+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 Security Operations Engineer Certification Training

4 days (28 hours)

Overview

The Professional Security Operations Engineer is a Google Cloud certification designed for professionals responsible for detecting, analyzing, and responding to security incidents in a cloud environment. It validates advanced skills in Security Operations, monitoring, investigation, threat response, and continuous improvement of security posture.

Our Professional Security Operations Engineer Certification training will enable you to master security operations on Google Cloud by covering essential tools and practices related to SOC, SIEM, log collection, threat detection, and incident response.

You will learn to collect, correlate, analyze, and act on security events using services such as Security Command Center, Cloud Logging, and Google Security Operations. The training emphasizes real-world scenarios to help you understand how to triage an alert, investigate an incident, and implement appropriate remediation actions.

By the end of the course, you will be able to secure cloud workloads, enhance a SOC's detection capabilities, automate certain responses, and monitor key operational security metrics in a Google Cloud environment.

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

Objectives

- Understand the principles of Security Operations on Google Cloud

- Collect, centralize, and analyze security logs
- Detect threats using Security Command Center and Google Security Operations
- Investigate incidents and triage critical alerts
- Implement response and remediation actions
- Effectively prepare for the Professional Security Operations Engineer certification

Target audience

- SOC analysts and cybersecurity analysts
- Cloud security engineers
- Security-focused system and network administrators
- DevSecOps and SRE engineers and operations managers
- Professionals preparing for the Google Cloud Security Operations Engineer certification

Prerequisites

- Basic knowledge of Google Cloud or cloud computing
- Basic understanding of cybersecurity, networking, and systems
- Understanding of logs, alerts, incidents, and vulnerabilities
- Some experience in SOC, operations, or cloud security is recommended

Professional Security Operations Engineer Certification Training

[Day 1 - Morning]

Understanding security operations on Google Cloud

- Defining the role of a Security Operations Engineer in a cloud environment
- Understand the principles of a SOC, SIEM, and SOAR
- Identify the challenges of incident detection, analysis, and response
- Explore the Google Cloud security ecosystem
- Positioning the Professional Security Operations Engineer certification
- Hands-on workshop: Mapping the security needs of a cloud environment.

[Day 1 - Afternoon]

Implementing cloud security fundamentals

- Understanding the shared responsibility model
- Applying IAM best practices and the principle of least privilege
- Securing Google Cloud projects, folders, and organizations
- Use organization policies and compliance controls

- Identify risky configuration errors
- Hands-on workshop: Auditing IAM access in a Google Cloud environment.

Collect and centralize security logs

- Understand the role of Cloud Logging in security operations
- Identify critical logs: admin activity, data access, network, and workloads
- Configure log exports and centralization
- Organize logs to facilitate detection and investigation
- Implement a log retention and utilization strategy
- Hands-on workshop: Configure security log collection that can be utilized by a SOC.

[Day 2 - Morning]

Using Security Command Center

- Discover the features of Security Command Center
- Analyze findings, vulnerabilities, and misconfigurations
- Prioritize risks based on their business impact
- Monitor the exposure of cloud resources and workloads
- Implement remediation processes
- Hands-on workshop: Analyzing and prioritizing Security Command Center findings.

[Day 2 - Afternoon]

Detect threats with Google Security Operations

- Understand the role of Google Security Operations in a cloud SOC
- Security data ingestion and event normalization
- Searching for suspicious events in collected logs
- Using detection rules and indicators of compromise
- Identifying abnormal behavior across identities, networks, and workloads
- Hands-on workshop: Detecting suspicious activity from correlated events

Investigating security incidents

- Apply a structured investigation methodology
- Assess an alert and determine its severity level
- Search for traces of an incident in logs and events
- Identify accounts, resources, and data that may be affected
- Document evidence and prepare an incident report
- Hands-on workshop: Conduct a comprehensive investigation of a cloud attack scenario.

[Day 3 - Morning]

Respond to incidents and contain threats

- Understand the phases of incident response: containment, eradication, recovery
- Define priority actions based on the type of incident
- Isolate compromised resources and revoke suspicious access
- Coordinate the response among SOC, cloud, network, and business teams
- Formalize remediation and return-to-normal procedures
- Hands-on workshop: Execute an incident response plan in a compromised environment.

[Day 3 - Afternoon]

Secure workloads, networks, and data

- Monitor Compute Engine, GKE, Cloud Run, and managed service workloads
- Identify risks related to network configurations, firewalls, and public exposure
- Protect sensitive data with encryption, keys, and access controls
- Detect abnormal behavior in network traffic and application services
- Apply cloud security best practices in production
- Hands-on workshop: Analyze a cloud application’s exposure and propose remediation measures.

Automate security operations

- Understand the benefits of automation in a modern SOC
- Create workflows to respond to recurring alerts
- Using notifications, serverless functions, and security integrations
- Reducing false positives and improving response time
- Structuring cloud security playbooks
- Hands-on workshop: Automating a remediation action based on a critical alert.

[Day 4 - Morning]

Monitor SOC metrics and improve detection

- Define key metrics: MTTD, MTTR, alert volume, and severity
- Create dashboards tailored for SOC analysts and security managers
- Measuring the quality of detection rules and reducing operational noise
- Establish a continuous improvement loop
- Document post-incident lessons learned
- Hands-on workshop: Building an operational dashboard for security monitoring.

[Day 4 - Afternoon]

Governance, compliance, and security reporting

- Aligning security operations with compliance requirements
- Understanding relevant standards: NIST, ISO 27001, cloud best practices

- Implementing risk control and monitoring policies
- Produce reports that are understandable to technical teams and management
- Structure a continuous improvement process for security posture
- Hands-on workshop: Generate a security posture report based on a cloud scenario.

Preparation for the Professional Security Operations Engineer exam

- Understand the structure of the Professional Security Operations Engineer exam
- Review key areas: detection, investigation, response, governance, and cloud security
- Analyze exam scenarios and identify the most appropriate answers
- Recognize common pitfalls related to Google Cloud security operations
- Create a personalized study plan after the training
- Hands-on workshop: Taking the practice exam + review.

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 industry knowledge or modern methodologies.

Assessment upon enrollment

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

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.