

## Certified Incident Handler

**Course Duration: 24 Hrs.**

**Course code: E|CIH**

### Course Overview

The EC-Council Certified Incident Handler (ECIH) program is a specialist-level course that equips IT professionals with the knowledge and skills to effectively handle and respond to cybersecurity incidents, focusing on reducing the impact of breaches both financially and reputationally.

### What you'll learn?

- ❖ **Understanding the Incident Handling Process:**  
Learn the fundamentals of incident handling, including the incident handling process and procedures.
- ❖ **Incident Response Planning:**  
Develop and maintain effective incident response plans, including communication channels and protocols.
- ❖ **Incident Identification and Classification:**  
Learn to identify, classify, and analyze the impact of various security incidents.
- ❖ **Containment and Eradication:**  
Implement containment strategies to limit the impact of incidents and eradicate the root cause.

### Target Audience

- ❖ Cybersecurity Analysts
- ❖ Incident Response Team Members
- ❖ IT Security Managers
- ❖ Network Security Engineers
- ❖ Security Operations Center (SOC) Analysts

## Pre-Requisites

### ❖ **Cybersecurity Experience:**

A minimum of one year of experience in the cybersecurity domain is generally recommended.

### ❖ **IT Knowledge:**

A basic understanding of IT concepts, including networking, security services, and operating systems (Windows, Unix, Linux) is beneficial.

### ❖ **Ethical Hacking and Digital Forensics:**

Familiarity with ethical hacking and digital forensics concepts can also be advantageous.

## Course content

### **MODULE 01: INTRODUCTION TO INCIDENT HANDLING AND RESPONSE**

- A. Understand Information Security Threats and Attack Vectors
- B. Explain Various Attack and Defense Frameworks
- C. Understand Information Security Concepts
- D. Understand Information Security Incidents
- E. Understand the Incident Management Process
- F. Understand Incident Response Automation and Orchestration
- G. Describe Various Incident Handling and Response Best Practices
- H. Explain Various Standards Related to Incident Handling and Response
- I. Explain Various Cybersecurity Frameworks
- J. Understand Incident Handling Laws and Legal Compliance

### **MODULE 02: INCIDENT HANDLING AND RESPONSE PROCESS**

- A. Understand Incident Handling and Response (IH&R) Process
- B. Explain Preparation Steps for Incident Handling and Response
- C. Understand Incident Recording and Assignment
- D. Understand Incident Triage
- E. Explain the Process of Notification
- F. Understand the Process of Containment

- G. Describe Evidence Gathering and Forensics Analysis
- H. Explain the Process of Eradication
- I. Understand the Process of Recovery
- J. Describe Various Post-Incident Activities
- K. Explain the Importance of Information Sharing Activities

## **MODULE 03: FIRST RESPONSE**

- A. Explain the Concept of the First Response
- B. Understand the Process of Securing and Documenting the Crime Scene
- C. Understand the Process of Collecting Evidence at the Crime Scene
- D. Explain the Process for Preserving, Packaging, and Transporting Evidence

## **MODULE 04: HANDLING AND RESPONDING TO MALWARE INCIDENTS**

- A. Understand the Handling of Malware Incidents
- B. Explain Preparation for Handling Malware Incidents
- C. Understand Detection of Malware Incidents
- D. Explain the Containment of Malware Incidents
- E. Describe How to Perform Malware Analysis
- F. Understand Eradication of Malware Incidents
- G. Explain Recovery After Malware Incidents
- H. Understand the Handling of Malware Incidents-Case Study
- I. Describe Best Practices against Malware Incidents

## **MODULE 05: HANDLING AND RESPONDING TO EMAIL SECURITY INCIDENTS**

- A. Understand the Handling of Network Security Incidents
- B. Prepare to Handle Network Security Incidents
- C. Understand Detection and Validation of Network Security Incidents
- D. Understand the Handling of Unauthorized Access Incidents
- E. Understand the Handling of Inappropriate Usage Incidents
- F. Understand the Handling of Denial-of-Service Incidents
- G. Understand the Handling of Wireless Network Security Incidents

- H. Understand the Handling of Network Security Incidents-Case Study
- I. Describe Best Practices Against Network Security Incidents

## **MODULE 06: HANDLING AND RESPONDING TO NETWORK SECURITY INCIDENTS**

- A. Understand the Handling of Network Security Incidents
- B. Prepare to Handle Network Security Incidents
- C. Understand Detection and Validation of Network Security Incidents
- D. Understand the Handling of Unauthorized Access Incidents
- E. Understand the Handling of Inappropriate Usage Incidents
- F. Understand the Handling of Denial-of-Service Incidents
- G. Understand the Handling of Wireless Network Security Incidents
- H. Understand the Handling of Network Security Incidents-Case Study
- I. Describe Best Practices against Network Security Incidents

## **MODULE 07: HANDLING AND RESPONDING TO WEB APPLICATION SECURITY INCIDENTS**

- A. Understand the Handling of Web Application Incidents
- B. Explain Preparation for Handling Web Application Security Incidents
- C. Understand Detection and Containment of Web Application Security Incidents
- D. Explain Analysis of Web Application Security Incidents
- E. Understand Eradication of Web Application Security Incidents
- F. Explain Recovery After Web Application Security Incidents
- G. Understand the Handling of Web Application Security Incidents-Case Study
- H. Describe Best Practices for Securing Web Applications

## **MODULE 08: HANDLING AND RESPONDING TO CLOUD SECURITY INCIDENTS**

- A. Understand the Handling of Cloud Security Incidents
- B. Explain Various Steps Involved in Handling Cloud Security Incidents
- C. Understand How to Handle Azure Security Incidents
- D. Understand How to Handle AWS Security Incidents

- E. Understand How to Handle Google Cloud Security Incidents
- F. Understand the Handling of Cloud Security Incidents-Case Study
- G. Explain Best Practices Against Cloud Security Incidents

## MODULE 09: HANDLING AND RESPONDING TO INSIDER THREATS

- A. Understand the Handling of Insider Threats
- B. Explain Preparation Steps for Handling Insider Threats
- C. Understand the Detection and Containment of Insider Threats
- D. Explain Analysis of Insider Threats
- E. Understand the Eradication of Insider Threats
- F. Understand the Process of Recovery After Insider Attacks
- G. Understand the Handling of Insider Threats-Case Study
- H. Describe Best Practices Against Insider Threats

## MODULE 10: HANDLING AND RESPONDING TO ENDPOINT SECURITY INCIDENTS

- A. Understand the Handling of Endpoint Security Incidents
- B. Explain the Handling of Mobile-Based Security Incidents
- C. Explain the Handling of IoT-Based Security Incidents
- D. Explain the Handling of OT-Based Security Incidents
- E. Understand the Handling of Endpoint Security Incidents-Case Study

## Exam Preference

Exam Code	212-89
Number Of Questions	100 MCQ.
Length Of Test	180 Minutes
Passing Score	70%