E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security

EC-Council

CERTIFIED INCIDENT HANDLER

MASTER THE CRITICAL FIRST LINE OF DEFENSE

Gain The Ultimate Skills to Identify, Contain and Minimize Cyber Incidents

Average Incident Response Time : A Growing Problem

277 days

Average time to identify and contain a data breach.

49 days

Ransomware breaches took 49 days longer than average to identify and contain.

303 Days

Average time to identify and contain a supply chain compromise.

Why Organizations Need Incident Response?

1. Organizations Invested in buying expensive security products?

› **YES**

2. Did they over rely on the deployed security products?

› **Yes**

3. Hire Individuals or teams to configure those security products?

› **Not Often**

4. Were they successful in evading security incidents?

› **No**

5. Did they predict the possibilities of the attack and its impact?

› **No**

6. Did they have a structured incident handling and response plan in-place to tackle potential security incidents?

› **NO**

What is Incident Response?

1. A Process That Allows organizations To **Handle And Respond To Various Security Incidents** Instantly

2. A Process That Enables organizations To **Detect, Validate, Contain, And Eradicate** Various Security Incidents

3. A Process That Ensures **Safe And Systematic Recovery** Of All The Organizational Assets From The Impact Of Security Incidents

4. A Process That Assures organizations are **Well Prepared** For Handling the most common Security Incidents

In short, Organizations need

Incident Handling and Response Plan/Process

Organizations needs

EC-Council Certified Incident Handler

E|CIH Program Overview

What is E|CIH?

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.

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

E|CIH Course Modules:

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

E|CIH Course Modules:

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

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. Eradication
9. Evidence Gathering & Forensics Analysis

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	

Unique Benefits of E|CIH Advanced Labs

01

Lab setup

simulates Real-time Environment with real-life networks and platforms

02

Every learning

objective is demonstrated using Complex and advanced labs

03

Lab-intensive

Program (Demonstration of Various Cybersecurity Incidents via Scenario-based Labs)

04

Hands-on Program

(Dedication of 50% of Training Time to Labs)

05

Latest Patched

Windows operating systems

06

Ubuntu,

Parrot Security, Pfsense Firewall, OSSIM Server, And Android for Performing Labs.

07

Advanced

Forensic Software

08

Latest

Threat Intelligence Platforms

09

Latest

Network Monitoring Solutions Scenario-based labs

10

Learn

to handle and respond to various types of security incidents on a real-time organizational network.

11

Understand

Detect & analyze modern attack TTPs using various incident handling tools

E|CIH Is Built to Remediate Modern Cyber Threats

Key Benefits / Critical Components of E|CIH Course Explained:

1) 100% Compliance with NICE Special Publication 800-181 Cybersecurity Workforce Framework

E|CIH fully maps to the National Initiative for Cybersecurity Education (NICE) in the Protect and Defend (PR) category and Incident Response (CIR) specialty area handling deals with investigating, analyzing, and responding to cyber incidents within a network environment or enclave.

2) 100% Compliance with CREST Certified Incident Manager (CCIM) Frameworks

E|CIH fully maps to the CREST Certified Incident Manager (CCIM), which is a broad-based scheme focused on maintaining an appropriate standard for incident response, managed by an industry professional body, delivered by the industry, and endorsed by CESG and CPNI. The CCIM scheme, currently administered by CREST, is also known as CREST Certified Incident Response Scheme (CSIR).

3) Based on a Comprehensive Industry-wide Job Task Analysis

The E|CIH program was developed after intensive analysis of all possible combinations of Task, Knowledge, Skill, and Ability (TKSA) from relevant job postings of various multinational companies.

4) Focus on a Structured Approach for IH&R

This process includes various stages such as IH&R preparation, incident recording and assignment, incident triage and notification, incident containment, evidence gathering and forensic analysis, incident eradication, system recovery, and post-incident activities.

5) Large Collection of Incident Handling Templates, Checklists, and Toolkits

This vast collection of documentation material enables incident handlers to effectively accomplish incident-related documentation in their organization within a reasonable timeframe. Incident handling templates help incident handlers to draft comprehensive reports based on the target audience and incidents, thus providing wider options to students and incident handlers than any other program in the market.

6) Large Collection of Incident Handling Playbooks and Runbooks

When used together, playbooks and runbooks can guide incident handlers in orchestrating various security processes based on the type of incident. Ready-to-use playbooks and runbooks help the IH&R team to automate common cyber-attacks such as phishing, malware, and denial-of-service.

7) Focus on Developing Skills to Handle Various Cybersecurity Incidents

This program systematically demonstrates the complete IH&R process for various types of cybersecurity incidents, including malware, email security, network security, web application security, cloud security, insider threat, mobile-based security, IoT-based security, and OT-based security incidents. Covering the end-to-end IH&R process making E|CIH a unique program in the market.

8) Emphasis on Forensic Readiness and First Response Procedures

A lack of forensic readiness or the first response process to incidents can cause drastic and disastrous damage to organizations. The E|CIH program focuses on how an organization should be prepared and equipped to tackle any type of cyber incident, along with the steps to be taken by the first responder to record or deal with incidents.

