ECIH™
EC-Council Certified Incident Handler

EC-Council Certified Incident Handler (ECIH)

Course Description

The ECIH 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.

The comprehensive training program will make students proficient in handling as well as responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats.

Key Outcomes

- Principals, processes and techniques for detecting and responding to security threats/ breaches
- Liaison with legal and regulatory bodies
- Learn to handle incidents and conduct assessments
- Cover various incidents like malicious code, network attacks, and insider attacks

Exam Information

- Exam Title: EC-Council Certified Incident Handler
- Exam Code: 212-89
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Introduction to Incident Response and Handling
- Risk Assessment
- Incident Response and Handling Steps
- CSIRT
- Handling Network Security Incidents
- Handling Malicious Code Incidents
- Handling Insider Threats
- Forensic Analysis and Incident Response
- Incident Reporting
- Incident Recovery
- Security Policies and Laws