ECIH – EC-Council Certified Incident Handler v2

Kestus: 24 academic hours

Vana-Lõuna 39/1, Tallinn

Vaata kõiki toimumiskuupäevi

The EC-Council Certified Incident Handler 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 policy related to incident handling. After attending the course, they will be able to create incident handling and response policies and deal with various types of computer security incidents. The comprehensive training program will make students proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats.

In addition, the students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, incident reporting methods, and incident recovery techniques in detail.

The E|CIH certification will provide professionals greater industry acceptance as the seasoned incident handler.

Certification

The ECIH 212-89 exam will be conducted on the last day of training. Students need to pass the online exam to receive the ECIH certification.

Target audience:

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

The results of the training

- 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

Prerequisites to the course (recommended): 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.

Additional information:

http://www.eccouncil.org/Certification/ec-council-certified-incident-handler

Training Principles:

- 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

Length*: 24academic hours*

The prerequisite for issuing the certificate is full participation in training.

The training price also includes:
teaching materials;
a trainer's consultation on the topics learned by e-mail after the training;
certificate;
exam.

The exam can be taken at our Exam Centre

As an added value, we offer:
free parking;
hot drinks with cookies;
fresh fruits;
lunch on each training day.

LISAINFO

Osalemise tingimused
Registreerudes e-poe, e-kirja või telefoni teel, saadame Teile arve ja täpsema info osalemise kohta.
Üks nädal enne koolitust saadame Teile e-kirjaga meenutuse osalemise infoga.

Koolitusel osalemine on nimeline, kuid saate osalejat tasuta muuta kuni koolitusprogrammi alguseni. Kui Te ei saa mingil põhjusel osaleda, palun andke sellest kindlasti teada e-posti aadressil info@koolitus.ee või telefonil 618 1727. Kui teatate koolitusel mitteosalemisest kuni nädal enne algust, pakume mõnd muud samaväärset koolitust samal hooajal või tagastame 100% tasutud koolituse maksumusest. Mitteosalemisest vähemalt 3 tööpäeva varem teatades, tagastame 50%. Muul juhul kuulub arve tasumisele. Raha tagastame etteantud summas juhul, kui pole tehtud koolituse korraldamisega seotud kulutusi (ostetud õppematerjale jms.). Koolitusele mitteilmumisel, sellest mitteteatamisel või koolituse poolelijätmisel õppetasu ei

tagastata.

IT Koolitus on Eesti Töötukassa koolituskaardi koostööpartner. Tutvuge koolituskaardi infoga SIIN.
Täpsema info saamiseks võtke meiega ühendust telefonil 618 1727 või info@koolitus.ee.