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

Updated on September 10, 2026

Sign Up

GIAC GCIH® Certification Training

5 days (35 hours)

Overview

The GIAC GCIH Certification Training prepares you to take the official GIAC Certified Incident Handler certification exam and validates your ability to detect, analyze, contain, and resolve IT security incidents.

The GIAC GCIH certification is designed for professionals involved in incident response, technical investigation, and system defense. It assesses operational skills covering attack techniques, forensic analysis, and remediation in realistic scenarios.

Our GIAC GCIH Certification training will help you structure your exam preparation, review the assessed topics, and strengthen your mastery of incident handling methods. You will learn to identify intrusion vectors, characterize malicious activities, and apply appropriate containment measures.

You will cover key topics for the certification, including network scanning, password attacks, SMB services, tools such as Nmap, Metasploit, and Netcat, as well as attacks targeting web applications, APIs, and cloud environments.

Upon completion of the course, you will be able to effectively prepare for the GIAC Certified Incident Handler exam, respond appropriately during an incident, and demonstrate practical skills in detection, investigation, containment, and remediation.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Master the technical areas assessed by the GIAC Certified Incident Handler certification
- Identify and classify common attack techniques to accelerate incident response
- Analyze network and system traces using essential investigation tools
- Apply appropriate containment, eradication, and remediation strategies
- Develop a strategy for reviewing, organizing, and managing your time for the GIAC GCIH exam

Target Audience

- SOC Analyst
- Incident Responder
- System Administrator
- Cybersecurity Engineer
- Security Consultant

Prerequisites

- Knowledge of the fundamentals of cybersecurity and incident response
- Proficiency with Windows and Linux environments
- Knowledge of TCP/IP networks, network services, and system logs
- Basic understanding of account, permission, and SMB service administration

Technical Prerequisites

- Windows and Linux lab environments configured for attack and incident response scenarios
- Reconnaissance and exploitation tools required for the exercises, including Nmap, Netcat, and Metasploit
- Network capture and analysis tools, as well as system logs prepared for investigation exercises
- Deliberately vulnerable lab web applications and APIs for exploitation and remediation
- A demonstration cloud environment configured for exercises involving exposed credentials, permissions, and data

Our GIAC GCIH® Training Program

[Day 1 - Morning]

Certification framework and incident response

- Positioning of the GIAC Certified Incident Handler certification and validated skills
- Exam format, time management, open-book policy, and preparation of printed materials
- Incident response lifecycle: preparation, detection, analysis, containment, eradication, and lessons learned

- Alert triage, initial information gathering, and preservation of relevant evidence
- Developing an objective-based study plan and creating a reference index that can be used on exam day

[Day 1 - Afternoon]

Network reconnaissance, scanning, and mapping

- Principles of reconnaissance, enumeration, and mapping of exposed assets
- Analyzing TCP/IP traffic, identifying ports, services, banners, and configuration errors
- Using Nmap to scan hosts, ports, versions, and targeted scripts
- Interpreting scan results and prioritizing risks for investigation
- Hands-on workshop: mapping a lab network with Nmap, identifying exposed services, and developing an initial investigation hypothesis

[Day 2 - Morning]

Exploitation, Shells, and Covert Communications

- Overview of exploitable vulnerabilities and the relationship between exploitation, post-exploitation, and defensive response
- How Metasploit works, modules, payloads, and limitations of use in an analysis
- The role of Netcat, remote shells, port redirects, and command-and-control communications
- Detection of anomalous behavior related to outbound connections, tunnels, and unexpected services
- Preparation for certification exam questions on exploitation tools and covert communication channels

[Day 2 - Afternoon]

Detection and analysis of evasion techniques

- Indicators of compromise, attack timeline, and correlation between network and system events
- Persistence, privilege escalation, process concealment, and post-exploitation techniques
- Analysis of evasion mechanisms: encoding, obfuscation, trace removal, and bypassing controls
- Defense measures: logging, process monitoring, detection rules, and validation of alerts
- Hands-on workshop: Analyze a persistence and evasion scenario, reconstruct the timeline, and define containment actions

[Day 3 - Morning]

Attacks on Passwords and Usernames

- How Passwords Work, Hashing, Salting, and Major Authentication Weaknesses
- Attack techniques: dictionary attacks, brute force attacks, username reuse, and interception of secrets
- Recognizing attack indicators and selecting appropriate protective measures
- Managing privileged credentials, rotating secrets, and responding to account compromises
- Key considerations for certification objectives related to understanding and securing Passwords

[Day 3 - Afternoon]

SMB and investigation of internal services

- Architecture and uses of the SMB protocol in Windows environments
- Enumeration of shares, permissions, anonymous access, and configuration risks
- SMB attack techniques: accessing shares, lateral movement, and credential abuse
- Detection of suspicious SMB activity and service hardening measures
- Hands-on Workshop: Investigating a Lab SMB Share, Identifying Data Exposure, and Proposing a Prioritized Remediation Plan

[Day 4 - Morning]

Web Attacks and API Security

- How Web Applications Work: HTTP Requests, Sessions, and Authentication Mechanisms
- Common attack vectors: injection, access bypass, parameter manipulation, and data exposure
- API-specific considerations: tokens, authorizations, object-based access control, and input validation
- Identifying signs of exploitation in application logs and network traffic
- Certification-focused review of web application and API compromise scenarios

[Day 4 - Afternoon]

Credentials and data in the cloud

- Risks associated with cloud credentials, exposed secrets, and inadequately protected storage
- Analysis of configuration errors, excessive permissions, and unauthorized access to data
- Detection of misuse of accounts, access keys, and tokens in a cloud environment
- Mitigation actions: revocation, secret rotation, privilege reduction, and log collection
- Hands-on workshop: handling a cloud credential leak incident, assessing the impact, containing access, and
  document corrective actions

[Day 5 - Morning]

Incident response and consolidation of knowledge

- Organizing an investigation: hypotheses, scope, priorities, evidence, and response decisions
- Containment and eradication strategies based on the attack vector and the level of compromise
- Technical communication, documentation of actions, and preparation of lessons learned
- Cross-functional overview of GCIH® objectives and identification of areas for improvement
- Hands-on workshop: managing an end-to-end incident response based on a multi-vector case, from the initial alert to remediation

[Day 5 – Afternoon] Final

exam preparation

- Targeted review of exam topics: scanning, exploitation, bypassing, passwords, SMB, cloud, web, and APIs
- Techniques for reading questions, eliminating distractors, and making decisions when faced with ambiguous cases
- Optimizing your personal index, organizing references, and managing your time over four hours
- Preparation for CyberLive simulations and the requirements of the proctored exam
- Hands-on workshop: taking a timed mock exam, reviewing answers, and finalizing your certification preparation plan

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific professional knowledge or modern methods.

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 level across 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

Hands-On Training: 60% hands-on, 40% theory. Training materials distributed in digital format to all participants.

Organization

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

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

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