EC-COUNCIL CERTIFIED INCIDENT HANDLER

SaniSoft
information technologies

Well Trained People,
Better Served Customers.

COURSE OVERVIEW

he EC-Council Certified Incident Handler (ECIH) program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and various laws and policies related to incident handling. After attending this course, they will be able to create incident handling and response policies as well as deal with various types of computer security incidents.

The IT incident management training program will enable students to be proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats. In addition, students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, incident management training methods, and incident recovery techniques in detail. The ECIH certification will provide professionals greater industry acceptance as the seasoned incident handler.

DURATION: 16 HOURS | EXAM CODE: 212-89

COURSE PREREQUISITES

- System / Network Administration experience is essential

COURSE OBJECTIVE

The age requirement for attending the training or attempting the exam is restricted to any candidate that is at least 18 years old.

If the candidate is under the age of 18, they are not eligible to attend the official training or eligible to attempt the certification exam unless they provide the accredited training center (ATC) or EC-Council a written consent of their parent or their legal guardian and a supporting letter from their institution of higher learning. Only applicants from nationally accredited institutions of higher learning shall be considered.

Disclaimer

EC-Council reserves the right to impose additional restriction to comply with the policy. Failure to act in accordance with this clause shall render the authorized training center (ATC) in violation of their agreement with EC-Council. EC-Council reserves the right to revoke the certification of any person in breach of this requirement.

COURSE OUTLINE

- Module 01: Introduction to Incident Handling and Response
- Module 02: Incident Handling and Response Process
- Module 03: Forensic Readiness and First Response
- Module 04: Handling and Responding to Malware Incidents
- Module 05: Handling and Responding to Email Security Incidents
- Module 06: Handling and Responding to Network Security Incidents
- Module 07: Handling and Responding to Web Application Security Incidents
- Module 08: Handling and Responding to Cloud Security Incidents
- Module 09: Handling and Responding to Insider Threats

TARGET AUDIENCE

Anyone involved in the selection and implementation of VPN's or digital certificates should attend this course. Without understanding the cryptography at some depth, people are limited to following marketing hype. Understanding the actual cryptography allows you to know which one to select. A person successfully completing this course will be able to select the encryption standard that is most beneficial to their organization and understand how to effectively deploy that technology.

SaniSoft
information technologies

410, AL-DANA CENTER, AL MAKTOUM ROAD DEIRA, DUBAI, UAE

+971 55 3575426 ☎ +971 4 2238786 ✉ training@sanisoft-it.com