EC-Council Certified Incident Handler (ECIH)

Introduction

The ECIH program is designed to provide the fundamental skills to handle and respond to 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

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

Prerequisites

- One year of experience managing Windows/Unix/Linux systems or have equivalent knowledge and skills

- A good understanding of common network and security services is required

Target Audience

- Incident handlers
- Risk assessment administrators
- Penetration testers
- Cyber forensic investigators
- Venerability assessment auditors
- System administrators and engineers
- Firewall administrators
- Network managers
- IT managers

Duration

24 hours training course