EC-Council Certified Incident Handler ECIH v3 Zertifizierung

Trainings-ID: ECIH

Zum Seminar →

Das nehmen Sie mit

This programm addresses all the stages involved in incident handling and the response process to enhances 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. The skills taught in EC-Council ´s E|CIH program are desired by cybersecurity professionals from around the world and is respected by employers.

The Purpose of E|CIH 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 possbile and mitigate the negative impact on the business opeerations
- to be able to draft security policies with efficacy and ensure that the quality of services is mantained at the agreeed 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 E|CIH 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

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

- Learn to combat different types fo 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 fundamentsl of vunlerability 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 acqusition, volatile and static evidence collection, and evidence analysis
- Understand antiforensics techniques used by attackers to find cyberscurity incident cover-ups

Zielgruppen

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/EngineersSystem 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
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,-