OVERVIEW

The EC-Council Certified Incident Handler program is designed to provide 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. After attending the course, they will be able to create incident handling and response policies and deal with various types of computer security incidents.

EC COUNCIL CERTIFIED INCIDENT HANDLER (ECIH)

COURSE OBJECTIVES

An incident is any event that has an impact on organizational security. They range considerably in severity levels and occur every day. It is not a question of if an incident will occur, but when and how much damage it will cause. Incident response policies mitigate the resultant impact of such disruptions by proactively addressing the issues. In a nutshell, you define what can happen, how bad it will be, and what to do to respond. Students attending the ECIH class will learn best practices in policy development and response. They will leave with the skillset to develop and implement their own incident response policies, resulting in a more resilient security posture for their organization.

TARGET STUDENT

This course will significantly benefit incident handlers, risk assessment administrators, penetration testers, cyber forensic investigators, venerability assessment auditors, system administrators, system engineers, firewall administrators, network managers, IT managers, IT professionals and anyone who is interested in incident handling and response.

COURSE CONTENT

Lesson 1: Introduction to Incident Response & Handling

- Cyber Incident Statistics
- Computer Security Incident
- Information as Business Asset
- Data Classification
- Common Terminologies
- Information Warfare
- Key Concepts of Information Security
- Vulnerability, Threat, and Attack
- Types of Computer Security Incidents
- Examples of Computer Security Incidents
- Verizon Data Breach Investigations Report – 2008
- Incidents That Required the Execution of Disaster Recovery Plans
- Signs of an Incident
- Incident Categories
- Incident Prioritization
- Incident Response
- Incident Handling
- Use of Disaster Recovery Technologies
- Impact of Virtualization on Incident Response and Handling
- Estimating Cost of an Incident
- Key Findings of Symantec Global Disaster Recovery Survey – 2009
- Incident Reporting
- Incident Reporting Organizations
- Vulnerability Resources

Lesson 2: Risk Assessment

- Risk
- Risk Policy
- Risk Assessment
- NIST's Risk Assessment Methodology
- Steps to Assess Risks at Work Place
- Risk Analysis
- Risk Mitigation
- Cost/Benefit Analysis
- NIST Approach for Control Implementation
- Residual Risk
- Risk Management Tools

Lesson 3: Incident Response & Handling Steps

- How to Identify an Incident
- Handling Incidents
- Need for Incident Response
- Goals of Incident Response
- Incident Response Plan
- Incident Response and Handling Steps
- Training and Awareness
- Security Awareness and Training Checklist
- Incident Management
- Incident Response Team
- Defining the Relationship between Incident Response, Incident Handling, and Incident Management
- Incident Response Best Practices
- Incident Response Policy
- Incident Response Plan Checklist
- Incident Handling System: RTIR
- RPIER 1st Responder Framework

Lesson 4: CSIRT

- What is CSIRT?
- What is the Need of an Incident Response Team (IRT)

- CSIRT Goals and Strategy
- CSIRT Vision
- Common Names of CSIRT
- CSIRT Mission Statement
- CSIRT Constituency
- CSIRT Place in the Organization
- CSIRT Relationship with Peers
- Types of CSIRT Environments
- Best Practices for creating a CSIRT
- Role of CSIRTs
- Roles in an Incident Response Team
- CSIRT Services
- CSIRT Policies and Procedures
- How CSIRT Handles a Case
- CSIRT Incident Report Form
- Incident Tracking and Reporting Systems
- CERT
- CERT-CC
- CERT(R) Coordination Center: Incident Reporting Form
- CERT:OCTAVE
- World CERTs
- IRTs Around the World

Lesson 5: Handling Network Security Incidents

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

Lesson 6: Handling Malicious Code Incidents

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

Lesson 7: Handling Insider Threats

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

Lesson 8: Forensic Analysis & Incident Response

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

Lesson 9: Incident Reporting

- Incident Reporting
- Why to Report an Incident
- Why Organizations do not Report Computer Crimes
- Whom to Report an Incident
- How to Report an Incident
- Details to be Reported
- Preliminary Information Security Incident Reporting Form
- CERT Incident Reference Numbers
- Contact Information
- Summary of Hosts Involved

- Description of the Activity
- Log Extracts Showing the Activity
- Time Zone
- Federal Agency Incident Categories
- Organizations to Report Computer Incident
- Incident Reporting Guidelines
- Sample Incident Reporting Form
- Sample Post Incident Report Form

Lesson 10: Incident Recovery

- Incident Recovery
- Principles of Incident Recovery
- Incident Recovery Steps
- Contingency/Continuity of Operations Planning
- Business Continuity Planning
- Incident Recovery Plan
- Incident Recovery Planning Process

Lesson 11: Security Policies & Laws

- Security Policy
- Key Elements of Security Policy
- Goals of a Security Policy
- Characteristics of a Security Policy
- Design of Security Policy
- Implementing Security Policies
- Acceptable Use Policy (AUP)
- Access Control Policy
- Asset Control Policy
- Audit Trail Policy
- Logging Policy
- Documentation Policy
- Evidence Collection Policy
- Evidence Preservation Policy
- Information Security Policy
- National Information Assurance Certification & Accreditation Process (NIACAP) Policy
- Physical Security Policy
- Physical Security Guidelines
- Personnel Security Policies & Guidance
- Law and Incident Handling
- Laws and Acts
- Intellectual Property Laws