+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 GCLD Certification Training

5 days (35 hours)

Overview

The official GIAC Cloud Security Essentials certification validates your ability to protect cloud environments using preventive, detective, and reactive controls.

The GIAC GCLD Certification Training course prepares you for the official GIAC Cloud Security Essentials certification, designed for professionals responsible for securing workloads in public and multicloud environments. You will develop an operational understanding of risks, shared responsibilities, and defense mechanisms tailored to cloud services.

You will learn to evaluate service models and secure identities, external access, networks, computing resources, containers, storage, and sensitive data. The course also covers logging, network monitoring, secret management, automation, and DevSecOps practices.

Practical exercises will allow you to apply the exam objectives to configuration, audit, and incident response scenarios. You will learn to analyze cloud exposure, select appropriate controls, and interpret logs to detect suspicious activity.

Upon completion of the training, you will have a structured approach for preparing for the GIAC Cloud Security Essentials exam, organizing your review, and validating the expected cloud security competencies. You will also be able to apply these skills to your security, compliance, and continuous improvement efforts.

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 Cloud Security Essentials certification.
- Analyze shared responsibilities and the key risks of cloud and multicloud environments.
- Secure identities, access, networks, computing resources, and cloud data.
- Utilize logging, monitoring, and incident response mechanisms in the cloud.
- Effectively prepare for the exam through practical case studies and targeted practice exercises.

Target Audience

- Cloud Security Engineer
- Security Analyst
- Systems and Cloud Administrator
- DevOps Engineer
- Security Auditor

Prerequisites

- Knowledge of the fundamentals of information systems security.
- Experience with network administration, segmentation, and access control concepts.
- Understanding of cloud services, accounts, roles, and access policies.
- Basic knowledge of scripting or automation using Python, PowerShell, or an equivalent language.

Technical Prerequisites

- Cloud lab environments configured for security and audit exercises
- Demo IAM accounts and roles for managing identities, permissions, and access policies
- Virtual networks, computing resources, and cloud storage spaces prepared for Security
- Cloud logging and monitoring services enabled for incident detection and response exercises
- Infrastructure-as-Code environment and CI/CD pipeline prepared for automation and DevSecOps exercises

Our GIAC GCLD® Training Program

[Day 1 - Morning]

Fundamentals and preparation strategy

- Overview of the GIAC Cloud Security Essentials certification and the skills assessed.
- Exam structure, question types, and time management strategies.

- Overview of IaaS, PaaS, and SaaS models and multicloud environments.
- Division of responsibilities between the cloud provider and the customer.
- Identifying cloud assets, threats, and attack surfaces.
- Hands-on workshop: Analyzing a cloud migration scenario and creating a shared responsibility matrix.

[Day 1 – Afternoon]

Identities, Accounts, and External Access

- Principles of identity and access management in cloud platforms.
- Human accounts, service accounts, roles, federation, and multi-factor authentication.
- Applying the principle of least privilege and designing authorization policies.
- Securing third-party integrations, API access, and trust relationships.
- Identifying common errors related to excessive privileges and exposed secrets.

[Day 2 - Morning]

Securing Cloud Networks

- Virtual network architecture, subnets, routing, and exposure points.
- Security groups, access control lists, and traffic filtering.
- Segmentation, microsegmentation, and isolation of sensitive environments.
- Secure remote access, bastions, VPNs, and reducing the attack surface.
- Major network attacks against cloud resources and appropriate countermeasures.
- Hands-on workshop: auditing a cloud network architecture and correcting risky filtering rules.

[Day 2 - Afternoon]

Secure computing, images, and deployments

- Principles of hardening virtual machines and computing services.
- Image assessment, patch management, and reducing the attack surface.
- Security of serverless functions and control of execution permissions.
- Containers, orchestration, and workload isolation.
- Best practices for secure deployment and initial compliance checks.

[Day 3 - Morning]

Data protection and secret management

- Data classification and risks specific to shared environments.
- Encryption of data at rest and in transit, key management, and key rotation.
- Securing object, block, and file storage with appropriate access policies.

- Data leak prevention and discovery of sensitive information.
- Management of secrets, tokens, certificates, and application credentials.
- Hands-on workshop: Securing cloud storage containing sensitive data and implementing a secrets management strategy.

[Day 3 - Afternoon]

Security Logging and Monitoring

- Cloud log sources, audit events, and retention policies.
- Centralization, standardization, and protection of log integrity.
- Identity, administration, network, and data access logs.
- Network traffic, packet captures, and indicators useful for detection.
- Interpreting alerts and building monitoring use cases.

[Day 4 - Morning]

Automation and Integrated Security

- Principles of Infrastructure as Code and deployment reproducibility.
- Automation of configuration checks and drift detection.
- Integrating security into CI/CD and DevSecOps cycles.
- Continuous assessment of resources, policies, and remediation practices.
- Secure development frameworks, threat modeling, and security by design.
- Hands-on workshop: Review an infrastructure model and identify security controls to automate.

[Day 4 - Afternoon]

Risk, Compliance, and Security Assurance

- Cloud security governance and business risk management.
- Assessment of vendors, contractual requirements, and third-party dependencies.
- Concepts of compliance, audit evidence, and continuous monitoring.
- Prioritizing vulnerabilities based on exposure, impact, and likelihood.
- Developing a plan to improve cloud security posture.

[Day 5 - Morning]

Detection, Response, and Investigation

- Incident response cycle applied to cloud resources.
- Analysis of an account compromise, an exposed key, or a public resource.
- Evidence collection, log preservation, and initial investigation.

- Containment, eradication, and remediation actions in a cloud environment.
- Introduction to penetration testing and threat-informed defense considerations.
- Hands-on workshop: handling a cloud incident scenario using logs, alerts, and indicators of compromise.

[Day 5 - Afternoon]

Review and final exam preparation

- Comprehensive review of the official certification objectives.
- Analysis of common pitfalls related to identities, networks, data, logs, and automation.
- Techniques for reading questions, eliminating inconsistent answers, and making decisions under time pressure.
- Organizing review sessions and preparing authorized resources for the exam.
- Assessment of knowledge and identification of individual areas for improvement.
- Hands-on workshop: taking a targeted practice exam, reviewing answers, and developing a final study plan.

Target Companies

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technology 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 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

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.