Certified Incident Handler v3

24 Hrs

What is the EC-Council Certified Incident Handling Response Program?

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 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.

The E|CIH (EC-Council Certified Incident Handler) 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.

The E|CIH is a method-driven course that provides a holistic approach covering vast concepts related to organizational IH&R, from preparing/planning the incident handling response process to recovering organizational assets from the impact of security incidents. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

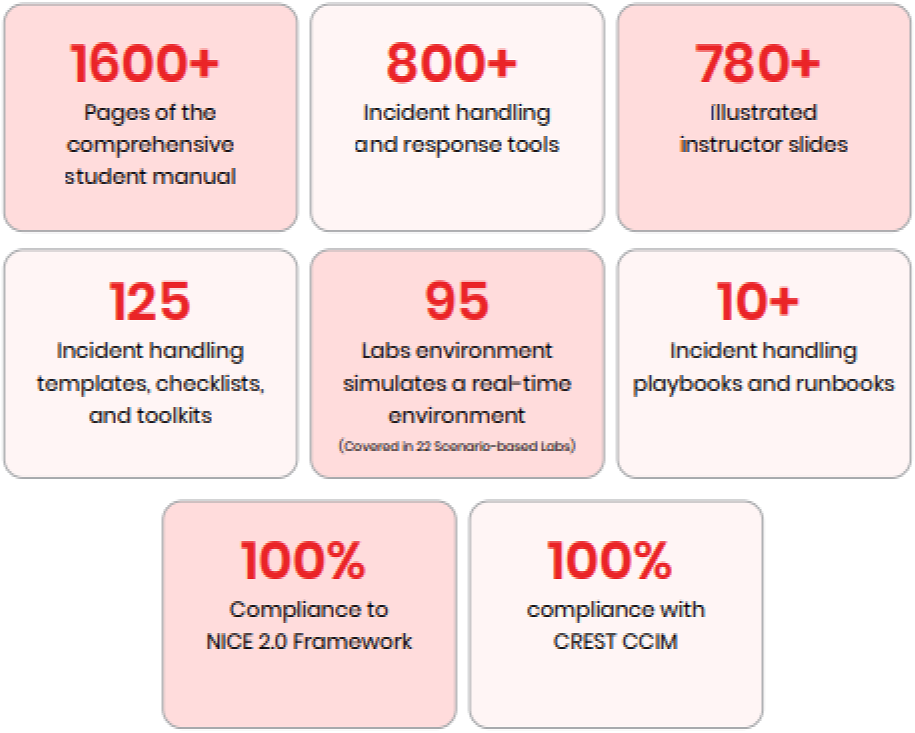
With over 95 advanced labs, 800 tools covered, and exposure to incident handling activities on many different operating systems, E|CIH provides a well-rounded, but tactical approach to planning for and dealing with cyber incidents.

The E|CIH program addresses all stages involved in the IH&R process, and this attention toward a realistic and futuristic approach makes E|CIH one of the most comprehensive IH&R-related certifications in the market today

Certified Incident Handler v3

24 Hrs

Key Features & Critical Components of E|CIH Program



1600+
Pages of the comprehensive student manual

800+
Incident handling and response tools

780+
Illustrated instructor slides

125
Incident handling templates, checklists, and toolkits

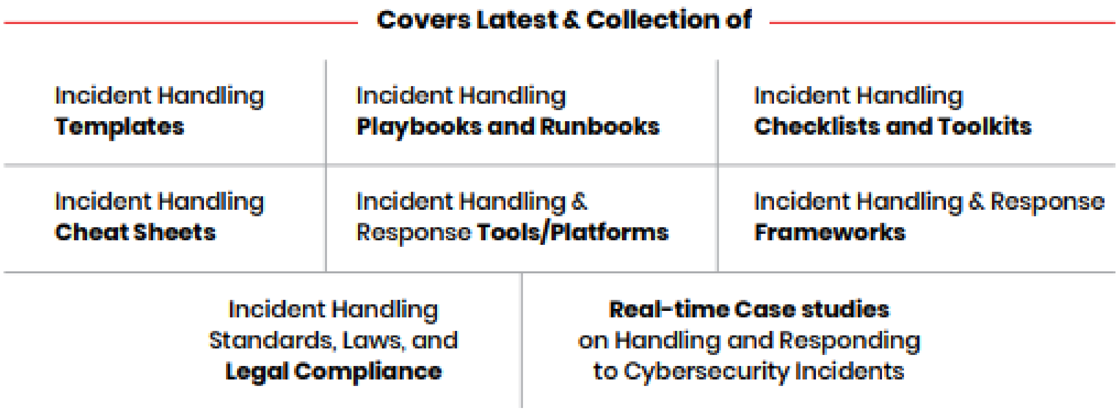
95
Labs environment simulates a real-time environment
(Covered in 22 Scenario-based Labs)

10+
Incident handling playbooks and runbooks

100%
Compliance to NICE 2.0 Framework

100%
compliance with CREST CCIM

- Based on a Comprehensive Industry-wide Job Task Analysis (JTA)
- Structured approach for performing incident handling and response process.
- Focus on developing skills in handling different types of cybersecurity incidents



Covers Latest & Collection of

Incident Handling **Templates**

Incident Handling **Playbooks and Runbooks**

Incident Handling **Checklists and Toolkits**

Incident Handling **Cheat Sheets**

Incident Handling & Response **Tools/Platforms**

Incident Handling & Response **Frameworks**

Incident Handling Standards, Laws, and **Legal Compliance**

Real-time Case studies on Handling and Responding to Cybersecurity Incidents

Certified Incident Handler v3

24 Hrs

What Do You Learn from E|CIH ?

- 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, 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)

Learn the 9 Stages of Incident Handling & Response (IH & R) Process

1. Planning
2. Recording & Assignment
3. Triage
4. Notification
5. Containment
6. Post Incident Activities
7. Recovery
8. Eradicatio
9. Evidence Gathering & Forensics Analysis

Certified Incident Handler v3

24 Hrs

E|CIH Course Modules:

MODULE 01: INTRODUCTION TO INCIDENT HANDLING AND RESPONSE

- Understand Information Security Threats and Attack Vectors
- Explain Various Attack and Defense Frameworks
- Understand Information Security Concepts
- Understand Information Security Incidents
- Understand the Incident Management Process
- Understand Incident Response Automation and Orchestration
- Describe Various Incident Handling and Response Best Practices
- Explain Various Standards Related to Incident Handling and Response
- Explain Various Cybersecurity Frameworks
- Understand Incident Handling Laws and Legal Compliance

MODULE 02: INCIDENT HANDLING AND RESPONSE PROCESS

- Understand Incident Handling and Response (IH&R) Process
- Explain Preparation Steps for Incident Handling and Response
- Understand Incident Recording and Assignment
- Understand Incident Triage
- Explain the Process of Notification
- Understand the Process of Containment
- Describe Evidence Gathering and Forensics Analysis
- Explain the Process of Eradication
- Understand the Process of Recovery
- Describe Various Post-Incident Activities
- Explain the Importance of Information Sharing Activities

MODULE 03: FIRST RESPONSE

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

MODULE 04: HANDLING AND RESPONDING TO MALWARE INCIDENTS

- Understand the Handling of Malware Incidents
- Explain Preparation for Handling Malware Incidents
- Understand Detection of Malware Incidents
- Explain Containment of Malware Incidents
- Describe How to Perform Malware Analysis
- Understand Eradication of Malware Incidents
- Explain Recovery after Malware Incidents

- Understand the Handling of Malware Incidents - Case Study
- Describe Best Practices against Malware Incidents

MODULE 05: HANDLING AND RESPONDING TO EMAIL SECURITY INCIDENTS

- Understand Email Security Incidents
- Explain Preparation Steps for Handling Email Security Incidents
- Understand Detection and Containment of Email Security Incidents
- Understand Analysis of Email Security Incidents
- Explain Eradication of Email Security Incidents
- Understand the Process of Recovery after Email Security Incidents
- Understand the Handling of Email Security Incidents - Case Study
- Explain Best Practices against Email Security Incidents

MODULE 06: HANDLING AND RESPONDING TO NETWORK SECURITY INCIDENTS

- Understand the Handling of Network Security Incidents
- Prepare to Handle Network Security Incidents
- Understand Detection and Validation of Network Security Incidents
- Understand the Handling of Unauthorized Access Incidents
- Understand the Handling of Inappropriate Usage Incidents
- Understand the Handling of Denial-of-Service Incidents
- Understand the Handling of Wireless Network Security Incidents
- Understand the Handling of Network Security Incidents - Case Study
- Describe Best Practices against Network Security Incidents

MODULE 07: HANDLING AND RESPONDING TO WEB APPLICATION SECURITY INCIDENTS

- Understand the Handling of Web Application Incidents
- Explain Preparation for Handling Web Application Security Incidents
- Understand Detection and Containment of Web Application Security Incidents
- Explain Analysis of Web Application Security Incidents
- Understand Eradication of Web Application Security Incidents
- Explain Recovery after Web Application Security Incidents
- Understand the Handling of Web Application Security Incidents - Case Study
- Describe Best Practices for Securing Web Applications

MODULE 08: HANDLING AND RESPONDING TO CLOUD SECURITY INCIDENTS

- Understand the Handling of Cloud Security Incidents
- Explain Various Steps Involved in Handling Cloud Security Incidents
- Understand How to Handle Azure Security Incidents
- Understand How to Handle AWS Security Incidents

- Understand How to Handle Google Cloud Security Incidents
- Understand the Handling of Cloud Security Incidents - Case Study
- Explain Best Practices against Cloud Security Incidents

MODULE 09: HANDLING AND RESPONDING TO INSIDER THREATS

- Understand the Handling of Insider Threats
- Explain Preparation Steps for Handling Insider Threats
- Understand Detection and Containment of Insider Threats
- Explain Analysis of Insider Threats
- Understand Eradication of Insider Threats
- Understand the Process of Recovery after Insider Attacks
- Understand the Handling of Insider Threats - Case Study
- Describe Best Practices against Insider Threats

MODULE 10: HANDLING AND RESPONDING TO ENDPOINT SECURITY INCIDENTS

- Understand the Handling of Endpoint Security Incidents
- Explain the Handling of Mobile-based Security Incidents
- Explain the Handling of IoT-based Security Incidents
- Explain the Handling of OT-based Security Incidents
- Understand the Handling of Endpoint Security Incidents - Case Study

Training and Exam Details

Number of Questions: 100

Exam Duration: 3 Hours

Availability: EC-Council Exam Portal

Exam Title: EC-Council Certified Incident Handler

Exam Format: Multiple Choice