Formation Sécuriser GCP : IAM, chiffrement & monitoring

Informations

Durée : 3 jours (21h.)

Tarif* : Nous consulter

Réf : GCPS

Niveau : Facile

intra

Mise à jour le 18/12/25

*tarif valable jusqu'au 31/12/2026

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Connaissances de base en GCP (Compute, IAM, Réseaux)
- Notions en sécurité des systèmes et réseaux
- Expérience pratique avec la console GCP ou gcloud CLI

Objectifs

Objectifs pédagogiques :

- Comprendre les enjeux de la sécurité dans le cloud et le modèle de responsabilité partagée
- Maîtriser les concepts de gestion des identités et des accès (IAM)
- Protéger les données sensibles avec KMS et Secret Manager
- Déployer une stratégie de supervision et de réponse aux menaces avec Security Command Center

Objectifs opérationnels :

- Mettre en place une stratégie de sécurité complète sur GCP : configurer des identités IAM granulaires, protéger les données via chiffrement et gestion des secrets, et activer la surveillance et les alertes via le Security Command Center pour détecter et réagir aux menaces en production.

Programme

Jour 1 – Fondamentaux de la sécurité GCP & IAM

Le modèle de sécurité Google : responsabilité partagée
Présentation des outils et services de sécurité GCP
IAM (Identity & Access Management) : rôles prédéfinis, personnalisés et basés sur des conditions
Meilleures pratiques de gestion des accès (least privilege)
Service Accounts et Workload Identity
Lab pratique : mise en place d’un projet avec IAM granulaire et rôles conditionnels

Jour 2 – Chiffrement, gestion des clés & secrets

Cloud KMS (Key Management Service) : gestion centralisée des clés de chiffrement
Clés gérées par Google vs clés gérées par le client (CMEK)
Rotation et audit des clés
Secret Manager : stockage et gestion des secrets (mots de passe, API keys)
Gestion des versions et rotation automatique
Lab pratique : intégrer KMS et Secret Manager dans une application Cloud Run

Jour 3 – Supervision & sécurité opérationnelle

Security Command Center (SCC) : détection des menaces et gestion des vulnérabilités
Intégration avec Cloud Logging & Monitoring
Workflows d’alerting et remédiation
Autres outils de sécurité GCP : VPC Service Controls, Identity-Aware Proxy (IAP), Cloud Armor (protection DDoS)
Projet fil rouge : sécurisation complète d’un projet GCP (IAM, chiffrement, secrets, supervision SCC)