AYI NEDJIMI Consultants

GCP Security Command Center : Audit et Durcissement

Catégorie : Cloud Security Lecture : 8 min Publié le : 04/03/2026 Auteur : Ayi NEDJIMI

Maîtrisez Google Cloud Security Command Center pour auditer et durcir votre infrastructure GCP : findings, compliance, détection de menaces et.

Résumé exécutif

Google Cloud Security Command Center (SCC) est la plateforme centralisée de gestion de la sécurité GCP. Ce guide détaille sa configuration, l'exploitation des findings, le durcissement des ressources et les stratégies d'intégration avec les outils SOC.
Google Cloud Platform a longtemps été perçu comme le troisième cloud, loin derrière AWS et Azure en matière de sécurité. Cette perception est désormais obsolète. Avec Security Command Center Premium, Google propose une plateforme CNAPP mature qui rivalise avec les meilleures solutions du marché. Après avoir accompagné plusieurs migrations critiques vers GCP et conduit des audits de sécurité approfondis sur des organisations GCP complexes, je constate que la principale lacune ne vient pas de la plateforme elle-même mais de sa méconnaissance par les équipes sécurité encore majoritairement formées sur AWS et Azure. Ce guide technique vous fournit les clés pour exploiter pleinement Security Command Center, depuis la configuration initiale jusqu'à l'automatisation de la remédiation, en passant par l'analyse des findings et l'intégration avec votre écosystème SOC existant pour une visibilité complète sur votre posture de sécurité Google Cloud.

Comment configurer Security Command Center Premium ?

Security Command Center existe en deux tiers : Standard (gratuit) et Premium (payant). Le tier Standard offre la découverte d'assets, le scanning de vulnérabilités web via Web Security Scanner et les findings Security Health Analytics basiques. Le tier **Premium** ajoute Event Threat Detection, Container Threat Detection, Virtual Machine Threat Detection, l'analyse de conformité avancée et l'export continu vers BigQuery. Activez SCC au niveau de l'**organization** GCP pour couvrir tous les projets et dossiers automatiquement.

La configuration initiale requiert l'activation des services intégrés : **Security Health Analytics** (évaluation continue de la posture), **Web Security Scanner** (scan de vulnérabilités des applications web), **Event Threat Detection** (analyse des logs Cloud Audit pour détecter les menaces) et **Container Threat Detection** (monitoring runtime des conteneurs GKE). Chaque service génère des findings classés par sévérité : critique, haute, moyenne et basse. Consultez la documentation officielle de GCP Security pour les prérequis IAM nécessaires à l'activation.

Service SCC	Tier	Fonction	Sources de données
Security Health Analytics	Standard+	Posture assessment	Asset inventory
Web Security Scanner	Standard+	Vuln scanning web	URLs applicatives
Event Threat Detection	Premium	Détection menaces	Cloud Audit Logs
Container Threat Detection	Premium	Runtime container	GKE nodes
VM Threat Detection	Premium	Cryptomining, rootkits	Hyperviseur
Rapid Vulnerability Detection	Premium	Scan réseau agentless	Network scanning

Mon avis : Le tier Premium est indispensable pour toute utilisation sérieuse de GCP. Le Standard manque de la détection de menaces en temps réel, ce qui revient à n'avoir qu'un rétroviseur sans radar dans une voiture lancée sur autoroute. L'investissement se justifie dès que vous avez plus de cinq projets GCP en production.

Quelles vulnérabilités Security Health Analytics détecte-t-il ?

Security Health Analytics (SHA) évalue en continu plus de 150 détecteurs couvrant les principaux services GCP. Les catégories incluent : IAM et organisation (rôles primitifs owner/editor, comptes de service avec clés externes, absence de MFA), réseau (firewall rules trop permissives, SSL non enforced, IP forwarding activé), compute (instances avec IP publique, disques non chiffrés, OS obsolètes), storage (buckets publics, absence de versioning, pas de *retention policy*), et bases de données (Cloud SQL accessible publiquement, backups non chiffrés, SSL non requis).

Chaque finding SHA inclut une description, une recommandation de remédiation, un lien vers la documentation et un asset path identifiant précisément la ressource concernée. Les findings sont exportables vers **BigQuery** pour des analyses historiques et la création de dashboards Looker Studio personnalisés. Notre analyse sur la sécurité offensive GCP détaille les vecteurs d'attaque spécifiques à GCP que SHA peut aider à détecter.

