EC-Council Certified Incident Handler (ECIH)

Duration 3 days

COURSE DESCRIPTION

EC-Council's Certified Incident Handler program equips students with the knowledge, skills, and abilities to effectively prepare for, deal with, and eradicate threats and threat actors in an incident. This program provides the entire process of Incident Handling and Response and hands-on labs that teach tactical procedures and techniques required to effectively Plan, Record, Triage, Notify and Contain. ECIH also covers post incident activities such as Containment, Eradication, Evidence Gathering and Forensic Analysis, leading to prosecution or countermeasures to ensure the incident is not repeated. With over 95 labs, 800 tools covered, and exposure to Incident Handling activities on four different operating systems, E|CIH provides a well-rounded, but tactical approach to planning for and dealing with cyber incidents.

COURSE OBJECTIVES

- Key issues plaguing the information security world
- Various types of cyber security threats, attack vectors, threat actors, and their motives, goals, and objectives of cyber security attacks
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- Fundamentals of information security concepts (Vulnerability assessment, risk management, cyber threat intelligence, threat modeling, and threat hunting)
- Fundamentals of incident management (information security incidents, signs and costs of an incident, incident handling and response, and incident response automation and orchestration)
- Different incident handling and response best practices, standards, cyber security frameworks, laws, acts, and regulations
- Various steps involved in planning incident handling and response program (Planning, recording and assignment, triage, notification, containment, evidence gathering and forensic analysis, eradication, recovery, and post-incident activities)
- Importance of first response and first response procedure (Evidence collection, documentation, preservation, packaging, and transportation)
- How to handle and respond to different types of cyber security incidents in a systematic way (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, insider threat-related incidents, and endpoint security incidents)

COURSE OUTLINE

- Introduction to Incident Handling and Response
- Incident Handling and Response Process
- First Response
- Handling and Responding to Malware Incidents
- Handling and Responding to Email Security Incidents
- Handling and Responding to Network Security Incidents
- Handling and Responding to Web Application Security Incidents
- Handling and Responding to Cloud Security Incidents
- Handling and Responding to Insider Threats
- Handling and Responding to Endpoint Security Incidents

CERTIFICATION

Exam Name: ECIH 212-89
Number of Questions: 100
Test Format: Multiple Choice

WHO SHOULD ATTEND

- Incident Handler
- Incident Responder
- Incident Response
- Consultant/Associate/Analyst/Engineer/Specialist/Expert/Manager CSIRT Analyst/Engineer/Manager
- Information Security Associate/ Analyst/Engineer/Specialist/Manager
- Cyber Defense Security Consultant/Associate/Analyst
- IT Security Operations Center Analyst (SOC Analyst/Engineer)
- Cyber Forensic Investigator/Consultant/Analyst/Manager Digital Forensic Analyst
- Cyber Risk Vulnerability Analyst/Manager
- Cyber Intelligence Analyst and Cyber Security Threat Analyst/Specialist
- Cyber Security Incident Response Team Lead
- Penetration Tester