

# EC-Council Certified Incident Handler ECIH v3

## Zertifizierung

Trainings-ID: ECIH

[Zum Seminar →](#)

### Das nehmen Sie mit

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 ECIH one of the most comprehensive incident handling and response related certifications on the market today. The skills taught in EC-Council's ECIH program are desired by cybersecurity professionals from around the world and are respected by employers.

The Purpose of ECIH is:

- to enable individuals and organizations with the ability to handle and respond to different types of cybersecurity incidents in a systematic way
- to ensure that organization can identify, contain, and recover from an attack
- to reinstate regular operations of the organization as early as possible and mitigate the negative impact on the business operations
- to be able to draft security policies with efficacy and ensure that the quality of services is maintained at the agreed levels
- to minimize the loss and after-effects breach of the incident
- for individuals: to enhance skills on incident handling and boost their employability

Learning Objectives of ECIH Program:

- Understand the key issues plaguing the information security world
- 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

Sie haben Fragen? ☎ +43 1 533 1777-0 ✉ [info@etc.at](mailto:info@etc.at) 📍 Modecenterstraße 22, 1030 Wien

security incidents, cloud security incidents, and insider threat-related incidents

- 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 antiforensics techniques used by attackers to find cybersecurity incident cover-ups

## Zielgruppen

The incident handling skills taught in ECIH 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

### **Wichtige Informationen**

Dieses Training bereitet auf die Prüfung **EC-Council Certified Incident Handler** vor.

Testfragen: 100 Testdauer: 3 Stunden Testform: Multiple Choice

Das Examen ist im Trainingspreis inkludiert!

## Termine & Optionen

Datum	Dauer	Ort	Angebot	Preis
29.07.2024-31.07.2024	3 Tage		Preis (Online)	€ 2.950,-
30.09.2024-02.10.2024	3 Tage		Preis (Online)	€ 2.950,-
27.11.2024-29.11.2024	3 Tage		Preis (Online)	€ 2.950,-
03.02.2025-05.02.2025	3 Tage		Preis (Online)	€ 2.950,-

Sie haben Fragen?  +43 1 533 1777-0  [info@etc.at](mailto:info@etc.at)  Modecenterstraße 22, 1030 Wien