EC-Council

Prepare to Handle and Respond to Security Incidents

ECIH™
EC-Council Certified Incident Handler

EC-Council Certified Incident Handler v2

THE CRITICAL NATURE OF INCIDENT HANDLING READINESS

> An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster.
> **- Symantec**

Why Incident Handling Is a Must for Every Organization

Global Lack of Incident Response Planning

To identify a malicious attack	To contain and recover from an attack	Organizations do not have an Incident Response plan
214 days	77 days	76%

74% of the employers rate the difficulty in hiring their skilled IH & R personnel as **very high**.

Two of the Top 10 Cost Saving Measures in the case of a Data Breach

Average cost savings with trained security employees	Average cost savings with an Incident Response team
$9.30	$14 per record

IS YOUR ORGANIZATION READY TO HANDLE THE NEXT INCIDENT EFFECTIVELY AND EFFICIENTLY?

Prepare to Handle and Respond to Security Incidents

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

It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

LEARN REAL-WORLD INCIDENT HANDLING SKILLS

Following a rigorous development, which included a careful Job Task Analysis (JTA) related to incident handling and incident first responder jobs, EC-Council developed a highly interactive, comprehensive, standards-based, intensive 3-day training program and certification that provides a structured approach to learning real-world incident handling and response requirements.

NOT ONLY DETECT BUT MANAGE SECURITY INCIDENTS

Organizations are under constant attack and with the knowledge and skills found in the E|CIH program, professionals can now not only detect incidents, but also quickly manage and respond holistically to these incidents.

MAPS TO INDUSTRY FRAMEWORKS

Professionals interested in pursuing incident handling and response as a career require comprehensive training that not only imparts concepts but also allows them to experience real scenarios. The E|CIH program includes hands-on learning delivered through labs within the training program. True employability after earning a certification can only be achieved when the core of the curricula maps to and is compliant with government and industry-published incident and response frameworks.

METHOD DRIVEN PROGRAM

E|CIH is a method-driven program that uses a holistic approach to cover vast concepts concerning organizational incident handling and response from preparing and planning the incident handling response process to recovering organizational assets after a security incident. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

LEARN ALL STAGES IN INCIDENT HANDLING

This program addresses all the stages involved in incident handling and the response process to enhance your skills as an incident handler and responder, increasing your employability. This approach makes E|CIH one of the most comprehensive incident handling and response related certifications on the market today.

THINK GLOBAL EMPLOYABILITY

The skills taught in EC-Council's E|CIH program are desired by cybersecurity professionals from around the world and is respected by employers.

> “Organizations are looking for professional incident handlers and response personnel who can prepare security policies and plans to tackle incidents with efficacy in time-constrained scenarios in order to reduce the impact of incidents. – ***Jay Bavisi, President of EC-Council Group***”

E|CIH IS ONE OF THE BEST INCIDENT HANDLING PROGRAMS

Gain Access to new, advanced labs:
The E|CIH program comes with access to over 50 labs, 800 tools, and 4 OSs!

Compliant with Major Industry Frameworks:
100% Complaint with the NICE 2.0 Framework AND CREST Framework.

Comprehensive Templates Available:
A large array of templates, checklists, and cheat sheets.

E|CIH also Covers a Huge Variety of Security Incidents

Malware Incidents Malware detections targeting businesses increased by 270 percent	**Cloud Security Incidents** 681 million cyberattacks were launched against cloud customers in 2018	**Email Security Incidents** 9 out of 10 infection attempts throughout the year were spam email
Web App Security Incidents 3.6% of websites suffered web application attacks	**Network Security Incidents** 21.2% of devices were exposed to network threats in the 1st month, rising to 43.7% after 4 months	**Insider Threats** $8.76 million is the avg yearly cost of insider threats

Source: Malwarebytes Annual "State of Malware" Report | Armor | F-Secure | Automated Code Analysis: Web Application Vulnerabilities in 2017 | ResearchGate | 018 Cost of Insider Threats: Global Organizations by Ponemon Institute

E|CIH Target Audience

There is no organization that is truly safe from a cyberattack. An Incident Manager with the proper incident handling skills can help reduce the impact of a breach.

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.

Suggested Course Duration

3 Days	24 hours total class time

Certification:

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 (ATC) 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.

Exam Details

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

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).

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.

Clause: Age Requirements and Policies Concerning Minors

The age requirement for attending the training or the exam is restricted to any candidate that is permitted by his/her country of origin/residency.

If the candidate is under the legal age as permitted by his/her country of origin/residency, they are not eligible to attend the official training or eligible to attempt the certification exam unless they provide the accredited training center/EC-Council a written consent/indemnity of their parent/legal guardian and a supporting letter from their institution of higher learning. Only candidates from a nationally accredited institution of higher learning shall be considered.

E|CIH Is Built to Remediate Modern Cyber Threats

1. 100% compliant with NICE Special Publication 800-181 Cybersecurity Workforce Framework

E|CIH maps 100 percent to the NICE framework under the category "Protect and Defend (PR)" and the specialty "Incident Response (CIR)".

NICE stands for National Initiative for Cybersecurity Education (NICE). The Incident Response (CIR) specialty area deals with investigating, analyzing, and responding to cyber incidents within the network environment or enclave. This area enables incident responders to handle crises within the pertinent domain and mitigate potential threats. CIRs evaluate the effectiveness of and improvements to existing practices in any organization, which in turn leads to maximizing the survival of life, preservation of property, and information security.

2. 100% compliant with CREST frameworks

E|CIH maps 100 percent to the CREST Certified Incident Manager (CCIM) framework. It is focused on maintaining an appropriate standard for incident response that determines the path of investigation based on considerable real-world incident handling experience and the pertinent information available. E|CIH maps to CREST Certified level examinations which are designed to set the benchmark for senior incident handlers. By gaining the E|CIH certification, individuals are globally recognized as certified incident handlers.

3. Engineered based on a comprehensive industry-wide job task analysis

E|CIH was developed by subject matter experts and practitioners in the incident handling and response domain by performing a rigorous, industry-wide job task analysis. The program was designed after performing an intensive analysis of all possible combinations of task, knowledge, skill, and ability (TKSA) from relevant job postings of various multinational companies across the globe. This comprehensive mapping and analysis synchronize the E|CIH program to that of the industry-wide incident handler job requirement criteria, opening the gate of opportunities to E|CIH certification holders into various multinational organizations.

4. Focuses on a structured approach to perform the incident handling and response process

The E|CIH program focuses on a structured approach for performing the incident handling and response (IH&R) process. The IH&R process includes stages like 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 incident responders in knowing how to respond to various types of security incidents.

5. Focus on developing skills in handling different types of cybersecurity incidents

This program demonstrates the complete IH&R process in a systematic way for various types of cybersecurity incidents including malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents. Covering the end-to-end IH&R process for all these types of security incidents makes the E|CIH an outstanding program for aspiring and current incident handlers.

6. Emphasis on forensic readiness and first response procedures

Every organization must be well prepared to respond to any security incident. It is crucial for an incident handler to respond quickly, effectively, and efficiently to handle, contain, and mitigate the incident. This first response requires a strict and precise set of rules that an incident responder must follow to deal with the incident appropriately. If there is any lack of forensic readiness or first response process, the incident can cause disastrous damage to the organization. The E|CIH program focuses on how an organization should prepare to tackle any sort of cyber incidents along with the steps that a first responder should perform in recording or dealing with the incident.

7. Hands-on program

E|CIH comes integrated with labs so that students can practice the skills they learn. In fact, more than 40 percent of class time is dedicated to practical learning through EC-Council labs. The theory to practice ratio for the E|CIH program is 60:40, providing students with a hands-on experience using the latest incident handling and response tools, techniques, methodologies, and frameworks across different operating platforms that are required by incident handlers to effectively handle and respond to various organizational threats and incidents.

8. Lab environment simulates a real-time environment

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. The lab environment simulates a real-time situation for incident handlers, giving students skills they can apply immediately to protect their respective organizations.

9. Emphasis on incident handling standards and laws

Incident handling professionals are bound to operate under certain well-defined rules and regulations. The E|CIH program covers various cybersecurity and IH&R standards, laws, and policies, enabling incident handling professionals to align their incident handling process in accordance with industry standards.

10. Huge inventory of incident handling templates, checklists, and cheat sheets

The program accompanies more than a hundred incident handling templates, checklists, and cheat sheets for effective incident response planning, which helps in dealing with an incident effectively. This vast collection of documentation material enables an incident handler to implement required incident related documentation in their organization. The templates also help incident handlers to draft comprehensive reports based on the target audience and incidents.

Course Outline

- Introduction to Incident Handling and Response
- Incident Handling and Response Process
- Forensic Readiness and First Response
- Handling and Responding to Malware Incidents
- Handling and Responding to Email Security Incidents
- Handling and Responding to Network Security Incidents
- Handling and Responding to Web Application Security Incidents
- Handling and Responding to Cloud Security Incidents
- Handling and Responding to Insider Threats

Learning Objectives of the E|CIH Program

- 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

EC-Council
www.eccouncil.org