EC-Council Certified Incident Handler (ECIH)

Description

Develop essential incident management skills

The EC-Council Certified Incident Handler (ECIH) training is designed for IT security professionals looking to enhance their ability to manage security incidents. This comprehensive program covers all critical stages of incident management, from preparation to responding to cyber threats and recovering assets after an attack.

This course enables you to acquire the necessary skills to respond quickly and effectively to incidents such as malware, network attacks, or internal threats. The program is globally recognized and highly valued by employers seeking experts to protect their information systems.

Reference
ECIH
Course Content
Module 1: Introduction to Incident Handling and Response

- Definition and importance of incident management
- Introduction to incident response

Module 2: Incident Handling and Response Process

- Key steps in incident management
- Incident methodologies and frameworks

Module 3: First Response

- Incident identification and triage
- Evidence collection procedures

Module 4: Handling and Responding to Malware Incidents

- Malware identification and isolation
- Malware response measures

Module 5: Handling and Responding to Email Security Incidents

- Types of email threats
- Responding to email-based attacks

Module 6: Handling and Responding to Network Security Incidents

- Network threat monitoring and detection
- Responding to network attacks

Module 7: Handling and Responding to Web Application Security Incidents

- Common web application vulnerabilities
- Responding to web application attacks

Module 8: Handling and Responding to Cloud Security Incidents

- Threats specific to cloud environments
- Responding to cloud-based incidents

Module 9: Handling and Responding to Insider Threats

- Identifying insider threats
- Responding to insider-related incidents

Module 10: Handling and Responding to Endpoint Security Incidents

- Monitoring endpoint devices
- Responding to endpoint incidents

Documentation

- Digital course material included

Exam

- This course prepares to the EC-Council Certified Incident Handler certification
- In order to receive the EC-Council Certified Incident Handler, learners must pass two exams: 212-89.
- Number of questions: 100
- Duration: 3 hours
- If you wish to take this exam, please contact our secretariat who will let you know the cost of the exam and will take care of all the necessary administrative procedures for you.

Participant profiles

- IT Security Managers
- SOC Analysts
- Cybersecurity Consultants
- Network Administrators
- IT professionals seeking specialization in incident management

Prerequisites

- Basic understanding of cybersecurity concepts
- Fundamental knowledge of incident management
- Experience with operating systems and networks

- Knowledge of email and web application security

Objectives

- Learn to respond quickly to security incidents
- Master handling malware and network attacks
- Effectively address insider threats
- Understand and apply incident management frameworks
- Analyze and manage incidents in cloud environments
- Apply incident management practices to web applications

Description
EC-Council Certified Incident Handler (ECIH) training
Niveau
Intermédiaire
Classroom Registration Price (CHF)
3700
Virtual Classroom Registration Price (CHF)
3550
Duration (in Days)
3