Document Generated: 12/15/2025

Learning Style: On Demand

Technology: EC-Council

Difficulty: Intermediate

Course Duration: 20 Hours

EC Council Certified Incident Handler (ECIH)

What's Included:

- *Official EC Council Training Videos*
- *Official EC Council Courseware included*
- *Official EC Council ilabs subscription (6 months)*
- *EC Council Exam Voucher with Remote Proctoring Service included*

About this Course:

The ECIH program focuses on a structured approach for performing the incident handling and response (IH&R) process. The IH&R process includes stages like incident handling and response preparation, incident validation and prioritization, incident escalation and notification, forensic evidence gathering and analysis, incident containment, systems recovery, and incident eradication. This systematic incident handling and response process creates awareness among incident responders in knowing how to respond to various types of security incidents.

Cybersecurity Professionals interested in pursuing incident handling and response as a career require comprehensive training on the IH&R concepts as well as real-world scenarios. The ECIH program includes hands-on learning delivered through iLabs, online labs within the training program.

The Purpose of E|CIH is

- To enable individuals and organizations with the ability to handle and respond to different types of cybersecurity incidents in a systematic way.
- To ensure that organization can identify, contain, and recover from an attack.
- To reinstate regular operations of the organization as early as possible and mitigate the negative impact on the business operations.
- To be able to draft security policies with efficacy and ensure that the quality of services is maintained at the agreed levels.
- To minimize the loss and after-effects breach of the incident.
- For individuals: To enhance skills on incident handling and boost their employability.

Course Objectives:

- Understand the key issues plaguing the information security world
- Learn to combat different types of cybersecurity threats, attack vectors, threat actors and their motives
- Learn the fundamentals of incident management including the signs and costs of an incident
- Understand the fundamentals of vulnerability management, threat assessment, risk management, and incident response automation and

orchestration
- Master all incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
- Decode the various steps involved in planning an incident handling and response program
- Gain an understanding of the fundamentals of computer forensics and forensic readiness
- Comprehend the importance of the first response procedure including evidence collection, packaging, transportation, storing, data acquisition, volatile and static evidence collection, and evidence analysis
- Understand anti-forensics techniques used by attackers to find cybersecurity incident cover-ups
- Apply the right techniques to different types of cybersecurity incidents in a systematic manner including malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents

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

Course Outline:

Module 01:
Introduction to Incident Handling and Response

Module 02:
Incident Handling and Response Process

Module 03:
Forensic Readiness and First Response

Module 04:
Handling and Responding to Malware Incidents

Module 05:
Handling and Responding to Email Security Incidents

Module 06:
Handling and Responding to Network Security Incidents

Module 07:

Handling and Responding to Web Application Security Incidents

Module 08:
Handling and Responding to Cloud Security Incidents

Module 09:
?Handling and Responding to Insider Threats