EC-Council Certified Incident Handler (ECIH) + Exam voucher

Duration: 2 Days **Course Code: ECIH** **Version: 3.0** **Delivery Method: Virtual Learning**

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 incidents. Students will learn the handling of various types of incidents, risk assessment methodologies, as well as laws and policies related to incident handling.
After attending the course, students will be able to create IH&R policies and deal with different types of security incidents such as malware, email security, network security, web application security, cloud security, and insider threat-related incidents.
The E|CIH (EC-Council Certified Incident Handler) 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.
The E|CIH is a method-driven course that provides a holistic approach covering concepts related to organizational IH&R, from preparing and planning the incident handling response process to recovering organizational assets from the impact of security incidents. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.
With over 95 advanced labs, 800 tools covered, and exposure to incident handling activities on many different operating systems, E|CIH provides a well-rounded and tactical approach to planning for and dealing with cyber incidents.
The E|CIH program addresses all stages involved in the IH&R process, and this attention toward a realistic and futuristic approach makes E|CIH one of the most comprehensive IH&R-related certifications in the market today.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

- Mid-level to high-level cybersecurity professionals with a minimum of 3 years of experience
- Individuals from the information security profession who want to enrich their skills and knowledge in incident handling and response
- Individuals interested in preventing cyber threats

Objectives:

- **What You Learn from E|CIH?**
- Key issues plaguing the information security world
- Various types of cybersecurity threats, attack vectors, threat actors, and their motives, goals, and objectives
- 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)
- Fundamentals of incident management (information security incidents, signs and costs of an incident, incident handling and response, and incident response automation and orchestration)
- Incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
- Steps involved in planning an 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 procedures (evidence collection, documentation, preservation, packaging, and transportation)
- Handling and responding to different types of cybersecurity incidents (malware, email security, network security, web application security, cloud security, insider threats, and endpoint security incidents)

Prerequisites:

Attendees should meet the following prerequisites:

- It is recommended that you have at least 1 year of experience in the cybersecurity domain in order to maximize course outcomes.

Testing and Certification

Recommended as preparation for the following exam:

- 212-89 - EC-Council Certified Incident Handler

Examination

Exam Availability
ECC Exam Portal

Number of Questions
100

Duration
3 Hours

Test Format
Multiple Choice

Content:

MODULE 01: INTRODUCTION TO INCIDENT HANDLING AND RESPONSE

- Information security threats and attack vectors
- Attack and defense frameworks
- Information security concepts
- Information security incidents
- Incident management process
- Incident response automation and orchestration
- Incident handling and response best practices
- Standards related to incident handling and response
- Cybersecurity frameworks
- Incident handling laws and legal compliance

MODULE 02: INCIDENT HANDLING AND RESPONSE PROCESS

- Incident handling and response (IH;R) process
- Preparation for incident handling and response
- Incident recording and assignment
- Incident triage
- Notification process
- Containment process
- Evidence gathering and forensic analysis
- Eradication process
- Recovery process
- Post-incident activities
- Information sharing activities

MODULE 03: FIRST RESPONSE

- Concept of first response
- Securing and documenting the crime scene
- Collecting evidence at the crime scene
- Preserving, packaging, and transporting evidence

MODULE 04: HANDLING AND RESPONDING TO MALWARE INCIDENTS

- Malware incident handling
- Preparation for malware incidents
- Detection of malware incidents
- Containment of malware incidents
- Malware analysis
- Eradication of malware incidents
- Recovery after malware incidents
- Malware incident case study
- Best practices against malware incidents

MODULE 05: HANDLING AND RESPONDING TO EMAIL SECURITY INCIDENTS

- Email security incidents
- Preparation for email security incidents
- Detection and containment of email security incidents
- Analysis of email security incidents
- Eradication of email security incidents
- Recovery after email security incidents
- Email security incident case study
- Best practices against email security incidents

MODULE 06: HANDLING AND RESPONDING TO NETWORK SECURITY INCIDENTS

- Network security incident handling
- Preparation for network security incidents
- Detection and validation of network security incidents
- Unauthorized access incidents
- Inappropriate usage incidents
- Denial-of-service incidents
- Wireless network security incidents
- Network security incident case study
- Best practices against network security incidents

MODULE 07: HANDLING AND RESPONDING TO WEB APPLICATION SECURITY INCIDENTS

- Web application incident handling
- Preparation for web application security incidents
- Detection and containment of web application security incidents
- Analysis of web application security incidents
- Eradication of web application security incidents
- Recovery after web application security incidents
- Web application incident case study
- Best practices for securing web applications

MODULE 08: HANDLING AND RESPONDING TO CLOUD SECURITY INCIDENTS

- Cloud security incident handling
- Steps involved in handling cloud security incidents
- Azure security incident handling
- AWS security incident handling
- Google Cloud security incident handling
- Cloud security incident case study
- Best practices against cloud security incidents

MODULE 09: HANDLING AND RESPONDING TO INSIDER THREATS

- Insider threat handling
- Preparation for insider threats
- Detection and containment of insider threats
- Analysis of insider threats
- Eradication of insider threats
- Recovery after insider attacks
- Insider threat case study
- Best practices against insider threats

MODULE 10: HANDLING AND RESPONDING TO ENDPOINT SECURITY INCIDENTS

- Endpoint security incident handling
- Mobile-based security incidents
- IoT-based security incidents
- OT-based security incidents
- Endpoint security incident case study

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo