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

Mis à jour le 24/04/2026

S'inscrire

Formation Certification GCP Professional Security Operations Engineer

4 jours (28 heures)

Présentation

Professional Security Operations Engineer est une certification Google Cloud destinée aux professionnels chargés de détecter, analyser et répondre aux incidents de sécurité dans un environnement cloud. Elle valide des compétences avancées en Security Operations, supervision, investigation, réponse aux menaces et amélioration continue de la posture sécurité.

Notre formation Certification Professional Security Operations Engineer vous permettra de maîtriser les opérations de sécurité sur Google Cloud en abordant les outils et pratiques essentiels autour du SOC, du SIEM, de la collecte de logs, de la détection des menaces et de la réponse aux incidents.

Vous apprendrez à collecter, corréler, analyser et exploiter les événements de sécurité à l'aide de services tels que Security Command Center, Cloud Logging et Google Security Operations. La formation met l'accent sur des scénarios terrain pour comprendre comment qualifier une alerte, investiguer un incident et mettre en œuvre les actions de remédiation adaptées.

À l'issue de la formation, vous serez en mesure de sécuriser les workloads cloud, d'améliorer les capacités de détection d'un SOC, d'automatiser certaines réponses et de piloter les indicateurs clés de sécurité opérationnelle dans un environnement Google Cloud.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre les principes des Security Operations sur Google Cloud

- Collecter, centraliser et exploiter les logs de sécurité
- Détecter les menaces avec Security Command Center et Google Security Operations
- Investiguer les incidents et qualifier les alertes critiques
- Mettre en œuvre des actions de réponse et de remédiation
- Préparer efficacement la certification Professional Security Operations Engineer

Public visé

- Analystes SOC et analystes cybersécurité
- Ingénieurs sécurité cloud
- Administrateurs systèmes et réseaux orientés sécurité
- Ingénieurs DevSecOps, SRE et responsables d'exploitation
- Professionnels souhaitant préparer la certification Google Cloud Security Operations Engineer

Pré-requis

- Connaissances de base en Google Cloud ou en cloud computing
- Notions en cybersécurité, réseaux et systèmes
- Compréhension des concepts de logs, alertes, incidents et vulnérabilités
- Une première expérience en SOC, exploitation ou sécurité cloud est recommandée

Formation Certification Professional Security Operations Engineer

[Jour 1 - Matin]

Comprendre les opérations de sécurité sur Google Cloud

- Définir le rôle d'un Security Operations Engineer dans un environnement cloud
- Comprendre les principes d'un SOC, d'un SIEM et d'un SOAR
- Identifier les enjeux de détection, d'analyse et de réponse aux incidents
- Découvrir l'écosystème sécurité de Google Cloud
- Positionner la certification Professional Security Operations Engineer
- Atelier pratique : Cartographier les besoins sécurité d'un environnement cloud.

[Jour 1 - Après-midi]

Mettre en place les fondamentaux de sécurité cloud

- Comprendre le modèle de responsabilité partagée
- Appliquer les bonnes pratiques IAM et le principe du moindre privilège
- Sécuriser les projets, dossiers et organisations Google Cloud
- Utiliser les politiques d'organisation et contrôles de conformité

- Identifier les erreurs de configuration à risque
- Atelier pratique : Auditer les accès IAM d’un environnement Google Cloud.

Collecter et centraliser les logs de sécurité

- Comprendre le rôle de Cloud Logging dans les opérations de sécurité
- Identifier les logs critiques : activité admin, accès aux données, réseau et workloads
- Configurer les exports et la centralisation des journaux
- Structurer les logs pour faciliter la détection et l’investigation
- Mettre en place une stratégie de rétention et d’exploitation des logs
- Atelier pratique : Configurer une collecte de logs sécurité exploitable par un SOC.

[Jour 2 - Matin]

Exploiter Security Command Center

- Découvrir les fonctionnalités de Security Command Center
- Analyser les findings, vulnérabilités et mauvaises configurations
- Prioriser les risques selon leur impact métier
- Suivre l’exposition des ressources cloud et workloads
- Mettre en place des processus de remédiation
- Atelier pratique : Analyser et prioriser les findings Security Command Center.

