Iverson Associates Sdn Bhd (303330-M)
Suite T113 – T114, 3rd Floor, Centrepoint, Lebuh Bandar Utama
Bandar Utama, 47800 Petaling Jaya, Selangor Darul Ehsan
Tel: 03-7726 2678 Fax: 03-7727 9737 Website: www.iverson.com.my

Module Title : EC-Council Certified Incident Handler v2
Duration : 3 days

Description

The E|CIH exam can be attempted after the completion of the official E|CIH course taught either by any EC-Council Authorized Training Center (ATCs) or by EC-Council directly. Candidates that successfully pass the exam will receive the E|CIH certificate and membership privileges. Members are required to adhere to the policies of EC-Council's Continuing Education Policy.

Learning 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

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

Who Is It For?

The incident handling skills taught in E|CIH are complementary to the job roles below as well as many other cybersecurity jobs:

- 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

E|CIH is a specialist-level program that caters to mid-level to high-level cybersecurity professionals. In order to increase your chances of success, it is recommended that you have at least 1 year of experience in the cybersecurity domain.

E|CIH members are ambitious security professionals who work in Fortune 500 organizations globally.

About the Exam

E|CIH allows cybersecurity professionals to demonstrate their mastery of the knowledge and skills required for Incident Handling.

Exam Title	EC-Council Certified Incident Handler
Exam Code	212-89
Number of Questions	100
Duration	3 hours
Availability	EC-Council Exam Portal
Test Format	Multiple Choice
Passing Score	70%

Eligibility Criteria

To be eligible to sit the E|CIH Exam, the candidate must either:

Attend official E|CIH training through any of EC-Council's Authorized Training Centers (ATCs) or attend EC-Council's live online training via iWeek or join our self-study program through iLearn (see https://iclass.eccouncil.org).

OR

Candidates with a minimum of 1 year of work experience in the domain that would like to apply to take the exam directly without attending training are required to pay the USD100 Eligibility Application Fee. This fee is included in your training fee should you choose to attend training.