Event Threat Detection : détecter les attaques en temps réel

Event Threat Detection (ETD) analyse les logs Cloud Audit en temps réel pour détecter les comportements malveillants. Les catégories de détection incluent : **credentials access** (utilisation de clés de compte de service depuis des IP suspectes), **cryptomining** (création de VMs avec des configurations de minage), **data exfiltration** (copies de données vers des projets externes), **evasion** (désactivation de VPC Flow Logs, suppression de Cloud Audit Logs), **initial access** (connexion root suspecte, invitation de membres externes) et **lateral movement** (impersonation de compte de service cross-projet).

Les findings ETD sont enrichis de contexte MITRE ATT&CK, facilitant la corrélation avec les techniques connues des attaquants cloud. Pour les environnements GKE, **Container Threat Detection** complète ETD en détectant les binaires suspects exécutés dans les conteneurs, les

shells inversés, les chargements de modules kernel malveillants et les accès au metadata service IMDS. Pour approfondir les techniques offensives GCP, notre article sur escalades de privilèges AWS est une ressource complémentaire essentielle.

Lors d'un audit GCP pour une fintech européenne, Event Threat Detection a révélé qu'un compte de service IAM avec le rôle Editor au niveau du projet était utilisé depuis une adresse IP géolocalisée en Asie alors que l'équipe est exclusivement européenne. L'investigation a montré que la clé JSON du compte de service avait fuité dans un dépôt Git public trois mois auparavant. Sans ETD, cette compromission aurait pu persister des mois supplémentaires et générer des coûts de compute estimés à plus de 40 000 euros en cryptomining.

Pourquoi utiliser l'analyse de conformité intégrée ?

SCC Premium intègre des évaluations de conformité contre les frameworks majeurs : **CIS GCP Benchmark**, **PCI DSS**, **NIST 800-53**, **ISO 27001** et les standards spécifiques à certains secteurs. Chaque contrôle est mappé sur les findings Security Health Analytics correspondants, fournissant une vue unifiée entre la posture technique et les exigences réglementaires.

Pour les organisations européennes, la conformité NIS 2 et le référentiel *SecNumCloud* imposent des exigences supplémentaires. Google Cloud a obtenu la qualification SecNumCloud pour certaines régions françaises, mais la responsabilité de la configuration sécurisée des workloads reste entièrement du côté du client. L'ANSSI publie des guides de durcissement complémentaires aux évaluations SCC. L'export vers BigQuery permet de construire des rapports de conformité personnalisés avec des requêtes SQL analytiques sur l'historique des findings.

Comment automatiser la remédiation des findings ?

L'automatisation de la remédiation dans GCP repose sur **Cloud Functions** déclenchées par les notifications SCC via **Pub/Sub**. Le workflow est le suivant : SCC détecte un finding, publie une notification sur un topic Pub/Sub, une Cloud Function consomme le message, évalue la sévérité et le type de finding, puis exécute l'action corrective appropriée via l'API GCP. Exemples d'actions automatisées : fermer un firewall rule 0.0.0.0/0, révoquer une clé de compte de service compromise, supprimer un bucket public, et désactiver un compte de service inutilisé.

Attention : la remédiation automatique nécessite des garde-fous stricts. Implémentez un système de dry-run qui loggue les actions sans les exécuter pendant une période de rodage. Ajoutez des exclusions pour les findings connus et acceptés (risques assumés documentés). Utilisez les *Organization Policy Constraints* comme prévention complémentaire : par exemple, le constraint `constraints/compute.vmExternalIpAccess` empêche la création de VMs avec des IP publiques, éliminant le besoin de remédier après coup.

Pour automatiser le durcissement via Infrastructure as Code, notre guide sur audit Terraform compliance détaille les bonnes pratiques Terraform applicables à GCP. De même, la gestion des secrets évoquée dans secrets sprawl et collecte est critique pour les comptes de service GCP.

Faut-il exporter les findings vers un SIEM externe ?

L'export des findings SCC vers un SIEM externe est recommandé pour les organisations qui opèrent des environnements multi-cloud ou qui disposent déjà d'un SIEM centralisé (Splunk, Sentinel, Elastic). L'export continu vers BigQuery constitue la première étape, depuis laquelle vous pouvez configurer des pipelines Dataflow vers votre SIEM. Google propose également des intégrations natives avec Chronicle (le SIEM de Google) et des connecteurs pour Splunk et QRadar.

L'alternative Chronicle mérite attention : ce SIEM cloud-native ingère les logs GCP sans coût de stockage supplémentaire (inclus dans la licence SCC Premium Enterprise) et offre des capacités de détection et d'investigation puissantes avec une rétention de 12 mois par défaut. Pour les organisations full-GCP, Chronicle élimine le besoin d'un SIEM tiers et simplifie considérablement l'architecture SOC. Consultez notre article sur escalade de privilèges IAM cloud pour les techniques d'investigation post-compromission applicables aux logs GCP.

À retenir : Security Command Center Premium est bien plus qu'un simple scanner de vulnérabilités. C'est une plateforme CNAPP complète qui combine CSPM, CWP et CIEM. Son efficacité maximale est atteinte lorsqu'il est couplé avec des Organization Policy Constraints préventives et des automatisations de remédiation via Cloud Functions et Pub/Sub.

Peut-on comparer SCC avec AWS Security Hub et Azure Defender ?

Chaque hyperscaler propose sa propre plateforme de sécurité intégrée, mais les approches diffèrent. AWS Security Hub agrège les findings de services distincts (GuardDuty, Inspector, Macie) dans un format normalisé ASFF. Azure Defender for Cloud offre une plateforme intégrée avec des plans de protection par type de workload. GCP SCC se distingue par son intégration profonde avec BigQuery pour l'analytique, sa détection au niveau hyperviseur (VM Threat Detection) et son approche API-first facilitant l'automatisation. En termes de couverture de détection, les trois plateformes sont comparables pour les menaces courantes, mais chacune excelle dans son écosystème natif. Le choix dépend davantage de votre cloud principal que des fonctionnalités intrinsèques.

L'utilisation des **Organization Policy Constraints** comme première ligne de défense est souvent sous-estimée. Contrairement à SCC qui détecte les problèmes après leur création, les Organization Policies empêchent les configurations non conformes d'être créées. Les contraintes les plus utiles incluent : `constraints/iam.allowedPolicyMemberDomains` qui restreint les membres IAM aux domaines approuvés, `constraints/compute.vmExternalIpAccess` qui bloque les IP publiques sur les VMs, `constraints/storage.uniformBucketLevelAccess` qui impose l'accès uniforme sur les buckets, et `constraints/compute.requireShieldedVm` qui impose les VMs sécurisées avec Secure Boot et vTPM activés pour prévenir les rootkits au niveau du boot.

Votre organisation a-t-elle réellement évalué les trois plateformes natives avant de choisir un CSPM tiers, ou avez-vous opté pour le confort d'un outil unique sans considérer la profondeur d'intégration native ?

Comment intégrer SCC dans un workflow DevSecOps ?

L'intégration de Security Command Center dans les pipelines DevSecOps permet de détecter les misconfigurations avant le déploiement. Utilisez **gcloud scc findings list** dans vos scripts CI/CD pour vérifier qu'aucun finding critique n'existe sur les ressources récemment déployées. Les **Organization Policy Constraints** agissent comme des guardrails préventifs qui bloquent les déploiements non conformes au niveau de l'API GCP, avant même que SCC ne détecte le problème. Combinez avec des outils de scanning IaC comme Checkov ou tfsec qui évaluent les templates Terraform contre les mêmes règles que Security Health Analytics, créant une boucle de feedback rapide pour les développeurs.

Le modèle **Infrastructure as Code auditée** impose que toute modification d'infrastructure passe par un pipeline de revue incluant un scan de sécurité automatisé, une validation par un pair, et un audit trail complet dans Cloud Audit Logs. Les findings SCC post-déploiement servent de filet de sécurité pour les cas où le scanning IaC pré-déploiement a manqué un problème, créant une défense en profondeur entre la prévention et la détection. Cette approche réduit le nombre de findings SCC de production de manière exponentielle car la majorité des misconfigurations sont détectées et corrigées avant d'atteindre l'environnement de production, transformant la sécurité d'un processus réactif en un processus proactif intégré naturellement au workflow des équipes de développement et d'opérations.

Les organisations operant exclusivement sur GCP beneficient de la profondeur d integration native avec Cloud Audit Logs et Cloud Asset Inventory. L inclusion potentielle de Chronicle SIEM dans le tier Enterprise transforme SCC en solution SOC complete pour les environnements Google Cloud. Evaluez le cout total de possession en comparant SCC Premium avec la somme des outils tiers que vous utilisez actuellement pour la detection de menaces et la gestion de la posture securite sur vos projets GCP.

Sources et références : CISA · Cloud Security Alliance

Conclusion : plan d'action Security Command Center

Déployez SCC Premium en quatre phases. Phase 1 : activez SCC au niveau organization avec SHA et Web Security Scanner. Phase 2 : activez ETD, Container Threat Detection et VM Threat Detection. Phase 3 : configurez les exports Pub/Sub et les automatisations de remédiation via Cloud Functions. Phase 4 : déployez les dashboards de conformité, intégrez Chronicle ou votre SIEM existant, et établissez des processus de revue hebdomadaire des findings. Cette approche progressive garantit une adoption maîtrisée et une montée en compétence de vos équipes sur les spécificités sécuritaires de Google Cloud Platform.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr