ECIHv3

Certified Incident Handler

The EC-Council Certified Incident Handler (ECIH) program is designed to provide the fundamental skills to manage and respond to security incidents in information systems, while preparing you to pass the ECIH exam. The course provides incident response training by covering various fundamental principles and techniques for detecting and responding to current and emerging computer security threats. After attending the course, you will be able to create incident handling and response policies and deal with different types of security incidents.

The ECIH certification fully meets the requirements of the NICE 2.0 and CREST frameworks and is internationally recognized. This provides you with valuable confirmation of your knowledge of incident management. In this practice-oriented intensive course, you will learn how to recognize, control and resolve cyber attacks.

Course Contents
- Introduction to Incident Handling and Response
- Incident Handling and Response Process
- 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
- Handling and Responding to Endpoint Security Incidents

Target Group
- All mid to senior level cyber security professionals with at least 3 years of experience
- Information security professionals looking to expand their skills and knowledge in incident handling and response
- Persons interested in preventing cyber threats

Prerequisites
- At least one year of experience in the administration of Windows/Unix/Linux systems
- Understanding of common network and security services

Course Target
ECIH V3 certification (EC-Council Certified Incident Handler)

This Course in the Web

You can find the up-to-date information and options for ordering under the following link: www.experteach-training.com/go/**ECCI**

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training		Prices, excl. of V.A.T.
Classes in Germany	**3 Days**	**€ 2,950**
Online Training	**3 Days**	**€ 2,950**
Date/course venue	Course language German	
08/12-10/12/25 ON Online		

Status 05/07/2025

ECIHv3

EC-Council

ExperTeach

Table of Contents

ECIHv3 – Certified Incident Handler

Introduction to Incident Handling and Response
Understand Information Security Threats and Attack Vectors
Explain Various Attack and Defence Frameworks
Understand Information Security Concepts
Understand Information Security Incidents
Understand the Incident Management Process
Understand Incident Response Automation and Orchestration
Describe Various Incident Handling and Response Best Practices
Explain Various Standards Related to Incident Handling and Response
Explain Various Cybersecurity Frameworks
Understand Incident Handling Laws and Legal Compliance

Incident Handling and Response Process
Understand Incident Handling and Response (IH&R) Process
Explain Preparation Steps for Incident Handling and Response
Understand Incident Recording and Assignment
Understand Incident Triage
Explain the Process of Notification
Understand the Process of Containment
Describe Evidence Gathering and Forensics Analysis
Explain the Process of Eradication
Understand the Process of Recovery
Describe Various Post-Incident Activities
Explain the Importance of Information Sharing Activities

First Response
Explain the Concept of First Response
Understand the Process of Securing and Documenting the Crime Scene
Understand the Process of Collecting Evidence at the Crime Scene
Explain the Process for Preserving, Packaging, and Transporting Evidence

Handling and Responding to Malware Incidents
Understand the Handling of Malware Incidents
Explain Preparation for Handling Malware Incidents
Understand Detection of Malware Incidents
Explain Containment of Malware Incidents
Describe How to Perform Malware Analysis
Understand Eradication of Malware Incidents
Explain Recovery after Malware Incidents
Understand the Handling of Malware Incidents - Case Study
Describe Best Practices against Malware Incidents

Handling and Responding to Email Security Incidents
Understand Email Security Incidents
Explain Preparation Steps for Handling Email Security Incidents
Understand Detection and Containment of Email Security Incidents
Understand Analysis of Email Security Incidents
Explain Eradication of Email Security Incidents
Understand the Process of Recovery after Email Security Incidents
Understand the Handling of Email Security Incidents - Case Study
Explain Best Practices against Email Security Incidents

Handling and Responding to Network Security Incidents
Understand the Handling of Network Security Incidents
Prepare to Handle Network Security Incidents
Understand Detection and Validation of Network Security Incidents
Understand the Handling of Unauthorized Access Incidents
Understand the Handling of Inappropriate Usage Incidents
Understand the Handling of Denial-of-Service Incidents
Understand the Handling of Wireless Network Security Incidents
Understand the Handling of Network Security Incidents - Case Study
Describe Best Practices against Network Security Incidents

Handling and Responding to Web Application Security Incidents
Understand the Handling of Web Application Incidents
Explain Preparation for Handling Web Application Security Incidents
Understand Detection and Containment of Web Application Security Incidents
Explain Analysis of Web Application Security Incidents
Understand Eradication of Web Application Security Incidents
Explain Recovery after Web Application Security Incidents
Understand the Handling of Web Application Security Incidents - Case Study
Describe Best Practices for Securing Web Applications

Handling and Responding to Cloud Security Incidents
Understand the Handling of Cloud Security Incidents
Explain Various Steps Involved in Handling Cloud Security Incidents
Understand How to Handle Azure Security Incidents
Understand How to Handle AWS Security Incidents
Understand How to Handle Google Cloud Security Incidents
Understand the Handling of Cloud Security Incidents - Case Study
Explain Best Practices against Cloud Security Incidents

Handling and Responding to Insider Threats
Understand the Handling of Insider Threats
Explain Preparation Steps for Handling Insider Threats
Understand Detection and Containment of Insider Threats
Explain Analysis of Insider Threats
Understand Eradication of Insider Threats
Understand the Process of Recovery after Insider Attacks
Understand the Handling of Insider Threats - Case Study
Describe Best Practices against Insider Threats

Handling and Responding to Endpoint Security Incidents
Understand the Handling of Endpoint Security Incidents
Explain the Handling of Mobile-based Security Incidents
Explain the Handling of IoT-based Security Incidents
Explain the Handling of OT-based Security Incidents
Understand the Handling of Endpoint Security Incidents - Case Study

ExperTeach Benelux B.V.
Ceresstraat 1· 4811 CA Breda· Phone: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach-training.com