+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 27/03/2026

S'inscrire

Formation Certification GCP Professional Cloud Security Engineer

5 jours (35 heures)

Présentation

Google Cloud Professional Cloud Security Engineer est une certification reconnue qui valide la capacité à concevoir, implémenter et gérer des solutions sécurisées sur Google Cloud Platform.

Notre formation Certification GCP Professional Cloud Security Engineer vous permettra de maîtriser les pratiques avancées de cybersécurité cloud sur l'environnement Google Cloud.

Vous apprendrez à sécuriser les identités, les accès, les données et les infrastructures tout en intégrant les meilleures pratiques de DevSecOps.

Vous serez en mesure de protéger vos environnements, de détecter les menaces, de répondre aux incidents et de concevoir des architectures sécurisées en vous appuyant sur les services natifs de GCP comme IAM, Cloud KMS et Security Command Center.

Grâce à une approche orientée cas concrets et ateliers pratiques, cette formation vous permettra de renforcer la sécurité de vos systèmes et d'améliorer votre posture de sécurité cloud.

Comme toutes nos formations, celle-ci s'appuie sur les dernières bonnes pratiques GCP en matière de sécurité cloud, de conformité et de protection des infrastructures sur Google Cloud Platform.

Objectifs

- Maîtriser la sécurité cloud sur GCP.
- Gérer les identités et les accès avec IAM.
- Protéger les données et les infrastructures.
- Détecter et répondre aux incidents de sécurité.

- Préparer la certification GCP Cloud Security Engineer.

Public visé

- Ingénieurs cybersécurité
- Ingénieurs cloud et DevOps
- Administrateurs systèmes et réseaux
- Architectes sécurité

Pré-requis

- Connaissances en cloud computing
- Bases en réseaux et sécurité
- Expérience en administration système ou cloud

Programme de formation certification GCP Professional Cloud Security Engineer

[Jour 1 - Matin]

Fondamentaux de la sécurité cloud et environnement GCP

- Comprendre les principes de la sécurité cloud et les enjeux actuels
- Positionner la certification Professional Cloud Security Engineer
- Découvrir les services clés de Google Cloud Platform
- Comprendre le modèle de responsabilité partagée
- Identifier les principes de sécurité cloud native
- Atelier pratique : Prise en main de l’environnement GCP.

[Jour 1 - Après-midi]

Gestion des identités et des accès (IAM)

- Maîtriser les concepts avancés de IAM
- Gérer les rôles, permissions et comptes de service
- Appliquer le principe du moindre privilège
- Mettre en place des identités fédérées
- Sécuriser les accès aux ressources cloud
- Atelier pratique : Configuration des accès sécurisés.

Organisation et gouvernance des ressources

- Structurer les ressources : organisations, dossiers et projets
- Mettre en place des politiques d'organisation
- Gérer des environnements multi-projets
- Contrôler les accès et les permissions
- Mettre en œuvre l'audit et la traçabilité
- Atelier pratique : Gouvernance sécurisée d'un environnement GCP.

[Jour 2 - Matin]

Protection des données sur GCP

- Comprendre le chiffrement des données au repos et en transit
- Utiliser Cloud KMS pour la gestion des clés
- Mettre en œuvre tokenisation et anonymisation
- Gérer les secrets et accès sensibles
- Appliquer les bonnes pratiques de sécurité des données
- Atelier pratique : Mise en place du chiffrement.

[Jour 2 - Après-midi]

Gestion des accès aux données

- Contrôler les accès aux datasets
- Sécuriser BigQuery et les données analytiques
- Gérer les permissions avancées
- Mettre en place l'isolation des données
- Auditer les accès et les usages
- Atelier pratique : Sécurisation d'un dataset.

Conformité et gouvernance des données

- Comprendre les normes de sécurité (ISO, RGPD)
- Mettre en place audit et reporting
- Gérer la data governance
- Exploiter les logs pour la conformité
- Assurer la traçabilité des actions
- Atelier pratique : Mise en conformité d'un projet GCP.

[Jour 3 - Matin]

Sécurité réseau sur GCP

- Comprendre les concepts de VPC, firewall et VPN
- Segmenter les réseaux et isoler les flux
- Contrôler les communications entrantes et sortantes

- Mettre en place des architectures sécurisées
- Appliquer les bonnes pratiques réseau
- Atelier pratique : Configuration réseau sécurisé.

[Jour 3 - Après-midi]

Sécurité des workloads

- Sécuriser les machines virtuelles et conteneurs
- Appliquer la sécurité sur Kubernetes (GKE)
- Gérer les vulnérabilités systèmes
- Mettre en œuvre le hardening
- Intégrer les pratiques DevSecOps
- Atelier pratique : Sécurisation d’un workload.

Gestion des vulnérabilités

- Identifier les vulnérabilités des systèmes
- Mettre en place des scans de sécurité
- Gérer les correctifs et mises à jour
- Analyser les risques
- Utiliser les outils de sécurité GCP
- Atelier pratique : Scan et correction de vulnérabilités.

[Jour 4 - Matin]

Monitoring et détection des menaces

- Utiliser Security Command Center
- Mettre en place le monitoring sécurité
- Détecter les anomalies et comportements suspects
- Configurer des alertes pertinentes
- Analyser les logs de sécurité
- Atelier pratique : Détection de menaces sur GCP.

[Jour 4 - Après-midi]

Réponse aux incidents

- Mettre en place un processus de réponse aux incidents
- Réaliser des investigations et analyses forensic
- Automatiser les réponses aux incidents
- Gérer les crises de sécurité
- Réaliser des post-mortem
- Atelier pratique : Simulation d’incident de sécurité.

Sécurité des applications

- Appliquer les principes de sécurité applicative
- Protéger contre les attaques web
- Sécuriser les API
- Appliquer les bonnes pratiques OWASP
- Intégrer la sécurité dans le cycle DevOps
- Atelier pratique : Sécurisation d’une application.

[Jour 5 - Matin]

Architecture sécurisée sur GCP

- Concevoir une architecture sécurisée
- Appliquer les bonnes pratiques Google
- Mettre en œuvre la défense en profondeur
- Gérer des environnements multi-cloud
- Optimiser les coûts liés à la sécurité
- Atelier pratique : Conception d’une architecture sécurisée.

[Jour 5 - Après-midi]

Automatisation et DevSecOps

- Automatiser les contrôles de sécurité
- Intégrer la sécurité dans les pipelines CI/CD
- Mettre en œuvre le Policy as Code
- Sécuriser l’Infrastructure as Code
- Mettre en place un monitoring continu
- Atelier pratique : Pipeline DevSecOps sécurisé.

Préparation à la certification

- Analyser les domaines de l’examen
- Étudier des cas concrets
- Comprendre les attentes Google
- Identifier les pièges fréquents
- Mettre en place une stratégie de réussite
- Atelier pratique : Passage de l'examen blanc + correction.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à

acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.