

Google Cloud Platform - Sécurité

Référence : **GCP300SEC**

Durée : **3 jours (21 heures)**

Certification : **Aucune**

Connaissances préalables

- 1-Avoir suivi la formation Suivi GCP100A - Google Cloud Fundamentals: Core Infrastructure ou avoir des connaissances équivalentes
- 2-Avoir suivi la formation GCP200N - Networking in Google Cloud ou avoir des connaissances équivalentes
- 3-Connaître les concepts fondamentaux de la sécurité de l'information, par l'expérience ou par une formation en ligne telle que la formation de SANS SEC301: Introduction to Cyber Security
- 4-Avoir des compétences de base avec les outils de ligne de commande et les environnements de système d'exploitation Linux
- 5-Avoir une expérience de l'exploitation des systèmes, y compris le déploiement et la gestion d'applications, sur site ou dans un environnement de cloud public
- 6-Compréhension de base de lecture de code en Python ou Javascript
- 7-Compréhension de base de la terminologie de Kubernetes (souhaité mais pas obligatoire)

Profil des stagiaires

- 1-Analystes, architectes et ingénieurs en sécurité de l'information dans le cloud
- 2-Spécialistes en sécurité de l'information/cybersécurité
- 3-Architectes d'infrastructure cloud

Objectifs

- Identifier les fondements de la sécurité Google Cloud.
- Gérer les identités d'administration avec Google Cloud.
- Implémenter l'administration des utilisateurs avec Identity and Access Management (IAM).
- Configurer des Virtual Private Clouds (VPC) pour l'isolation, la sécurité et la journalisation.
- Appliquer des techniques et des bonnes pratiques pour gérer en toute sécurité Compute Engine.
- Appliquer des techniques et des bonnes pratiques pour gérer en toute sécurité les données Google Cloud.
- Appliquer des techniques et des bonnes pratiques pour sécuriser les applications Google Cloud.
- Appliquer des techniques et des bonnes pratiques pour sécuriser les ressources Google Kubernetes Engine (GKE).
- Gérer la protection contre les attaques par déni de service distribué (DDoS).
- Gérer les vulnérabilités liées au contenu.
- Mettre en œuvre les solutions de surveillance, de journalisation, d'audit et d'analyse de Google Cloud

Certification préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 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 et de réflexions

Formateur·rice

- Consultant-Formateur expert Cloud

Méthodes d'évaluation des acquis

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

Contenu du cours

1. Les bases de la sécurité Google Cloud

- L'approche de Google Cloud en matière de sécurité
- Le modèle de responsabilité partagée en matière de sécurité
- Menaces atténuées par Google et Google Cloud
- Accéder à la transparence

2. Sécuriser l'accès à Google Cloud

- Identité Cloud
- Synchronisation d'annuaire Google Cloud
- Microsoft AD géré
- Authentification Google par rapport à l'authentification unique basée sur SAML
- Plate-forme d'identité
- Meilleures pratiques d'authentification
- Démonstration : Définir des utilisateurs avec Cloud Identity Console

3. Identity and Access Management (IAM)

- Gestionnaire de ressources
- Rôles IAM
- Comptes de service
- Politiques IAM et d'Organization
- Fédération d'identité de charge de travail
- Intelligence politique
- Exemple de Travaux Pratiques : Configuration d'IAM

4. Configuration du cloud privé virtuel pour l'isolation et la sécurité

- Pare-feu VPC
- Équilibrage de charge et politiques SSL
- Options d'interconnexion et d'appairage
- VPC Service Controls
- Access Context Manager
- VPC Flow Logs
- Cloud IDS
- Exemple de Travaux Pratiques : Configuration des pare-feu VPC
- Démonstration : Sécuriser des projets avec VPC Service Controls

5. Sécuriser Compute Engine : techniques et bonnes pratiques

- Service accounts, rôles IAM et champs d'application d'API
- Gestion des connexions aux VM
- Contrôles de la politique de l'Organization
- Shielded VMs et Confidential VMs
- Certificate Authority Service
- Bonnes pratiques de Compute Engine
- Exemple de Travaux Pratiques : Configuration, utilisation et audit des comptes de service et des étendues de VM

6. Securing Cloud Data: Techniques and Best Practices

- Autorisations Cloud Storage IAM et LCA
- Audit des données cloud
- URL et documents de politique signés
- Chiffrement avec CMEK et CSEK
- HSM cloud
- Rôles BigQuery IAM et vues autorisées
- Meilleures pratiques de stockage
- Exemples de Travaux Pratiques : Utilisation des clés de chiffrement fournies par le client avec Cloud Storage

7. Sécurisation des applications : techniques et bonnes pratiques

- Types de vulnérabilités de sécurité des applications
- Web Security Scanner
- Menace : hameçonnage d'identité et OAuth
- Identity-Aware Proxy
- Secret Manager
- Exemple de Travaux Pratiques : Utiliser Web Security Scanner pour rechercher des vulnérabilités dans une application App Engine

8. Sécuriser Google Kubernetes Engine : techniques et bonnes pratiques

- Authentification et autorisation
- Durcissement de vos clusters
- Sécurisation de vos charges de travail
- Surveillance et journalisation

9. Protection contre les attaques par déni de service distribué (DDoS)

- Comment fonctionnent les attaques DDoS
- Atténuations Google Cloud
- Types de produits partenaires complémentaires
- Exemple de Travaux Pratiques : Configurer la liste de blocage du trafic avec Google Cloud Armor

10. Vulnérabilités liées au contenu : techniques et bonnes pratiques

- Menace : rançongiciel
- Atténuation des ransomwares
- Menaces : utilisation abusive des données, violation de la vie privée, contenu sensible
- Atténuation liée au contenu
- Masquer les données sensibles avec l'API DLP
- Exemple de Travaux Pratiques : Masquer les données sensibles avec l'API DLP

11. Surveillance, journalisation, audit et analyse

- Centre de commandement de la sécurité
- Surveillance dans le cloud et journalisation dans le cloud
- Journaux d'audit cloud
- Automatisation de la sécurité dans le cloud
- Exemples de Travaux Pratiques : Configurer et utiliser Cloud Monitoring et Cloud Logging

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:01.71.19.70.30) ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.