# EC-Council Certified Incident Handler (E|CIH) + Exam voucher

**Duration: 3 Days  Course Code: ECIH  Version: 2.0**

## Overview:

The latest revision of EC-Council's Certified Incident Handler (E|CIH) certified program has been designed and developed in collaboration with cybersecurity and incident handling/response practitioners across the globe.

The ECIH program focuses on a structured approach to the incident handling and response (IH&R) process. This IH&R process includes stages such as; incident handling and response preparation, incident validation and prioritization, incident escalation and notification, forensic evidence gathering and analysis, incident containment, systems recovery, and incident eradication. This systematic incident handling and response process creates awareness among the incident responders in knowing how to respond to various types of security incidents happening in organisations today.The types of cybersecurity incidents covered include malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents.
It is a comprehensive specialist level program, that imparts knowledge and skills on how organisations can effectively handle post breach consequences by reducing the impact of the incident, both financially and reputationally. The learning objectives are emphasised through practical learning with 40% of this course covering hands-on experience of the latest incident handling and response tools, techniques, methodologies, frameworks, etc.

The E|CIH lab environment consists of the latest and patched operating systems including Windows 10, Windows Server 2016, Ubuntu Linux, and OSSIM for performing labs.
Students will have access to over 50 labs, 800 tools, and 4 OSs! as well as a large array of templates, check lists, and cheat sheets.

The ECIH Program is 100% Compliant with the NICE 2.0 Framework AND CREST Framework.
**Please Note: An exam voucher is included with this course**

## Target Audience:

This course will significantly benefit incident handlers, risk assessment administrators, penetration testers, cyber forensic investigators, venerability assessment auditors, system administrators, system engineers, firewall administrators, network managers, IT managers, IT professionals and anyone who is interested in incident handling and response.

## Objectives:

- **After completing this course you should be able to:**
- Understand the key issues plaguing the information security world
- Combat the different types of cybersecurity threats, attack vectors, threat actors and their motives, goals, and objectives of cybersecurity attacks
- Explain the fundamentals of incident management (information security incidents, signs and costs of an incident, incident handling and response and their advantages, etc.)
- Explain the fundamentals of vulnerability management, threat assessment, risk management, 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 incident handling and response program (Planning, Recording and Assignment, Triage, Notification, Containment, Evidence Gathering and Forensic Analysis, Eradication, Recovery, and Post-Incident Activities)
- Have an understanding of the fundamentals of computer forensics and forensic readiness
- Comprehend the importance of first response and first response procedure (Evidence collection, packaging, transportation, storing, data acquisition, volatile and static evidence collection, and evidence analysis)
- Find out anti-forensics techniques used by attackers to uncover cybersecurity incident cover-ups
- Apply the right techniques to different types of cybersecurity incidents in a systematic manner (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents)

## Prerequisites:

**Attendees should meet the following prerequsites:**

- It is recommended that you have at least 1 year of experience in the cybersecurity domain in order to maximize course outcomes.

## Testing and Certification

**Recommended as preparation for the following exam:**

- **212-89** - EC-Council Certified Incident Handler

**To be eligible to attend the E|CIH Exam, candidates must either:**

- Attend the 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.
- Candidates with a minimum of 1 year work experience in the domain that would like to apply to challenge the exams 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.

## Content:

Introduction to Incident Handling and Response

- Overview of Information Security Concepts
- Understanding Information Security Threats and Attack Vectors
- Understanding Information Security Incident
- Overview of Incident Management
- Overview of Vulnerability Management
- Overview of Threat Assessment
- Understanding Risk Management
- Understanding Incident Response Automation and Orchestration
- Incident Handling and Response Best Practices
- Overview of Standards
- Overview of Cybersecurity Frameworks
- Importance of Laws in Incident Handling
- Incident Handling and Legal Compliance

Incident Handling and Response Process

- Overview of Incident Handling and Response (IH;R) Process
- Step 1: Preparation for Incident Handling and Response
- Step 2: Incident Recording and Assignment
- Step 3: Incident Triage
- Step 4: Notification
- Step 5: Containment
- Step 6: Evidence Gathering and Forensics Analysis
- Step 7: Eradication
- Step 8: Recovery
- Step 9: Post-Incident Activities

Forensic Readiness and First Response

- Introduction to Computer Forensics
- Overview of Forensic Readiness
- Overview of First Response
- Overview of Digital Evidence
- Understanding the Principles of Digital Evidence Collection
- Collecting the Evidence
- Securing the Evidence
- Overview of Data Acquisition
- Understanding the Volatile Evidence Collection
- Understanding the Static Evidence Collection
- Performing Evidence Analysis
- Overview of Anti-Forensics

Handling and Response to Malware Incidents

- Overview of Malware Incident Response
- Preparation for Handling Malware Incidents
- Detecting Malware Incidents
- Containment of Malware Incidents
- Eradication of Malware Incidents
- Recovery after Malware Incidents
- Guidelines for Preventing Malware Incidents

Handling and Responding to Email Security Incidents

- Overview of Email Security Incidents
- Preparation for Handling Email Security Incidents
- Detection and Containment of Email Security Incidents
- Eradication of Email Security Incidents
- Recovery after Email Security Incidents

Handling and Responding to Network Security Incidents

- Overview of Network Security Incidents
- Preparation for Handling Network Security Incidents
- Detection and Validation of Network Security Incidents
- Handling Unauthorized Access Incidents
- Handling Inappropriate Usage Incidents
- Handling Denial-of-Service Incidents
- Handling Wireless Network Security Incidents

Handling and Responding to Web Application Security Incidents

- Overview of Web Application Incident Handling
- Web Application Security Threats and Attacks
- Preparation to Handle Web Application Security Incidents
- Detecting and Analyzing Web Application Security Incidents
- Containment of Web Application Security Incidents
- Eradication of Web Application Security Incidents
- Recovery from Web Application Security Incidents
- Best Practices for Securing Web Applications

Handling and Responding to Cloud Security Incidents

- Cloud Computing Concepts
- Overview of Handling Cloud Security Incidents
- Cloud Security Threats and Attacks
- Preparation for Handling Cloud Security Incidents
- Detecting and Analyzing Cloud Security Incidents
- Containment of Cloud Security Incidents
- Eradication of Cloud Security Incidents
- Recovering from Cloud Security Incidents
- Best Practices Against Cloud-based Incidents

Handling and Responding to Insider Threats

- Introduction to Insider Threats
- Preparation for Handling Insider Threats
- Detecting and Analyzing Insider Threats
- Containment of Insider Threats
- Eradication of Insider Threats
- Recovery after Insider Attacks
- Best Practices Against Insider Threats

## Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo