ITTcert
BY ORSYS

Course : Security in Google Cloud Platform

Official course, preparation for Google Cloud certification exams

Practical course - 3d - 21h00 - Ref. GQD
Price : 2990 € E.T.

With this training course, you'll learn how to master security controls and techniques on the Google Cloud Platform. Through hands-on experience, you'll explore and deploy the components of a secure Google Cloud solution. You'll also discover techniques for mitigating attacks at many points of a Google Cloud infrastructure, including distributed denial of service attacks, phishing attacks and threats involving content classification and use.

Teaching objectives

At the end of the training, the participant will be able to:

- Understand Google Cloud's security approach and key principles
- Manage administrative identities and access with Cloud Identity, Cloud IAM and Resource Manager
- Implement network security controls (VPC firewall, Cloud Armor, IAP)
- Securing application environments, especially Kubernetes
- Detecting, analyzing and correcting vulnerabilities with DLP, Forseti and risk reduction best practices

Intended audience

Information security analysts, architects and engineers, information security or cybersecurity specialists, cloud infrastructure architects.

Prerequisites

Completion of "GCP Fundamentals: Core Infrastructure", "Networking in GCP" or equivalent experience. Good knowledge of fundamental concepts of information security, etc.

Certification

We recommend you take this course if you want to prepare for certification as a "Google Cloud Professional Cloud Security Engineer".
Comment passer votre examen ?

PARTICIPANTS

Information security analysts, architects and engineers, information security or cybersecurity specialists, cloud infrastructure architects.

PREREQUISITES

Completion of "GCP Fundamentals: Core Infrastructure", "Networking in GCP" or equivalent experience. Good knowledge of fundamental concepts of information security, etc.

TRAINER QUALIFICATIONS

The experts who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

ASSESSMENT TERMS

Assessment of targeted skills prior to training.
Assessment by the participant, at the end of the training course, of the skills acquired during the training course.
Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.
At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.
An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

Practical details

Teaching methods

Training in French. Official course material in English.

Course schedule

1 Fundamentals of GCP security

- Understand the GCP model of shared responsibility for security.
- Understand Google Cloud's approach to security.
- Understand the types of threats mitigated by Google and GCP.
- Define and understand access transparency and access approval (beta).

2 Cloud Identity

- Cloud Identity.
- Synchronization with Microsoft Active Directory using Google Cloud Directory Sync.
- Using the managed service for Microsoft Active Directory (beta).
- Choose between Google authentication and SAML-based single sign-on.
- Best practices, including DNS configuration and super administrator accounts.

Hands-on work

Define users with Cloud Identity Console.

3 Identity, access and key management

- GCP resource manager: projects, files and organizations.
- GCP IAM roles, including custom roles.
- PCM IAM policies, including organization policies.
- Labels GCP Now.
- Now GCP recommends.
- GCP IAM troubleshooting tool.
- GCP IAM audit logs.
- Best practices, including segregation of duties and least privilege, etc.

Hands-on work

Cloud IAM configuration, including custom roles and organization rules.

4 Configure a Google virtual private cloud for isolation and security

- Configure VPC firewalls (entry and exit rules).
- Load balancing and SSL policies.
- Private access to the Google API.
- Use of SSL proxy.
- Best practices for VPC networks, including pairing and use of shared VPCs.
- Best security practices for VPNs.
- Safety considerations for interconnection and pairing options.
- Safety products available from our partners.
- Definition of a service perimeter, including perimeter bridges.
- Configure private connectivity to Google APIs and services.

Hands-on work

VPC firewall configuration.

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training course.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

5 Securing Compute Engine: techniques and best practices

- Compute Engine service accounts, default and customer-defined.
- IAM roles for virtual machines.
- API scope for virtual machines.
- SSH key management for Linux virtual machines.
- RDP connection management for Windows virtual machines.
- Organization policy controls: approved images, public IP address, serial port disable.
- Encrypt VM images with encryption keys managed by the customer and supplied by the customer.
- Research and correction of public access to VMs.
- Best practices, including the use of reinforced personalized images, personalized service accounts...
- Encrypt VM disks with encryption keys supplied by the customer.
- Use of shielded VMs to maintain VM integrity.

Hands-on work

Configure, use and audit VM accounts and service scopes. Perform disk encryption with customer-supplied encryption keys.

6 Securing cloud data: techniques and best practices

- Cloud Storage and IAM authorizations.
- Cloud Storage and ACLs.
- Audit of cloud data, including research and correction of publicly accessible data.
- URLs signed by Cloud Storage.
- Signed policy documents.
- Encrypt Cloud Storage objects with encryption keys managed and supplied by the customer.
- Best practices, including deletion of archived versions of objects after key rotation.
- Views authorized by BigQuery.
- BigQuery IAM roles.
- Best practices, including preferring IAM authorizations to ACLs.

Hands-on work

Use customer-provided encryption keys with Cloud Storage. Use customer-managed encryption keys with Cloud Storage and Cloud KMS. Create an authorized BigQuery view.

7 Application security: techniques and best practices

- Types of application security vulnerabilities.
- DoS protection in App Engine and Cloud Functions.
- Cloud Security Scanner.
- Identity Aware Proxy.

Hands-on work

Use Cloud Security Scanner to scan an App Engine application for vulnerabilities. Configure Identity Aware Proxy to protect a project.

8 Securing Kubernetes: techniques and best practices

- Authorization.
- Securing workloads.
- Securing clusters.
- Logging and monitoring.

9 Protect against Distributed Denial of Service (DDoS) attacks

- How DDoS attacks work.
- Mitigations: GCLB, Cloud CDN, autoscaling, VPC ingress and egress firewalls, Cloud Armor.
- Complementary partner products.

Hands-on work
Configure GCLB, CDN, blacklist traffic with Cloud Armor.

10 Protect against content-related vulnerabilities

- Threat: ransomware.
- Mitigation: backups, IAM, Data Loss Prevention API.
- Threats: data misuse, privacy breaches, sensitive/restricted/unacceptable content.
- Threat: identity phishing and Oauth.
- Mitigation: content classification using Cloud ML APIs.
- Scanning and editing data using the Data Loss Prevention API.

Hands-on work
Redaction of sensitive data with the Data Loss Prevention API.

11 Monitoring, logging, auditing and scanning

- Security Command Center.
- Stackdriver monitoring and logging.
- VPC flow logs.
- Cloud audit logging.
- Deploying and using Forseti.

Hands-on work
Install Stackdriver agents. Configure and use Stackdriver monitoring and logging. View and use VPC flow logs in Stackdriver. Configure and view audit logs in Stackdriver, etc.

Dates and locations

REMOTE CLASS
2026 : 2 June, 17 Nov.

PARIS LA DÉFENSE
2026 : 2 June, 17 Nov.