Google Cloud Platform - Sécurité

Contrôles et techniques de sécurité sur Google Cloud Platform

A distance

21 h | Prix inter : 2.650,00 € HT | Réf.: CC408

Idéal en Distanciel

Cette formation donne aux participants un aperçu approfondi des contrôles et techniques de sécurité sur Google Cloud Platform. À travers des présentations, des démonstrations et des ateliers pratiques, les participants découvrent et déploient les composants d'une solution GCP sécurisée. Ils apprennent également des techniques d'atténuation des risques d'attaques pouvant survenir en de nombreux points d'une infrastructure basée sur GCP, telles que des attaques par déni de service distribué (DDoS) ou par hameçonnage, ou des menaces impliquant une classification et une utilisation de contenu.
Cette formation prépare à la certification Google Professional Cloud Security Engineer.

A qui s'adresse cette formation ?

Pour qui

- Analystes, architectes et ingénieurs en sécurité de l'information
- Spécialistes en sécurité de l'information / cybersécurité
- Architectes d'infrastructure cloud, développeurs d'applications cloud

Prérequis

- Avoir suivi la formation "Google Cloud Platform - Les fondamentaux de l'infrastructure" (CC380) ou connaissances équivalentes
- Connaissances des concepts fondamentaux de la sécurité de l'information
- Compétences de base avec les outils de ligne de commande et les environnements de système d'exploitation Linux
- Posséder une expérience des opérations de systèmes, y compris le déploiement et la gestion d'applications, sur site ou dans un environnement de cloud public
- Compréhension du code en Python ou JavaScript

Programme

1 - Fondements de la sécurité GCP

- Comprendre le modèle de responsabilité partagée en matière de sécurité GCP
- Comprendre l'approche de Google Cloud en matière de sécurité
- Comprendre les types de menaces atténuées par Google et par GCP
- Définir et comprendre la transparence d'accès et l'approbation d'accès (bêta)

2 - Cloud Identity

- Cloud Identity
- Synchronisation avec Microsoft Active Directory à l'aide de Google Cloud Directory Sync
- Utilisation du service géré pour Microsoft Active Directory (version bêta)
- Choix entre l'authentification Google et l'authentification unique basée sur SAML
- Meilleures pratiques, y compris la configuration DNS, les comptes de super administrateur
- Lab : Définition d'utilisateurs avec Cloud Identity Console

3 - Gestion des identité, des accès et des clés

- GCP Resource Manager : projets, dossiers et organisations
- Rôles GCP IAM, y compris les rôles personnalisés
- Stratégies GCP IAM, y compris les stratégies d'organisation
- Labels GCP IAM
- GCP IAM Recommender
- Outil de dépannage GCP IAM
- Journaux d'audit GCP IAM
- Les meilleures pratiques, y compris la séparation des fonctions et le moindre privilège, l'utilisation de groupes Google dans les politiques et éviter l'utilisation des rôles primitifs
- Lab : Configuration de Cloud IAM, y compris les rôles personnalisés et l'organisation de stratégies

4 - Configurer un Google Virtual Private Cloud pour l'isolement et sécurité

- Configuration des pare-feu VPC (règles d'entrée et de sortie)
- Équilibrage de charge et politiques SSL
- Accès privé à l'API Google
- Utilisation du proxy SSL
- Meilleures pratiques pour les réseaux VPC, y compris l'homologation et le VPC partagé utilisation, utilisation correcte des sous-réseaux
- Meilleures pratiques de sécurité pour les VPN
- Considérations de sécurité pour les options d'interconnexion et d'appairage
- Produits de sécurité disponibles auprès des partenaires
- Définir un périmètre de service, y compris des ponts de périmètre
- Configuration de la connectivité privée aux API et services Google
- Lab : Configuration des pare-feu VPC

5 - Sécurisation de Compute Engine : techniques et meilleures pratiques

- Comptes de service Compute Engine, par défaut et définis par le client
- Rôles IAM pour les machines virtuelles
- Scope d'APIs pour les machines virtuelles
- Gestion des clés SSH pour les machines virtuelles Linux
- Gestion des connexions RDP pour les machines virtuelles Windows
- Contrôles de stratégie de l'organisation : images approuvées, adresse IP publique, désactivation du port série
- Chiffrement des images de machine virtuelle avec des clés de chiffrement gérées par le client et avec des clés de chiffrement fournies par le client
- Recherche et correction de l'accès public aux machines virtuelles
- Meilleures pratiques, notamment l'utilisation d'images personnalisées renforcées, comptes de service personnalisés (pas le compte de service par défaut), scope d'APIs personnalisés et l'utilisation des informations d'identification par défaut de l'application au lieu de clés gérées par l'utilisateur
- Chiffrement des disques VM avec des clés de chiffrement fournies par le client
- Utilisation de machines virtuelles blindées pour maintenir l'intégrité des machines virtuelles
- Lab : Configuration, utilisation et audit des comptes et des étendues de service de machine virtuelle
- Lab : Chiffrement de disques avec des clés de chiffrement fournies par le client

6 - Sécurisation des données cloud : techniques et meilleures les pratiques

- Cloud Storage et autorisations IAM
- Cloud Storage et ACLs
- Audit des données cloud, y compris la recherche et la correction données accessibles publiquement
- URL signées de Cloud Storage
- Signed policy documents
- Chiffrement des objets Cloud Storage avec des clés de chiffrement gérées par le client et avec des clés de chiffrement fournies par le client
- Meilleures pratiques, y compris la suppression de versions archivées d'objets après rotation des clés
- Vues autorisées par BigQuery
- Rôles BigQuery IAM
- Meilleures pratiques, notamment préférer les autorisations IAM aux ACL
- Lab : Utilisation de clés de chiffrement fournies par le client avec Cloud Storage
- Lab : Utilisation de clés de chiffrement gérées par le client avec Cloud Storage et Cloud KMS
- Lab : Création d'une vue autorisée BigQuery

7 - Sécurisation des applications : techniques et meilleures pratiques

- Types de vulnérabilités de sécurité des applications
- Protections DoS dans App Engine et les Cloud Functions

- Cloud Security Scanner
- Identity Aware Proxy
- Lab : Utilisation de Cloud Security Scanner pour rechercher des vulnérabilités dans une application App Egine
- Lab : Configurer Identity Aware Proxy pour protéger un projet

8 - Sécuriser Kubernetes : techniques et meilleures pratiques

- Autorisation
- Sécurisation des charges de travail
- Sécurisation des clusters
- Journalisation et surveillance

9 - Protéger contre les attaques Distributed Denial of Service

- Fonctionnement des attaques DDoS
- Mitigations : GCLB, Cloud CDN, autoscaling, pare-feu VPC ingress et egress, Cloud Armor (y compris son langage de règles)
- Types de produits partenaires complémentaires
- Lab : Configuration de GCLB, CDN, blacklister du trafic avec Cloud Armor

10 - Protéger contre les vulnérabilités liées au contenu

- Menace : Ransomware
- Atténuations : sauvegardes, IAM, Data Loss Prevention API
- Menaces : utilisation abusive des données, violations de la vie privée, contenu sensible / restreint / inacceptable
- Menace : phishing d'identité et Oauth
- Atténuation : classification du contenu à l'aide des API Cloud ML ; numérisation et rédaction de données à l'aide de l'API Data Loss Prevention
- Lab : Rédaction de données sensibles avec l'API Data Loss Prevention

11 - Surveillance, journalisation, audit et numérisation

- Security Command Center
- Surveillance et journalisation Stackdriver
- Journaux de flux VPC
- Journalisation d'audit cloud
- Déployer et utiliser Forseti
- Lab : Installation d'agents Stackdriver
- Lab : Configuration et utilisation de la surveillance et de la journalisation Stackdriver
- Lab : Affichage et utilisation des journaux de flux VPC dans Stackdriver
- Lab : Configuration et affichage des journaux d'audit dans Stackdriver
- Lab : Inventorier un déploiement avec Forseti Inventory (démo)
- Lab : Analyse d'un déploiement avec Forseti Scanner (démo)

Les objectifs de la formation

- Comprendre l'approche Google en matière de sécurité
- Gérer des identités d'administration à l'aide de Cloud Identity
- Implémenter un accès administrateur avec un principe de moindre privilège à l'aide de Google Cloud Resource Manager et Cloud IAM
- Implémenter des contrôles de trafic IP à l'aide de pare-feu VPC et de Cloud Armor
- Implémenter la fonctionnalité Identity-Aware Proxy
- Analyser les modifications apportées à la configuration ou aux métadonnées des ressources à l'aide des journaux d'audit GCP
- Être capable de sécuriser un environnement Kubernetes
- Détecter des données sensibles et les masquer à l'aide de l'API Data Loss Prevention
- Analyser un déploiement GCP à l'aide de Forseti
- Résoudre les problèmes liés aux principaux types de faille, et plus particulièrement dans le cas d'un accès public aux données et aux machines virtuelles

Evaluation

- Cette formation fait l'objet d'une évaluation formative.

Les points forts de la formation

- Une formation complète durant laquelle s'alternent les phases d'apports théoriques, de démonstrations et de travaux pratiques.
- Les consultants spécialistes de la technologie apportent leurs conseils et leur expérience.
- Une formation animée par un formateur certifié Google Cloud Platform.
- La qualité d'une formation officielle Google (support de cours en anglais).
- 82% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates 2026 - Référence CC408

Dernières places disponibles Session garantie

du 4 févr. au 6 févr.	du 4 août au 6 août
du 20 mai au 22 mai	du 23 nov. au 25 nov.