[Jour 2 - Après-midi]

Détecter les menaces avec Google Security Operations

- Comprendre le rôle de Google Security Operations dans un SOC cloud
- Ingestions des données de sécurité et normalisation des événements
- Rechercher des événements suspects à partir des logs collectés
- Utiliser les règles de détection et les indicateurs de compromission
- Identifier les comportements anormaux sur les identités, réseaux et workloads
- Atelier pratique : Détecter une activité suspecte à partir d’événements corrélés.

Investiguer les incidents de sécurité

- Appliquer une méthodologie d’investigation structurée
- Qualifier une alerte et déterminer son niveau de criticité
- Rechercher les traces d’un incident dans les logs et événements
- Identifier les comptes, ressources et données potentiellement impactés
- Documenter les preuves et préparer un rapport d’incident
- Atelier pratique : Mener une investigation complète sur un scénario d’attaque cloud.

[Jour 3 - Matin]

Répondre aux incidents et contenir les menaces

- Comprendre les phases de réponse aux incidents : containment, eradication, recovery
- Définir les actions prioritaires selon le type d’incident
- Isoler des ressources compromises et révoquer des accès suspects
- Coordonner la réponse entre équipes SOC, cloud, réseau et métier
- Formaliser les procédures de remédiation et de retour à la normale
- Atelier pratique : Exécuter un plan de réponse à incident sur un environnement compromis.

[Jour 3 - Après-midi]

Sécuriser les workloads, réseaux et données

- Surveiller les workloads Compute Engine, GKE, Cloud Run et services managés
- Identifier les risques liés aux configurations réseau, pare-feu et exposition publique
- Protéger les données sensibles avec chiffrement, clés et contrôles d’accès
- Détecter les comportements anormaux sur les flux réseau et services applicatifs
- Appliquer les bonnes pratiques de sécurité cloud en production
- Atelier pratique : Analyser l’exposition d’une application cloud et proposer des remédiations.

Automatiser les opérations de sécurité

- Comprendre les apports de l’automatisation dans un SOC moderne
- Créer des workflows de réponse aux alertes récurrentes
- Utiliser les notifications, fonctions serverless et intégrations de sécurité
- Réduire les faux positifs et améliorer le temps de réponse
- Structurer des playbooks de sécurité cloud
- Atelier pratique : Automatiser une action de remédiation à partir d’une alerte critique.

[Jour 4 - Matin]

Superviser les indicateurs SOC et améliorer la détection

- Définir les indicateurs clés : MTTD, MTTR, volume d’alertes et criticité
- Créer des tableaux de bord adaptés aux analystes SOC et responsables sécurité
- Mesurer la qualité des règles de détection et réduire le bruit opérationnel
- Mettre en place une boucle d’amélioration continue
- Formaliser les retours d’expérience après incident
- Atelier pratique : Construire un tableau de bord opérationnel pour le suivi sécurité.

[Jour 4 - Après-midi]

Gouvernance, conformité et reporting sécurité

- Aligner les opérations de sécurité avec les exigences de conformité
- Comprendre les référentiels utiles : NIST, ISO 27001, bonnes pratiques cloud

- Mettre en place des politiques de contrôle et de suivi des risques
- Produire des rapports lisibles pour les équipes techniques et la direction
- Structurer une démarche d’amélioration continue de la posture sécurité
- Atelier pratique : Produire un rapport de posture sécurité à partir d’un scénario cloud.

Préparation à l’examen Professional Security Operations Engineer

- Comprendre la structure de l’examen Professional Security Operations Engineer
- Réviser les domaines clés : détection, investigation, réponse, gouvernance et sécurité cloud
- Analyser les scénarios d’examen et identifier les réponses les plus adaptées
- Reconnaître les pièges fréquents liés aux opérations de sécurité Google Cloud
- Construire un plan de révision personnalisé après la formation
- Atelier pratique : Passage de l'examen blanc + corection.

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.