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

Updated on 04/24/2026

Sign up

GCP Professional Cloud Security Engineer Certification Training

1 day (7 hours)

Overview

Google Cloud Platform enables you to secure applications in a reproducible manner on cloud servers and complex environments, without relying on manual root access management. This certification is ideal for packaging secure pipelines and protecting multi-user executions.

This training aims to make your workflows portable and secure: identity management, execution on hardened compute nodes, and granular data protection. You will learn to choose between different security services (CMEK, VPC SC, IAP) and build your own security recipes. The goal is to equip you with the skills to manage a GCP infrastructure that meets the highest industry standards, while mastering the diagnosis of common errors related to permissions or the network.

The approach is 100% hands-on: it centers on guided workshops, configuration demos, and real-time diagnostics. Deliverables include a checklist of security best practices and sample commands to integrate security into your automation scripts. This practical immersion ensures immediate skill development and optimal preparation for the complex scenarios of the Professional Cloud Security Engineer exam.

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

Objectives

- Configure and manage access and identities in a secure cloud environment.
- Ensure data protection (encryption, key management, protection at rest and in transit).
- Configure network defenses and secure communications between cloud resources.

- Manage security operations, including environment monitoring and incident response.
- Support regulatory compliance requirements and implement appropriate controls.
- Be prepared to take the Professional Cloud Security Engineer certification exam

Target Audience

- Developers,
- Systems Operations Managers
- Solution architects new to Google Cloud
- Senior executives/decision-makers
- Anyone planning to deploy applications and create application environments on Google Cloud

Prerequisites

- Basic knowledge of application development, systems operations, Linux operating systems, and data analysis/machine learning will be helpful for understanding the technologies covered

Technical prerequisites

- The Google Cloud SDK command-line interface (gcloud) installed and configured.
- A computer with a modern browser (Chrome recommended)
- A Google Cloud account with billing enabled or access to a dedicated sandbox.

Our GCP Professional Cloud Security Engineer Certification Training Program

[Day 1 - Morning]

Governance and Identity Management

- Hierarchy and Structure: Organization, Folders, Projects, and Policy Inheritance
- Identity and Access Management (IAM): Principle of Least Privilege and Service Accounts
- Workload Identity: Securing interactions between Google applications and services
- Identity Federation: Synchronization with External Directories and Cloud Identity
- Hands-on Workshop: Configuring a Complex Project Structure and Resolving Permission Conflicts.

[Day 1 - Afternoon]

Access Control and Safeguards

- Implementing Organization Policy Constraints
- Service Account Key Management and Secure Rotation
- Access Scopes vs. IAM Roles: Best Practices and Limitations
- Access Auditing and Detection of Excessive Data Sharing
- Hands-on Workshop: Deploying Organizational Guardrails.

[Day 2 - Morning]

Network Security and Perimeter Protection

- VPC Segmentation: Subnets, Firewall Rules, and Advanced Routing
- VPC Service Controls (VPC SC): Creating perimeters to prevent data exfiltration
- Perimeter Defense: Cloud Armor (WAF/DDoS) and Identity-Aware Proxy (IAP)
- Secure Connectivity: HA VPN, Cloud Interconnect, and Google Private Access
- Hands-on Workshop: Deploying a VPC SC perimeter and isolating a sensitive service.

[Day 2 - Afternoon]

Workload and Data Protection

- Data Encryption: Choosing Between GMEK, CMEK (Cloud KMS), and CSEK
- Compute Security: Shielded VMs, OS Login, and image hardening
- Container Security: Binary Authorization and GKE Network Policies
- Cloud DLP: Discovery, Classification, and Anonymization of Sensitive Data
- Hands-on Workshop: CMEK Encryption and DLP Scan of a Dataset.

[Day 3 - Morning]

Operations, Detection, and Response

- Security Command Center (SCC): Posture Monitoring and Threat Detection
- Log Analysis: Cloud Logging, Activity Logs, and Data Access Logs
- Vulnerability Management: Container Analysis and Web Security Scanner
- Response Automation: Alerts and Remediation via Cloud Functions
- Hands-on Workshop: Intrusion Simulation and Detection via Security Command Center.

[Day 3 - Afternoon]

DevSecOps Strategy and Certification Preparation

- Integrating Security into CI/CD Pipelines (Cloud Build)
- Exam Methodology: Analysis of typical certification case studies
- Review of Google Cloud Best Practices for Secure Architecture

- Timed practice exam and detailed feedback on common pitfalls
- Practical workshop: Taking the condensed mock exam and final review.

Target Audience

This training is intended for both individuals and companies, large or small, wishing 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 regarding 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.

Assessment

At the end of the session, a multiple-choice questionnaire 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.