

Security in Google Cloud

In diesem Kurs erwerben Sie umfassendes Wissen über Sicherheitskontrollen und -techniken in der Google Cloud. Durch eine Kombination aus Vorträgen, Live-Demonstrationen und praxisnahen Übungen lernen Sie, die Bausteine einer sicheren Google-Cloud-Lösung zu verstehen und umzusetzen. Sie arbeiten mit leistungsstarken Tools und Diensten wie Cloud Identity, Identity and Access Management (IAM), Cloud Load Balancing, Cloud IDS, Web Security Scanner, BeyondCorp Enterprise und Cloud DNS, um Sicherheit auf höchstem Niveau zu gewährleisten.

Kursinhalt

- Grundlagen der Google Cloud-Sicherheit
- Sicherung des Zugriffs auf Google Cloud
- Identitäts- und Zugriffsmanagement (IAM)
- Konfigurieren der Virtual Private Cloud für Isolierung und Sicherheit
- Absicherung der Compute Engine: Techniken und bewährte Praktiken
- Sicherung von Cloud-Daten: Techniken und bewährte Praktiken
- Sicherung von Anwendungen: Techniken und bewährte Praktiken
- Absicherung der Google Kubernetes Engine: Techniken und bewährte Praktiken
- Schutz vor verteilten Denial-of-Service-Angriffen (DDoS)
- Inhaltsbezogene Schwachstellen: Techniken und bewährte Praktiken
- Überwachung, Protokollierung, Auditierung und Scannen

In diesem Kurs erwerben Sie die folgenden Fähigkeiten:

- Erkennen Sie die Grundlagen der Google Cloud-Sicherheit.
- Verwalten Sie Verwaltungsidentitäten mit Google Cloud.
- Implementieren Sie die Benutzerverwaltung mit Identity and Access Management (IAM).
- Konfigurieren Sie Virtual Private Clouds (VPCs) für Isolierung, Sicherheit und Protokollierung.
- Anwendung von Techniken und Best Practices für die sichere Verwaltung der Compute Engine.
- Anwendung von Techniken und Best Practices für die sichere Verwaltung von Google Cloud-Daten.
- Anwendung von Techniken und bewährten Verfahren zur Sicherung von Google Cloud-Anwendungen.
- Anwendung von Techniken und bewährten Verfahren zur Sicherung von Ressourcen der Google Kubernetes Engine (GKE).
- Verwalten Sie den Schutz vor verteilten Denial-of-Service-Angriffen (DDoS).
- Verwalten Sie inhaltsbezogene Schwachstellen.
- Implementieren Sie Lösungen für die Überwachung, Protokollierung, Prüfung und Überprüfung von Google Cloud.

Offizielle Google Cloud Unterlagen.

Zielgruppe

- Analysten, Architekten und Ingenieure im Bereich Cloud-Informationssicherheit.
- Experten für Informations- und Cybersicherheit.
- Architekten für Cloud-Infrastrukturen.

Voraussetzungen

- Vorheriger Abschluss eines Google Cloud Fundamentals: Core Infrastructure oder gleichwertige Erfahrung
- Kenntnisse grundlegender Konzepte der Informationssicherheit durch Erfahrung
- Grundlegende Kenntnisse im Umgang mit Befehlszeilentools und Linux-Betriebssystemumgebungen
- Erfahrung im Systembetrieb, einschließlich der Bereitstellung und Verwaltung von Anwendungen, entweder vor Ort oder in einer öffentlichen Cloud-Umgebung
- Leseverständnis von Code in Python oder JavaScript
- Grundlegendes Verständnis der Kubernetes-Terminologie

Stand 04.02.2026

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/GCSP

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in Deutschland	3 Tage CHF 2.085,-
Termine in Österreich	3 Tage CHF 2.085,-
Online Training	3 Tage CHF 2.085,-
Termin/Kursort	Kurssprache Deutsch
08.04.-10.04.26 Düsseldorf	26.08.-28.08.26 Online
08.04.-10.04.26 Online	26.08.-28.08.26 Wien
24.06.-26.06.26 München	21.10.-23.10.26 Online
24.06.-26.06.26 Online	



Inhaltsverzeichnis

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

