DAWAN

Plan de la formation

www.dawan.fr

Formation Google Cloud Platform : Professional Cloud Security Engineer

Durée :	1 jours (7 heures)
Tarif inter-entreprise :	1 175,00 € HT (standard) 940,00 € HT (remisé)
Public :	Développeurs, responsables d'exploitation de systèmes et architectes de solutions qui débutent avec Google Cloud Cadres dirigeants / décisionnaires ou toute personne prévoyant de déployer des applications et de créer des environnements applicatifs sur Google Cloud
Pré-requis :	Des connaissances de base sur le développement d'applications, l'exploitation de systèmes, les systèmes d'exploitation Linux et l'analyse de données/le machine learning seront utiles pour comprendre les technologies présentées
Objectifs :	Configurer et gérer l'accès et les identités dans un environnement cloud sécurisé - Assurer la protection des données (chiffrement, gestion des clés, protection au repos et en transit) - Configurer des défenses réseau et sécuriser les communications entre ressources cloud - Gérer les opérations de sécurité, incluant la surveillance des environnements et la réponse aux incidents - Soutenir les exigences de conformité réglementaire et appliquer des contrôles appropriés - Être préparé à passer la certification Professional Cloud Security Engineer
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.

Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CLO102963-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Gérer l’accès et les identités dans un environnement cloud sécurisé

Comprendre le rôle des identités et des accès dans la sécurisation d’un environnement Google Cloud
Structurer une logique d’authentification et d’autorisation adaptée aux usages
Appliquer les principes de moindre privilège et de séparation des responsabilités
Relier gestion des identités, gouvernance et exploitation sécurisée
Identifier les points de vigilance liés aux comptes, rôles et permissions
Mettre en cohérence sécurité des accès et organisation des environnements cloud

Atelier fil rouge
Définir une stratégie d’accès et d’identités pour un environnement Google Cloud comportant plusieurs profils d’utilisateurs et plusieurs niveaux de responsabilité

Protéger les données avec le chiffrement, la gestion des clés et les contrôles adaptés

Comprendre les enjeux de protection des données au repos et en transit
Relier chiffrement, gestion des clés et exigences de sécurité

Identifier les niveaux de protection adaptés selon la sensibilité des données
Prendre en compte les besoins de confidentialité, de traçabilité et d'exploitation
Mettre en relation sécurité des données, architecture applicative et conformité
Intégrer la protection des données dans une logique globale de sécurisation cloud

Atelier fil rouge
Qualifier les mécanismes de protection à mettre en œuvre pour plusieurs catégories de données dans un environnement Google Cloud

Sécuriser les réseaux et les communications entre ressources cloud

Comprendre les grands principes de sécurité réseau dans Google Cloud
Identifier les mécanismes contribuant à la sécurisation des flux et des communications entre ressources
Relier segmentation, contrôle des accès réseau et réduction de la surface d'attaque
Prendre en compte les communications entre services, applications et environnements
Concevoir une défense réseau cohérente avec le niveau d'exposition des ressources
Mettre en perspective sécurité réseau, performance et simplicité d'exploitation

Atelier fil rouge
Analyser les flux d'une architecture Google Cloud simple et proposer les mesures de sécurisation réseau prioritaires

Gérer les opérations de sécurité et la réponse aux incidents

Comprendre les principes de surveillance de sécurité dans Google Cloud
Identifier les événements et signaux utiles à la détection d'anomalies
Relier supervision, détection, investigation et remédiation
Qualifier les premiers niveaux de réponse à incident dans un environnement cloud
Structurer une logique de surveillance continue compatible avec les besoins d'exploitation
Mettre en place une lecture opérationnelle des incidents de sécurité

Atelier fil rouge
Analyser un scénario d'incident de sécurité sur Google Cloud et proposer une démarche de détection, d'investigation et de première réponse

Soutenir les exigences de conformité réglementaire et appliquer des contrôles appropriés

Comprendre le lien entre exigences réglementaires, sécurité cloud et contrôles techniques

Identifier les principaux enjeux de conformité dans un environnement Google Cloud
Relier gouvernance, journalisation, accès, sécurité des données et auditabilité
Choisir des contrôles appropriés selon le niveau de criticité et de contrainte
Structurer une approche de conformité intégrée à l'architecture et à l'exploitation
Mettre en cohérence sécurité opérationnelle et exigences de pilotage

Atelier fil rouge
Évaluer un environnement Google Cloud au regard d'exigences de conformité et proposer un ensemble cohérent de contrôles de sécurité

Préparer l'examen Professional Cloud Security Engineer

Comprendre la structure de l'examen et les domaines évalués
Identifier les attentes du niveau Professional sur Google Cloud
S'entraîner à raisonner sur des scénarios de sécurisation, d'exploitation et de conformité
Repérer les pièges fréquents dans les questions de certification
Adopter une méthode de lecture et de décision adaptée au niveau d'examen
Consolider les axes de révision avant inscription

Atelier fil rouge
Réaliser un entraînement guidé sur des questions de niveau Professional Cloud Security Engineer et corriger les réponses de manière argumentée