



# ECIHv3

## Certified Incident Handler

Das EC-Council Certified Incident Handler (ECIH) Programm ist darauf ausgelegt, die grundlegenden Fähigkeiten zu vermitteln, um Sicherheitsvorfälle in Informationssystemen zu bewältigen und darauf zu reagieren, und bereitet Sie gleichzeitig darauf vor, die ECIH-Prüfung zu bestehen. Der Kurs bietet Schulungen zur Vorfallreaktion, indem er verschiedene grundlegende Prinzipien und Techniken zur Erkennung und Reaktion auf aktuelle und aufkommende Bedrohungen der Computersicherheit behandelt. Nach der Teilnahme am Kurs werden Sie in der Lage sein, Richtlinien zur Handhabung und Reaktion auf Vorfälle zu erstellen und mit verschiedenen Arten von Sicherheitsvorfällen umzugehen.

Die ECIH-Zertifizierung erfüllt vollständig die Anforderungen der NICE 2.0- und CREST-Frameworks und ist international anerkannt. Damit erhalten Sie eine wertvolle Bestätigung Ihrer Kenntnisse im Incident Management. In diesem praxisorientierten Intensivkurs lernen Sie, wie Sie Cyberangriffe erkennen, steuern und beheben können.

### Kursinhalt

- 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

### Zielgruppe

- Alle Cyber-Sicherheitsfachleute auf mittlerer bis hoher Ebene mit mindestens 3 Jahren Erfahrung
- Personen aus dem Bereich der Informationssicherheit, die ihre Fähigkeiten und Kenntnisse im Bereich Incident Handling und Response erweitern möchten
- Personen, die daran interessiert sind, Cyber-Bedrohungen zu verhindern

### Voraussetzungen

- Mindestens ein Jahr Erfahrung in der Verwaltung von Windows/Unix/Linux Systemen
- Verständnis von gängigen Netzwerk und Security Services

### Kursziel

ECIH V3-Zertifizierung (EC-Council Certified Incident Handler)

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.at/go/ECCI](http://www.experteach.at/go/ECCI)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

ECIHv3

Stand 24.01.2025

Training		Preise zzgl. MwSt.
Termine in Österreich	3 Tage	€ 2.950,-
Online Training	3 Tage	€ 2.950,-
Termin/Kursort	Kurssprache Deutsch	
02.06.-04.06.25	08.12.-10.12.25	Online

EC-Council



EXPERTeach



# Inhaltsverzeichnis

## 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

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

### 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