9) Lab-intensive Program (Demonstration of Various Cybersecurity Incidents via Scenario-based Labs)

The E|CIH program demonstrates real-time security incidents using scenario-based labs with respect to various incident-handling phases. This helps students and incident handlers to gain in-depth knowledge and skills in IH&R preparation, incident recording and assignment, incident triage and notification, incident containment, evidence gathering and forensic analysis, incident eradication, system recovery, and post-incident activities.

10) Hands-On Program (Dedication of 50% of Training Time to Labs)

The theory-to-practice ratio in the E|CIH program is 50:50, providing students with real-time experience in IH&R scenarios and hands-on practice with the latest tools, techniques, methodologies, and frameworks.

11) Lab Environment Simulates post-breach Environment

The lab environment simulates a real-time situation for incident handlers, and this experience can help in effectively dealing with incidents in organizations.

12) Covers Latest IH&R Tools/Platforms and Frameworks

The E|CIH course includes a library of tools, platforms, and frameworks across different operating platforms required by incident handlers and responders to effectively handle and respond to various organizational threats and incidents.

13) Covers Latest Real-time Case studies on Handling and Responding to Cybersecurity Incidents

These case studies are specific to incidents reported by organizations or users, including incident handling procedures, from the detection phase to recovery, as well as lessons learned.

Exam Details:

Exam Title:

EC-Council Certified Incident Handler

Exam Code:	Number of Questions:	Duration:
212-89	100	3 hours

Exam Availability:	Test Format:
ECC Exam Portal	Multiple Choice

Passing Score: Refer https://cert.eccouncil.org/faq.html

Training Details:

Training: 3 Days

Training Options:

iLearn (Self-Study)

This solution is an asynchronous, self-study environment in a video-streaming format.

iWeek (Live Online)

This solution is an online, live training course led by an instructor.

Training Partner (In Person)

This solution offers in-person training so that you can get the benefit of collaborating with your peers.

Job Roles Mapped to E|CIH:

1. Incident Handler
2. Incident Responder
3. Incident Response Consultant/Associate /Analyst/Engineer/ Specialist/ Expert/Manager
4. CSIRT Analyst/Engineer/Manager
5. Information Security Associate/Analyst/Engineer/Specialist/Manager
6. Cyber Defense Security Consultant/Associate/Analyst
7. IT Security Operations Center Analyst (SOC Analyst/Engineer)
8. Cyber Forensic Investigator/Consultant/Analyst/Manager
9. Digital Forensic Analyst
10. Cyber Risk Vulnerability Analyst/Manager
11. Cyber Intelligence Analyst and Cyber Security Threat Analyst/Specialist
12. Cyber Security Incident Response Team Lead
13. Penetration Tester

Who Can apply for E|CIH:

- Any mid-level to high-level cyber security professionals with a minimum of 3 years of experience
- Individuals from the information security profession and who want to enrich their skills and knowledge in the field of incident handling and response.
- Individuals interested in preventing cyber threats.

Top Tools, Playbooks and more in E|CIH course

Top 10 Popular or Latest Tools:

- Cyber Triage
- KeepNote
- IDA and OllyDbg
- Wireshark
- MxToolbox
- Rmail
- AlienVault OSSIM
- RdpGuard
- Nessus
- dotDefender
- MalwareBytes
- ManageEngine Endpoint Central

Top 5 Playbooks and Runbooks:

- DDoS Incident Response Playbook
- Phishing Incident Response Playbook
- Insider Threat Incident Response Playbook
- Ransomware Incident Response Playbook
- DDoS Incident Response Runbook

Top Latest Methodologies & Framework:

- DDoS Incident Response Playbook
- Phishing Incident Response Playbook
- Insider Threat Incident Response Playbook
- Ransomware Incident Response Playbook
- DDoS Incident Response Runbook

Top: Latest Templates, Checklists, and Toolkits:

- Digital Forensics eadiness Policy Document Template
- Incident Handling and Response Plan Template
- Incident Handling and Response Policy and Procedure Document Template
- Incident Handler Checklist
- Incident Responder Toolkit Requirements
- Forensics Investigative Analysis Report Recognition / Endorsement / Mapping

EC-Council

Building A Culture Of Security

About EC-Council

EC-Council invented the Certified Ethical Hacker. Founded in 2001 in response to 9/11, EC-Council's mission is to provide the training and certifications apprentice and experienced cyber security professionals need to keep corporations, government agencies, and others who employ them safe from attack.

Best known for its Certified Ethical Hacker program, EC-Council today offers 200 different training programs, certifications, and degrees in everything from Computer Forensic Investigation and Security Analysis to Threat Intelligence and Information Security. An ISO/IEC 17024 Accredited Organization recognized under the US Defense Department Directive 8140/8570 and many other authoritative cybersecurity bodies worldwide, the company has certified over 350,000 professionals across the globe. Trusted by seven of the Fortune 10, half of the Fortune 100, and the various agencies public and private across 140 nations, EC-Council is the gold standard in cybersecurity education and certification.

A truly global organization with a driving belief in bringing diversity, equity, and inclusion to the modern cybersecurity workforce, EC-Council maintains 11 offices in the U.S., the UK, India, Malaysia, Singapore, and Indonesia.

www.eccouncil.org