Google Cloud Platform - Sécurité

Référence : **GCP300SEC** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Avoir suivi la formation Google Cloud Platform Fundamentals: Core Infrastructure ou avoir une expérience équivalente. • Avoir suivi la formation Networking in Google Cloud Platform ou avoir une expérience équivalente. • Certificate authorities. • Certificates. • Cipher types. • Compétence de base avec les outils de ligne de commande et les environnements de système d'exploitation Linux. • Compréhension du code en Python ou JavaScript. • Concepts fondamentaux:. • confidentiality, integrity, availability. • Connaissance des concepts fondamentaux de la sécurité de l'information:. • Expérience des opérations de systèmes, y compris le déploiement et la gestion d'applications, sur site ou dans un environnement de cloud public. • Key width. • Public and private key pairs. • Public key infrastructures. • Public-key cryptography. • Security policy. • Transport Layer Security/Secure Sockets Layer encrypted communication. • Types de menaces courantes et leurs stratégies d'atténuation. • vulnerability, threat, attack surface.

PROFIL DES STAGIAIRES

• Analystes, architectes et ingénieurs en sécurité de l'information. • Architectes d'infrastructure cloud. • En outre, le cours est destiné à Google et au personnel de terrain partenaire qui travaille avec des clients dans ces rôles. Le cours devrait également être utile aux développeurs d'applications cloud. • Spécialistes en sécurité de l'information / cybersécurité.

OBJECTIFS

• Comprendre l'approche de Google en matière de sécurité. • Gestion des identités administratives à l'aide de Cloud Identity.. • Implémentation de l'accès administratif au moindre privilège à l'aide de Google Cloud Resource Manager, Cloud IAM.. • Implémentation de contrôles de trafic IP à l'aide de pare-feu VPC et de Cloud Armor. • Implémentation des modifications Identity Aware Proxy Analyzing de la configuration ou des métadonnées des ressources avec les journaux d'audit GCP. • Recherche et expurgation de données sensibles avec l'API Data Loss Prevention. • Analyse d'un déploiement GCP avec Forseti. • Correction d'importants types de vulnérabilités, en particulier dans l'accès public aux données et aux machines virtuelles.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Cloud

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Fondations 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)

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

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

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

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
- Chiffrement de disques avec des clés de chiffrement fournies par le client

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
- Utilisation de clés de chiffrement gérées par le client avec Cloud Storage et Cloud KMS
- Création d'une vue autorisée BigQuery

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
- Configurer Identity Aware Proxy pour protéger un projet

Sécuriser Kubernetes: techniques et meilleures pratiques

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

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

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

Monitoring, Logging, Auditing, et Scanning

- Security Command Center
- Surveillance et journalisation Stackdriver
- Journaux de flux VPC
- Journalisation d'audit cloud
- Déployer et utiliser Forseti

Lab:

- Installation d'agents Stackdriver
- Configuration et utilisation de la surveillance et de la journalisation Stackdriver
- Affichage et utilisation des journaux de flux VPC dans Stackdriver
- Configuration et affichage des journaux d'audit dans Stackdriver
- Inventorier un déploiement avec Forseti Inventory (démo)
- Analyse d'un déploiement avec Forseti Scanner (démo)