EC-Council ECIH: Certified Incident Handler

Category: Networking & Security | **Vendor:** EC-Council

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Certified Incident Handler (ECIH)
Related Exam:	ECIH

Course Overview

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.

ECIH 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.

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

About This Course

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.

ECIH 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.

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

Prerequisites & Entry Requirements

General Prerequisites:

To qualify for the E|CIH program, one must have at least 3 years of experience working as a cyber security professional.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Key issues plaguing the information security world
- Various types of cybersecurity threats, attack vectors, threat actors, and their motives, goals, and objectives of cybersecurity 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)
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- 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 systemic way (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, insider threat-related incidents, and endpoint security incidents)

Detailed Course Outline

- Module 01: Introduction to Incident Handling and Response
- Module 02: Incident Handling and Response Process
- Module 03: First Response
- Module 04: Handling and Responding to Malware Incidents
- Module 05: Handling and Responding to Emails Security Incidents
- Module 06: Handling and Responding to Network Security Incidents

- Module 07: Handling and Responding to Web Application Security Incidents
- Module 08: Handling and Responding to Cloud Security Incidents
- Module 09: Handling and Responding to Insider Threats
- Module 10: Handling and Responding to Endpoint Security Incidents

□□ Certification Path

Certified Incident Handler (ECIH)

Exam: ECIH

Skills You Will Learn:

- Key issues plaguing the information security world
- Various types of cybersecurity threats, attack vectors, threat actors, and their motives, goals, and objectives of cybersecurity 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)
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- 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 systemic way (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, insider threat-related incidents, and endpoint security incidents)

Frequently Asked Questions

Q: What delivery options are available for EC-Council ECIH: Certified Incident Handler?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The EC-Council ECIH: Certified Incident Handler course helps prepare you for the Certified Incident Handler (ECIH) certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the ECIH official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 3-day EC-Council ECIH: Certified Incident Handler course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the EC-Council ECIH: Certified Incident Handler training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for EC-Council ECIH: Certified Incident Handler?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council ECIH: Certified Incident Handler. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: EC-Council Certified Incident Handler, Specialist, ECIH

Q: Why choose Nexus Human for EC-Council ECIH: Certified Incident Handler?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council ECIH: Certified Incident Handler training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)