Document Generated: 12/15/2025

Learning Style: Virtual Classroom

Technology: EC-Council

Difficulty: Intermediate

Course Duration: 3 Days

EC-Council Certified Incident Handler Instructor Led Training

What's Included:

- *Official EC Council Invitation to the virtual class*
- *Official EC Council Print or e-courseware included*

- *Official EC Council ilabs subscription*
- *EC Council Exam Voucher included*

About this course:

The latest version of EC-Council's Certified Incident Handler (ECIH) program is a specialist-level program developed in collaboration with cybersecurity experts and practitioners. It goes beyond incident detection, focusing on equipping professionals with the knowledge and skills to effectively handle the aftermath of a security breach. By addressing post-breach consequences, the program aims to minimize financial and reputational impact on organizations. Participants learn strategies and best practices to mitigate breach consequences, enhance incident response capabilities, and protect organizations from future threats, boosting employability in the cybersecurity field. Overall, the ECIH program provides a concise and practical approach to incident handling and response, safeguarding organizations from potential damage.

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 incident

Audience:

- Penetration Testers
- Application Security Engineers

- Vulnerability Assessment Auditors
- Cyber Forensic Investigators/ Analyst and SOC Analyst
- Risk Assessment Administrators
- System Administrators/Engineers
- Network Administrators
- Firewall Administrators and Network Managers/IT Managers

Prerequisites:

It is recommended that you have at least 1 year of experience in the cybersecurity domain.

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