training code: ECIH / ENG AA 3d / EN

Certified Incident Handler

Authorized EC-Council training - ECIH v2 - EC-Council Certified Incident Handler

It is delivered in the form of a lecture and practical workshops.

The EC-Council Certified Incident Handler v2 (E|CIH) training is a comprehensive, specialist-level program that provides the knowledge and skills organizations need to successfully deal with IT security incidents. The course covers the basic principles and techniques of detecting and responding to current and emerging computer security threats. After completing the training, students will have the opportunity to register for the ECIH exam. The ECIH certification is highly valued and helps increase the chances of employment as cybersecurity specialists around the world.

Purpose of the training

The is designed for:

- network administrators,
- people responsible for IT infrastructure,
- system engineers,
- VA auditors (Vulnerability Assessment),
- IT risk managers,
- security engineers,
- security analysts,
- CFI (Cyber Forensic Investigators) specialists,

- SOC employees
- IT employees planning to increase the level of IT security of their organization.

For people who are not specialists in the field of IT security, the training may be too intensive, but it will help to increase awareness of event handling and appropriate response to threats.
IT security specialists, security auditors and analysts as well as pentesters will be able to consolidate, systematize or update their knowledge.

Benefits of completing the training

Organizations are the target of constant attacks, and thanks to the knowledge and skills acquired during the E | CIH course, experts will not only be able to detect incidents, but also manage them immediately and respond to them as a whole. The training program teaches proficient handling and reaction to events such as network security breaches, malware infections or threats related to internal attacks. In addition, students learn the basics of computer forensics, its role in handling events and reacting to them. The course also covers the work of incident management and response teams, and introduces techniques to get your business back up and running. Students will learn how to deal with security breach situations, learn about risk assessment methods and various regulations related to incident handling. Upon completion of this course, participants will be able to create a consistent and thoughtful event handling policy.
The training participants will understand the incident handling and response processes and:

- Apply first reaction procedures and prepare the "ground" for computer forensics
- handle incidents and respond adequately
- handle malware events
- respond to incidents related to the security of e-mail and internet applications
- handle and respond to network security breaches
- deal with various cloud security incidents
- detect and respond to internal threats

Examination method

Note: If the participant would like to take the ECIH exam online (from anywhere) from the so-called with remote protection, there is an additional fee of USD 100 net. The cost includes hiring an exam supervisor (the so-called proctor). We purchase individually on the vendor website:
https://store.eccouncil.org/product/voucher-upgrade-rps-to-vue/

Exam description

- Exam title: EC-Council Certified Incident Handler
- Number of questions: 100
- Duration: 3 hours
- Format: multiple choice questions

Expected Listener Preparation

- Good knowledge of Windows and Linux operating systems,
- Knowledge of protocols and network services required.
- At least two years of cybersecurity experience is recommended.

Training Language

- Training: English
- Materials: English

Duration

3 days / 21 hours

Training agenda

1. Introduction to Incident Handling and Response
2. Incident Handling and Response Process
3. Forensic Readiness and First Response
4. Handling and Responding to Malware Incidents
5. Handling and Responding to Email Security Incidents
6. Handling and Responding to Network Security Incidents
7. Handling and Responding to Web Application Security Incidents

8. Handling and Responding to Cloud Security Incidents
9. Handling and Responding to Insider Threats