Module 1: Introduction to Incident Response and Handling**

- Cyber Incident Statistics
- Computer Security Incident
- Types of Computer Security Incidents
- Examples of Computer Security Incidents
- Information as Business Asset
- Data Classification
- Common Terminologies
- Information Warfare
- Key Concepts of Information Security
- Vulnerability, Threat, and Attack
- Incidents That Required the Execution of Disaster Recovery Plans
- Incident Reporting
- Signs of an Incident
- Incident Categories, Prioritization, Response & Handling
- Impact of Virtualization on Incident Response and Handling
- Use of Disaster Recovery Technologies
- Estimating Cost of an Incident
- Key Findings of Symantec Global Disaster Recovery Survey – 2009
- Vulnerability Resources

**Module 2: Risk Assessment**

- Risk Policy & Assessment
- NIST's Risk Assessment Methodology
- Steps to Assess Risks at Work Place

- Cost/Benefit Analysis
- NIST Approach for Control Implementation
- Risk Analysis
- Risk Mitigation
- Residual Risk
- Risk Management Tools

**Module 3: Incident Response and Handling Steps**

- Identifying an Incident
- Handling Incidents
- Analyze needs & goals for/of Incident Response
- Incident Response Plan & Handling Steps
- Security Awareness and Training Checklist
- Training and Awareness
- Defining the Relationship between Incident Response, Incident Handling, and Incident Management
- Incident Management
- Incident Response Best Practices
- Incident Response Policy

**Module 4: CSIRT**

- What is CSIRT?
- Analyzing the need of Incident Response Team (IRT)
- CSIRT Goals, Strategy, and Vision
- Common Names of CSIRT
- CSIRT Mission Statement, & Constituency
- CSIRT Place in the Organization
- CSIRT Relationship with Peers
- Types of CSIRT Environments
- Best Practices for creating a CSIRT Role of CSIRTs
- How CSIRT Handles a Case
- Roles in an Incident Response Team
- CSIRT Services
- CSIRT Incident Report Form
- Incident Tracking and Reporting Systems

**Module 5: Handling Network Security Incidents**

- Denial-of-Service Incidents
- Detecting DoS Attack
- Distributed Denial-of-Service Attack
- Incident Handling Preparation for DoS
- Inappropriate Usage Incidents
- Multiple Component Incidents
- Network Auditing Tools

**Module 6: Handling Malicious Code Incidents**

- Count of Malware Samples
- Virus, Worms, Trojans and Spywares
- Incident Handling Preparation & Incident Prevention
- Detection of Malicious Code
- Evidence Gathering and Handling
- Containment Strategy
- Eradication and Recovery
- Recommendations
- Antivirus Systems

**Module 7: Handling Insider Threats**

- Insider Threats
- Anatomy of an Insider Attack
- Insider Threats Detection
- Insider Threats Response
- Insider Risk Matrix
- Insider’s Incident Response Plan
- Guidelines for Detecting and Preventing Insider Threats
- Employee Monitoring Tools

**Module 8: Forensic Analysis and Incident Response**

- Computer Forensics
- Objectives of Forensics Analysis
- Role of Forensics Analysis in Incident Response
- Types of Computer Forensics
- Forensic Readiness and Business Continuity
- Computer Forensics Process
- People Involved in Computer Forensics
- Digital Evidence
- Characteristics of Digital Evidence
- Collecting Electronic Evidence
- Forensic Policy
- Forensics in the Information System Life Cycle

**Module 9: Incident Reporting**

- Incident Reporting
- Why to Report an Incident?
- How to Report an Incident?
- Why Organizations do not Report Computer Crimes?
- Whom to Report an Incident?
- Details to be Reported
- Preliminary Information Security Incident Reporting Form
- Incident Reporting Guidelines
- CERT Incident Reference Numbers
- Sample Incident Reporting Form
- Sample Post Incident Report Form

**Module 10: Incident Recovery**

- Principles of Incident Recovery
- Incident Recovery
- Incident Recovery Steps
- Contingency/Continuity of Operations Planning
- Business Continuity Planning
- Incident Recovery Planning Team
- Incident Recovery Planning Process
- Business Impact Analysis
- Incident Recovery Testing
- Incident Recovery Training
- Incident Recovery Plan Implementation

**Module 11: Security Policies and Laws**

- Design of Security Policy
- Security Policy
- Key Elements of Security Policy
- Goals & Characteristics of a Security Policy
- Implementing Security Policies
- Acceptable Use Policy (AUP)
- Asset Control Policy
- Access Control Policy
- Documentation Policy
- Audit Trail Policy
- Evidence Preservation Policy
- Evidence Collection Policy
- Information Security Policy
- NIACAP Policy
- Physical Security Policy & Guidelines
- Personnel Security Policies & Guidance
- Law and Incident Handling

## Who Should Attend

This course will significantly benefit:

- Incident handlers
- Risk assessment administrators
- Penetration testers
- Cyber forensic investigators
- Vulnerability assessment auditors
- System administrators
- System engineers
- Firewall administrators
- Network managers
- IT managers
- IT professionals

## Exams

EC-Council Certified Incident Handler (ECIH) [E|CIH 212-89 exam]


| | | | |
|---|---|---|---|
| 464, Udyog Vihar Phase V,Gurgaon (Delhi NCR)-122016,India | +91 8882 233 777 | training@mercury.co.in | www.mercurysolutions.co |


Date - Apr 16, 2024