Certified Incident Handler v3

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 ANAB ISO/IEC 17024 accredited and US DoD 8140 approved program provides the entire process of Incident Handling and Response and hands-on labs that teach the tactical procedures and techniques required to effectively Plan, Record, Triage, Notify and Contain. Students will learn the handling of various types of incidents, risk assessment methodologies, as well as laws and policies related to incident handling. After attending the course, students will be able to create IH&R policies and deal with different types of security incidents such as malware, email security, network security, web application security, cloud security, and insider threat-related incidents.

Course Objectives:

- Key issues plaguing the information security world.
- Various types of cybersecurity threats, attack vectors, threat actors, and their motives, goals, and objectives of cybersecurity 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)
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- 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, cybersecurity 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 cybersecurity 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)

Target Audience:

- Any mid-level to high-level cybersecurity professionals with a minimum of 1 year of experience
- Individuals from the information security profession and who want to enrich their skills and knowledge in the field of incident handling and response.
- Individuals interested in preventing cyber threats.

Course Outlines:

- Module 1: Introduction to Incident Handling and response
- Module 02: Incident Handling and Response Process
- Module 03: First Response
- Module 4: 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
- Module 10: Handling and Responding to Endpoint Security Incidents