Google Cloud Partner

Security in Google Cloud

In this course, you will gain comprehensive knowledge of security controls and techniques in the Google Cloud. Through a combination of lectures, live demonstrations and hands-on exercises, you will learn to understand and implement the building blocks of a secure Google Cloud solution. You will work with powerful tools and services such as Cloud Identity, Identity and Access Management (IAM), Cloud Load Balancing, Cloud IDS, Web Security Scanner, BeyondCorp Enterprise and Cloud DNS to ensure security at the highest level.

Course Contents

- Google Cloud Security Fundamentals
- Securing Access to Google Cloud
- Identity and Access Management (IAM)
- Configuring Virtual Private Cloud for Isolation and Security
- Securing Compute Engine: Techniques and Best Practices
- Securing Cloud Data: Techniques and Best Practices
- Securing applications: techniques and best practices
- Securing Google Kubernetes Engine: techniques and best practices
- Protection against distributed denial-of-service (DDoS) attacks
- Content-related vulnerabilities: techniques and best practices
- Monitoring, logging, auditing, and scanning

In this course, you will learn the following skills:

- Understand the fundamentals of Google Cloud security.
- Manage administrative identities with Google Cloud.
- Implement user management with Identity and Access Management (IAM).
- Configure Virtual Private Clouds (VPCs) for isolation, security, and logging.
- Apply techniques and best practices for secure Compute Engine management.
- Apply techniques and best practices for secure Google Cloud data management.
- Apply techniques and best practices for securing Google Cloud applications.
- Apply techniques and best practices for securing Google Kubernetes Engine (GKE) resources.
- Manage protection against distributed denial-of-service (DDoS) attacks.
- Manage content-related vulnerabilities.
- Implement solutions for monitoring, logging, auditing, and reviewing Google Cloud.

Official Google Cloud documentation.

Target Group

- Analysts, architects and engineers in the field of cloud information security.

Prerequisites

- Prior completion of a Google Cloud Fundamentals: Core Infrastructure or equivalent experience
- Knowledge of basic information security concepts through experience
- Basic knowledge of command line tools and Linux operating system environments
- Experience in system operations, including application deployment and management, either on-premise or in a public cloud environment
- Reading understanding of code in Python or JavaScript
- Basic understanding of Kubernetes terminology

This Course in the Web

You can find the up-to-date information and options for ordering under the following link: www.experteach-training.com/go/**GCSP**

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training		Prices, excl. of V.A.T.
Classes in Germany	**3 Days**	**€ 1,895**
Classes in Austria	**3 Days**	**€ 1,895**
Online Training	**3 Days**	**€ 1,895**

Date/course venue		Course language German	
08/04-10/04/26	HYDüsseldorf	26/08-28/08/26	HYOnline
08/04-10/04/26	HYOnline	26/08-28/08/26	HYWien
24/06-26/06/26	HYMünchen	21/10-23/10/26	ONOnline
24/06-26/06/26	HYOnline		

