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

Updated on 09/17/2026

Sign Up

GIAC GCED Certification Training

5 days (35 hours)

Overview

The GIAC Certified Enterprise Defender certification validates your ability to defend an enterprise environment through network monitoring, packet analysis, incident response, and malware analysis.

The GIAC GCED Certification Training prepares you for the official GIAC Certified Enterprise Defender certification and its proctored exam. You will build the skills needed to design, operate, and improve a technical defense tailored to enterprise environments.

You will learn how to implement a defensive infrastructure, analyze logs and network traffic, examine packet captures, and triage security alerts. The course also covers the fundamentals of penetration testing, evidence collection, and incident handling.

Upon completion of the training, you will be able to recognize intrusion techniques, conduct an initial malware analysis, and coordinate containment, eradication, and remediation efforts. You will also have a structured preparation method for the official GCED exam.

Finally, this course covers exam strategy, the organization of authorized materials, scenario-based exercises, and practice with representative cases. This will enable you to demonstrate operational skills in threat detection and corporate defense.

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 skill areas assessed by the GIAC Certified Enterprise Defender certification.
- Analyze packets, logs, and alerts to detect an intrusion.
- Implement appropriate network defense and monitoring controls.
- Apply an incident response process, from triage to remediation.
- Identify suspicious behavior and perform an initial malware analysis.
- Effectively prepare for the GCED exam using a review and indexing method.

Target Audience

- SOC Analyst
- Network Security Engineer
- Incident Responder
- Cybersecurity Consultant
- Penetration Tester

Prerequisites

- Proficiency in the fundamentals of TCP/IP networks and major protocols.
- Practical knowledge of Windows and Linux systems.
- Basic experience with log analysis and security tools.
- Basic knowledge of incident response and security architecture.

Technical Prerequisites

- Windows and Linux lab environments configured for defense and investigation exercises
- Wireshark and network analysis tools configured for analyzing packet captures and traffic
- SIEM and intrusion detection systems fed with logs and events prepared for the exercises
- Isolated forensic environment with disk images, Windows artifacts, and controlled samples for malware investigation and analysis exercises
- Network reconnaissance and diagnostic tools required for exercises validating defensive controls

Our GIAC GCED® Training Program

[Day 1 - Morning]

Certification Framework and Enterprise Defense

- Overview of the GIAC Certified Enterprise Defender certification and the skills it validates.
- Overview of the assessed domains, exam format, and preparation criteria.

- Principles of defense in depth and the enterprise security model.
- Mapping of assets, attack surfaces, and protection priorities.
- Roles of the SOC, the network team, incident response, and vulnerability management.

[Day 1 - Afternoon] Network

Protocols and Controls

- Review of TCP/IP, DNS, HTTP, TLS, SMTP, and SMB protocols from a defensive perspective.
- Identification of common attacks on protocols and hardening measures.
- Segmentation, filtering, firewalls, proxies, VPNs, and network access control.
- Secure configuration guidelines and essential security controls.
- Interpreting network indicators useful for detecting abnormal activity.
- Hands-on workshop: Analyzing a network capture with Wireshark to identify suspicious behavior and propose appropriate defensive controls.

[Day 2 - Morning]

Monitoring and Intrusion Detection

- Network security monitoring architecture and probe placement.
- Operation and configuration of intrusion detection and prevention systems.
- Types of packets, sessions, flows, metadata, and full captures.
- Developing a detection strategy based on assets and threat scenarios.
- Alert qualification, reducing false positives, and prioritizing investigations.

[Day 2 - Afternoon]

Logs, Flows, and Network Investigation

- Sources of network, system, security, and application logs.
- Centralization, normalization, and retention of events in a SIEM.
- Analyzing traffic data to identify abnormal communications.
- Correlation between alerts, logs, and enterprise context data.
- Creating an incident timeline based on technical traces.
- Hands-on workshop: conducting an investigation using a set of logs and flow data, characterizing the incident, and producing a well-reasoned timeline.

[Day 3 - Morning]

Incident Response and Threat Intelligence

- Incident Response Lifecycle: Preparation, Detection, Containment, Eradication, and Lessons Learned.
- Assessment, criticality, scope, and collection of information necessary for decision-making.
- Integration of threat intelligence, indicators, and the Cyber Kill Chain.
- Technical communication, evidence preservation, and stakeholder coordination.
- Selection of containment measures based on business and operational impacts.

[Day 3 – Afternoon]

Digital Investigation and Malware Analysis

- Principles of digital forensics and identification of useful artifacts.
- Signs of infection, persistence mechanisms, and common malicious behaviors.
- Static analysis, dynamic analysis, and security precautions in an isolated environment.
- Interpreting the results of automated tools and the limitations of their conclusions.
- Basics of disassembly, decompilation, and obfuscation techniques.
- Hands-on workshop: Analyzing artifacts from a compromised system in an isolated environment, identifying indicators, and defining remediation actions.

[Day 4 - Morning]

Penetration Testing for Defense Purposes

- Objectives, scope, rules of engagement, and ethics of penetration testing.
- Reconnaissance, enumeration, vulnerability identification, and risk validation.
- Understanding attack techniques to improve detection capabilities.
- Diagnostic and testing tools, interpretation of results, and limitations of use.
- Drafting technical reports and prioritized remediation recommendations.

[Day 4 - Afternoon]

Defensive architecture and continuous improvement

- Designing preventive, detective, and corrective controls in a hybrid architecture.
- Protection of network and cloud services, identity management, and logging.
- Hardening, patch management, and validation of security configurations.
- Measuring detection effectiveness through use cases and performance metrics.
- Developing a roadmap to strengthen the security posture.
- Hands-on workshop: Design a defensive architecture for a fictional company and justify the controls, log sources, and deployment priorities.

[Day 5 - Morning]

Exam Preparation Methodology

- Organizing review sessions according to the GCED certification objectives.
- Creating a printed reference index that can be used during an exam where printed materials are permitted.
- Time management, reading exam questions, and eliminating irrelevant answers.
- Comprehensive review of protocols, detection, incident response, and malware analysis.
- Analysis of recurring errors and development of an individual improvement plan.

[Day 5 - Afternoon]

Simulation and reinforcement of learned material

- Review of key concepts covering the GIAC Certified Enterprise Defender exam topics.
- Analysis of integrated scenarios combining network intrusion, logs, malware, and remediation.
- Justification of technical decisions based on evidence and business constraints.
- Final preparation tips, exam planning, and managing the proctored exam environment.
- Summary of the operational skills validated by the certification.
- Hands-on workshop: Conduct a mock exam simulation based on an enterprise defense case study, followed by a group review of investigation and remediation choices.

Target Audience

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 business 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% 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.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg