ECIH – EC-Council Certified Incident Handle

EC-Council

Live Training (também disponível em presencial)

Com certificação

- **Localidade:**
- **Data:** 21 Sep 2026
- **Preço:** 2100 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Laboral das 09h00 - 17h00
- **Nível:** Avançado
- **Duração:** 24h

Sobre o curso

This program 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 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.

How E|CIH Benefits Individuals

- **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 the CREST Framework
- **Comprehensive Templates Available:** A large array of templates, check lists, and cheat sheets

Destinatários

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.

Objetivos

Learning Objectives of 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

---

Condições

O exame EC-Council incluido no valor do curso deve ser obrigatoriamente realizado presencialmente, num dos centros de Exames GALILEU/Rumos.

Caso não tenha disponibilidade ou não pretenda realizar o exame de forma presencial e prefira uma solução remota acresce uma taxa de 89€ + IVA ao valor do curso.

Metodologia

Prepare to Handle and Respond to Security Incidents:

Organizations are under constant attacks 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.

E|CIH is a highly interactive, comprehensive, high-standard, intensive 3-day training program that teaches information security professionals to behave professional incident handlers and gain a distinct identity than other security professionals. The program teaches all the necessary components of incident handling, containment and reinstating the IT infrastructure.

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 (ATCs) 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.

Programa

- 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