Status 02/04/2026

Security in Google Cloud

Google Cloud Platform

ExperTeach

Table of Contents

Security in Google Cloud

Grundlagen der Google Cloud-Sicherheit
Der Sicherheitsansatz von Google Cloud
Das Modell der geteilten Sicherheitsverantwortung
Google und Google Cloud entschärfen Bedrohungen
Transparenz beim Zugang
Sicherung des Zugriffs auf Google Cloud
Cloud-Identität
Google Cloud Directory Sync
Verwaltetes Microsoft AD
Google-Authentifizierung gegenüber SAML-basiertem SSO
Identitätsplattform
Bewährte Authentifizierungsverfahren
Identitäts- und Zugriffsmanagement (IAM)
Ressourcenmanager
IAM-Rollen
Dienstleistungskonten
IAM- und Organisationsrichtlinien
Workload-Identitätsverbund
Politische Intelligenz
Übung: IAM konfigurieren
Konfigurieren der Virtual Private Cloud für Isolierung und Sicherheit
VPC-Firewalls
Lastausgleich und SSL-Richtlinien
Cloud-Zusammenschaltung
VPC-Netzwerk-Peering
VPC-Dienst-Kontrollen
Zugangskontext-Manager
VPC-Ablaufprotokolle
Cloud IDS
Laboratorien:
VPC-Firewalls konfigurieren
Konfigurieren und Verwenden von VPC-Flow-Protokollen in der Cloud-Protokollierung
Demo: Absicherung von Projekten mit VPC Service Controls
Erste Schritte mit Cloud IDS
Absicherung der Compute Engine: Techniken und bewährte Praktiken
Dienstkonten, IAM-Rollen und API-Bereiche
Verwaltung von VM-Anmeldungen
Kontrollen der Organisationspolitik
Abgeschirmte VMs und vertrauliche VMs
Dienst der Zertifizierungsstelle
Bewährte Praktiken für Compute Engine
Übung: Konfigurieren, Verwenden und Überwachen von VM-Service-Konten und -Bereichen
Sicherung von Cloud-Daten: Techniken und bewährte Praktiken
Cloud-Speicher IAM-Berechtigungen und ACLs
Prüfung von Cloud-Daten
Signierte URLs und Grundsatzdokumente
Verschlüsselung mit vom Kunden verwalteten Verschlüsselungscodes (CMEK) und vom Kunden bereitgestellten Verschlüsselungscodes (CSEK)
Wolke HSM
BigQuery IAM-Rollen und autorisierte Ansichten
Bewährte Praktiken bei der Lagerung
Übung: Verwendung von kundenseitig bereitgestellten Verschlüsselungsschlüsseln mit Cloud-Speicher
Übung: Verwendung von kundenverwalteten Verschlüsselungsschlüsseln mit Cloud-Speicher und Cloud-KMS
Übung: Erstellen einer BigQuery-autorisierten Ansicht
Sicherung von Anwendungen: Techniken und bewährte Praktiken
Arten von Sicherheitslücken in Anwendungen
Web Security Scanner
Bedrohung Identität und OAuth-Phishing
Identitätsbewusster Proxy
Secret Manager
Labor: Schwachstellen von Identitätsanwendungen mit Security Command Center
Übung: Absicherung von Compute Engine-Anwendungen mit BeyondCorp Enterprise
Übung: Konfigurieren und Verwenden von Berechtigungsnachweisen mit Secret Manager
Absicherung der Google Kubernetes Engine: Techniken und bewährte Praktiken
Arten von Sicherheitslücken in Anwendungen
Web Security Scanner
Bedrohung: Identitäts- und OAuth-Phishing
Identitätsbewusster Proxy
Secret Manager
Schutz vor verteilten Denial-of-Service-Angriffen (DDoS)
Wie DDoS-Angriffe funktionieren
Abschwächungen der Google Cloud
Arten von ergänzenden Partnerprodukten
Übung: Konfigurieren von Traffic Blocklisting mit Google Cloud Armor
Inhaltsbezogene Schwachstellen: Techniken und bewährte Praktiken
Bedrohung: Ransomware
Abschwächung von Ransomware
Bedrohungen: Datenmissbrauch, Verletzung der Privatsphäre, sensible Inhalte
Inhaltliche Abschwächung
Schwärzen von sensiblen Daten mit der DLP-API
Labor: Schwärzen sensibler Daten mit DLP API
Überwachung, Protokollierung, Auditierung und Scannen
Sicherheitskommandozentrale
Cloud-Überwachung und Cloud-Protokollierung
Cloud Audit Logs
Automatisierung der Cloud-Sicherheit
Übung: Konfigurieren und Verwenden von Cloud Monitoring und Cloud Logging
Übung: Konfigurieren und Anzeigen von Cloud-Audit-Protokollen

ExperTeach Benelux B.V.
Ceresstraat 1· 4811 CA Breda· Phone: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach-training.com