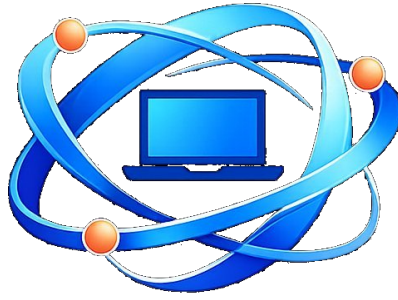




MFE-IT

Référence: GCP-PCSE

Formation Google Cloud Professional Cloud Security Engineer

Sécuriser les infrastructures et les données sur Google Cloud

Durée : 4 jours | Heures : 28 h

Distanciel • Sessions garanties dès 1 inscrit • 60% de pratique

Description

Cette formation prépare à la certification Google Cloud Professional Cloud Security Engineer. En petit groupe de 1 à 3 participants, vous apprenez à concevoir, mettre en œuvre et exploiter des contrôles de sécurité sur Google Cloud : gestion des identités et des accès, protection de l'infrastructure et des données, détection et réponse, conformité et gouvernance.

La formation alterne théorie et ateliers pratiques sur un environnement Google Cloud, pour acquérir les réflexes d'un ingénieur sécurité cloud.

Objectifs pédagogiques

À l'issue de la formation, le participant sera capable de :

- Concevoir et gérer les identités et les accès (IAM, comptes de service, fédération).
- Sécuriser le réseau : VPC Service Controls, pare-feu, Cloud Armor, segmentation.
- Protéger les données : chiffrement, gestion des clés (KMS), DLP.
- Mettre en œuvre la détection et la réponse avec Security Command Center.
- Assurer la conformité, l'audit et la gouvernance.
- Appliquer les bonnes pratiques de sécurité dès la conception (security by design).

Prérequis

Pour suivre cette formation dans de bonnes conditions, il est recommandé de :

- Bonnes bases en sécurité informatique et en réseau.
- Expérience pratique de Google Cloud (niveau Associate Cloud Engineer recommandé).
- Notions de cryptographie et de gestion des identités.
- Un entretien préalable permet d'adapter le contenu au profil et aux objectifs de chaque participant.

Parce que chaque participant est unique, un entretien préalable est systématiquement organisé en amont avec notre expert afin de concevoir un programme de formation parfaitement aligné sur ses objectifs, son niveau et ses enjeux professionnels.

Public visé

- Ingénieurs et architectes sécurité cloud.
- Analystes SecOps et équipes SOC.
- Administrateurs cloud en charge de la sécurité.
- Profils préparant la certification Professional Cloud Security Engineer.

Programme détaillé

Le programme alterne apports théoriques et travaux pratiques (environ 60 %). Les modules s'articulent autour d'exercices pratiques basés sur des cas métiers réels.

Identités et accès

- IAM avancé : rôles, conditions, comptes de service.
- Fédération d'identités et Cloud Identity.
- Atelier : concevoir un modèle d'accès au moindre privilège.

Sécurité du réseau

- VPC Service Controls, périmètres et segmentation.
- Pare-feu, Cloud Armor et protection contre les attaques.
- Atelier : sécuriser une architecture réseau.

Protection des données

- Chiffrement au repos et en transit ; Cloud KMS et CMEK.
- Data Loss Prevention (DLP) et classification des données.
- Atelier : protéger des données sensibles.

Détection et réponse

- Security Command Center : posture et menaces.
- Journalisation, audit et supervision de sécurité.
- Atelier : détecter et investiguer un incident.

Conformité et gouvernance

- Résidence des données, conformité réglementaire.
- Organization Policy et gouvernance à l'échelle.
- Atelier : appliquer des contrôles de gouvernance.

Préparation à l'examen PCSE

- Revue des domaines de l'examen.
- Questions de type scénario.
- Atelier de synthèse : durcir une solution de bout en bout.

Les plus de cette formation

- Prépare à la certification Professional Cloud Security Engineer
- Couvre IAM, réseau, données, détection et gouvernance
- Approche praticien sur un environnement Google Cloud réel
- Groupes de 1 à 3 participants pour un accompagnement individualisé

Modalités pédagogiques

Format et modalités

La formation est dispensée à distance via une classe virtuelle interactive et peut être enregistrée sur demande. Elle peut aussi être dispensée sur site, avec un contenu adapté aux besoins de votre projet professionnel. La répartition théorie/pratique est d'environ 40 %/60 %.

Format ultra-personnalisé MFE-IT

Chaque session accueille entre 1 et 3 participants, garantissant un accompagnement très individualisé. Un entretien préalable permet d'adapter le contenu au profil de chaque participant. Les sessions inter-entreprises sont garanties dès 1 inscrit (sauf cas de force majeure).

Évaluation des acquis

Tout au long de la formation, le formateur évalue la progression des participants via des QCM, des mises en situation et des travaux pratiques. À l'issue, une attestation de validation des acquis est remise à chaque participant.

Suivi post-formation

Pendant un mois après la formation, chaque participant peut contacter les formateurs MFE-IT pour toute question sur la mise en œuvre des connaissances acquises. Une réponse est apportée par e-mail ou téléphone sous 48 heures ouvrées.

Accessibilité

MFE-IT s'engage à accueillir les personnes en situation de handicap. Contact : contact@mfe-it.com.

Informations pratiques

Ressources formateur

- Démonstrations structurées alignées sur le programme détaillé
- Énoncés d'exercices et corrigés tout au long de la formation
- Un environnement technique prêt à l'emploi pour les ateliers pratiques
- Validation des acquis par le formateur à la fin de chaque atelier
- Documents de référence numériques

Certification et validation

À l'issue de la formation, une attestation est envoyée par e-mail précisant les objectifs, la nature, la durée et les résultats de l'évaluation. Un certificat de réalisation peut également être fourni sur demande.

Bénéfices pour les participants

- Se former depuis son lieu de travail ou son domicile, sans déplacement
- Bénéficier d'un formateur-consultant expert du sujet
- Profiter d'un format ultra-personnalisé (1 à 3 participants)
- Poursuivre la formation même en cas d'imprévu

Bénéfices pour l'organisation

- Optimiser le budget formation en réduisant les frais de déplacement et d'hébergement

- Offrir une formation de qualité à tous les collaborateurs, où qu'ils soient
- Réduire le temps d'absence lié aux déplacements
- Accompagner la montée en compétences des équipes dans tous les contextes