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

Updated on 08/31/2026

Sign Up

GIAC GSEC® Certification Training

5 days (35 hours)

Overview

The GIAC GSEC Certification Training prepares you for the official GIAC Security Essentials certification and equips you with the essential skills to secure systems, networks, and cloud environments against common threats.

This course helps you prepare for the GIAC Security Essentials exam by reinforcing the operational fundamentals of cybersecurity. You'll learn how to apply the principles of defense in depth, protect identities, analyze risks, and implement appropriate security controls.

You will study the areas covered by the certification, including network security, cryptography, Linux and Windows hardening, web application security, vulnerability management, and incident response.

The preparation is based on use cases and hands-on exercises inspired by the scenarios assessed during the exam. You will develop an effective study method, organize your approved study materials, and practice answering technical questions within the allotted time.

By the end of the course, you will be able to apply the skills validated by the official GIAC Security Essentials certification, interpret key security scenarios, and take the exam with a methodical preparation plan.

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 Security Essentials certification
- Apply the principles of defense in depth to systems, networks, and services
- Identify vulnerabilities, attack vectors, and appropriate remediation measures
- Strengthen the security of Linux, Windows, and cloud environments
- Effectively prepare for the exam through a review strategy and practice scenarios

Target Audience

- Systems and network administrators
- SOC analysts
- Cybersecurity engineers
- Security consultant
- IT Security Technician

Prerequisites

- Basic knowledge of TCP/IP networks and common protocols
- Proficiency in Linux or Windows administration
- Basic understanding of cybersecurity, identity management, and access control
- Understanding of virtualization principles and cloud services

Technical Prerequisites

- Computer running Windows 10 or 11, macOS 13 or later, or a recent Linux distribution
- Quad-core processor, 16 GB of RAM recommended, and at least 30 GB of disk space available
- VirtualBox 7 or an equivalent hypervisor capable of running virtual machines
- Stable internet connection; up-to-date Google Chrome or Mozilla Firefox browser

GIAC GSEC® Training Course Outline

[Day 1 - Morning]

Certification Framework and Security Fundamentals

- Overview of the official GIAC Security Essentials certification, its domains, and validated competencies
- Understanding the exam format, time management, and preparation strategies
- Fundamentals of cybersecurity: confidentiality, integrity, availability, and risk management
- Principles of defense in depth, attack surfaces, and control selection
- Organizing a study strategy: objectives, resource index, and technical priorities

[Day 1 - Afternoon]

Identities, access, and security policies

- Access Control Models: DAC, MAC, RBAC, and Least Privilege
- Identity management, multi-factor authentication, and account lifecycle
- Password best practices, secret vaults, and protection against credential attacks
- The Role of Policies, Standards, Procedures, and Awareness in Security Governance
- Hands-on Workshop: Analyzing an Account Compromise Scenario and Defining Access Controls and Remedial Measures

[Day 2 - Morning]

Networks, Protocols, and Defensible Architecture

- Review of TCP/IP, DNS, DHCP, HTTP, and TLS protocols
- Network segmentation, trust zones, filtering, and principles of defensible architecture
- Functionality and placement of firewalls, proxies, IDS, IPS, and logging systems
- Analysis of common network attacks: eavesdropping, spoofing, denial-of-service, and lateral movement
- Wireless network protection: encryption, authentication, and configuration risks

[Day 2 - Afternoon]

Communications security and network analysis

- Securing web traffic, email, remote access, and file transfers
- How symmetric and asymmetric cryptography, hashing, and digital signatures work
- Certificate management, certificate authorities, and common TLS deployment errors
- Analyzing network traffic and identifying indicators of suspicious activity in network communications
- Hands-on workshop: Analyzing a network capture with Wireshark to identify protocol vulnerabilities and anomalies

[Day 3 - Morning]

Linux Hardening and Security

- Linux Security Architecture, Users, Groups, Permissions, and Privilege Control
- Secure configuration of services, SSH access, logging, and updates
- System hardening: unnecessary services, host firewall, sensitive files, and scheduled tasks
- Monitoring processes, connections, logs, and persistence mechanisms
- Linux Security Tools and Evidence Collection Methods

[Day 3 - Afternoon]

Securing Windows Environments

- Managing Accounts, Groups, User Rights, and Windows Security Policies
- The Role of Active Directory, Group Policies, and Centralized Authentication
- Securing Network Services, File Sharing, PowerShell, and Workstations
- Event auditing, log analysis, and detection of suspicious activity
- Hands-on Workshop: Auditing a Windows Configuration, Prioritizing Discrepancies, and Proposing a Hardening Plan

[Day 4 - Morning]

Vulnerabilities, Attacks, and Asset Protection

- Vulnerability management lifecycle: discovery, qualification, prioritization, and remediation
- Principles of vulnerability scanning, result validation, and patch tracking
- Attack vectors: social engineering, exploitation, malware, privilege escalation, and data exfiltration
- Endpoint protection, application control, backups, and data loss prevention
- Risks in Virtualized and Cloud Environments: Isolation, Configuration, and Shared Responsibility Shared

[Day 4 - Afternoon]

Detection, incident response, and SIEM

- Phases of incident response: preparation, detection, containment, eradication, and lessons learned
- Alert prioritization, indicators of compromise, and escalation criteria
- Log collection, retention, and correlation in a SIEM
- Developing detection scenarios and aligning them with critical security controls
- Hands-on workshop: handling a simulated incident using system and network logs, then documenting response actions

[Day 5 - Morning]

Consolidation of exam topics

- Cross-cutting review of objectives: access, networks, systems, cryptography, cloud, and incident response
- Analysis of certification case studies involving multiple security controls
- Identifying common pitfalls: terminology, technical scenarios, prioritization, and selection of measures
- Preparation of authorized reference materials and optimization of the search index
- Problem-solving method: targeted reading, elimination of answers, management of deferred questions, and verification

[Day 5 – Afternoon]

Simulation and final preparation for the certification exam

- Review of exam procedures, proctoring, and applicable rules
- Managing the four-hour exam: time allocation, scheduled breaks, and handling complex questions
- Approach to CyberLive exercises: analyzing instructions, controlled execution, and validating results
- Assessment of knowledge, identification of areas for improvement, and individual preparation plan
- Hands-on workshop: conducting a mock exam with synthesis questions and a timed technical scenario

Target Companies

This training is intended for both individuals and companies—large or small—seeking 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 operation of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. 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.