+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 03/12/2026

Sign up

EC-Council CIH™ Certification Training

3 days (21 hours)

Overview

The EC-Council CIH™ training prepares you to conduct end-to-end digital investigations: collection, analysis, and reporting. It is designed for security incidents, fraud cases, or legal disputes requiring admissible evidence.

You will learn to apply a rigorous forensic methodology: scene preservation, chain of custody, reliable acquisition, analysis, and reporting. The goal is to produce defensible results while minimizing bias and adhering to legal and organizational constraints.

Our training takes a decidedly hands-on approach: guided workshops, tool demos, realistic mini-cases (workstations, system artifacts, network traces). Deliverables include incident response checklists, a report template, and reusable acquisition/triage procedures.

Objectives

- Structure an investigation according to a forensic methodology.
- Preserve and document evidence (chain of custody).
- Perform secure acquisitions and triage.
- Analyze relevant system artifacts and logs.
- Write a clear, reproducible, and actionable report.

Target Audience

- SOC/CSIRT analysts
- System and network administrators
- Cybersecurity / incident response consultants
- Technical auditors

Prerequisites

- Solid foundation in Windows and/or Linux (processes, files, permissions)
- Basic knowledge of TCP/IP networks and logs
- Understanding of security concepts (IOCs, malware, persistence)
- Documentary accuracy and best investigative practices

Technical requirements

- PC with 16 GB RAM recommended (8 GB minimum) and 40 GB free disk space
- Windows 10/11 or Linux (VM allowed), installation rights
- Virtualization enabled (Hyper-V/VirtualBox/VMware)
- Tools: text editor, terminal, hash utilities (SHA-256)

Our EC-Council CIH™ Training Program: Incident Handling & Forensics

[Day 1 - Morning]

IH Methodology and Environment Setup

- The Incident Lifecycle (NIST vs. SANS): Preparation, Detection, Containment
- Legal and Ethical Framework: Evidence Integrity and Chain of Custody
- Analysis Workstation: Setting Up a Virtual Investigation Machine (SIFT Workstation)
- Evidence Collection: Order of Volatility and Acquisition (Disk vs. RAM)
- Hands-on Workshop: Creating an investigation kit and acquiring an image with hash validation.

[Day 1 - Afternoon]

System Forensics: Windows & Linux

- Windows Artifacts: Registry (Run keys), Prefetch, Shimcache, and Event Logs
- Linux Traces: Cronjobs, SSH keys, Systemd services, and Bash history
- Timeline Analysis: Creating a Super-Timeline to Correlate Events
- Handling Volatile Artifacts: Processes, Connections, and Active Sessions
- Hands-on Workshop: Analyzing a disk image to identify the entry vector and persistence.

[Day 2 - Morning]

Memory Analysis and Malware Detection

- Advanced RAM Analysis: Using Volatility (Processes, DLLs, Sockets)
- Anomaly Detection: Code Injections and Orphaned Processes
- Malware triage: Rapid static analysis (strings, entropy, Capa)
- Dynamic Analysis in a Sandbox and Extraction of Indicators of Compromise (IOCs)
- Hands-on Workshop: Extracting malware from a memory dump and analyzing its capabilities.

[Day 2 - Afternoon]

Network Investigation and Data Flow

- Traffic Analysis (PCAP): Identification of Command & Control (C2) Tags
- Critical Protocols: DNS, HTTPS (certificates), and tunnel analysis
- Correlation with infrastructure logs: Firewall, Proxy, and SIEM
- Session reconstruction and extraction of transferred files
- Hands-on Workshop: Analyzing a network capture to reconstruct an exfiltration scenario.

[Day 3 - Morning]

Application and Cloud Forensics

- User Traces: Web Browsers (history, cache) and Email (Phishing)
- Introduction to Cloud Incidents: Specifics of AWS/Azure Logs (CloudTrail)
- Automated triage: Quick collection scripts for IOCs
- User Correlation: Tracing the "who, what, when" from the application context
- Hands-on Workshop: Tracing the Path of an Infection Using Browser Artifacts

[Day 3 - Afternoon]

Post-Incident, Reporting, and Certification

- Eradication and Remediation: Cleanup and Evolution Strategies
- Professional Reporting: Executive Summary and Technical Appendices
- CIH Exam Preparation: Review of concepts, quizzes, and common pitfalls
- Incident Closure Checklist and Information Sharing (MISP)
- Hands-on Workshop: Writing an Investigation Summary (Timeline + IOCs) and Debriefing.

FAQ – QUESTIONS / ANSWERS

In what language is the CIH™ training taught?

The training is in French.

Is the exam included in the training price?

Yes, the certification fee is included in the course cost ($450 as a rough estimate). You will be able to take the exam at the end of the session.

How is the CIH™ certification exam administered?

The exam consists of a performance-based multiple-choice test with a maximum of 100

questions. It is taken online at a Pearson Vue-approved testing center.

The exam lasts **180 minutes**; the available languages are English

Relevant companies

This training program is designed for both individuals and businesses—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Certification

At the end of the session, a multiple-choice quiz is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.