Audit Sécurité GCP 2026 : IAM, VPC Service Controls et SCC

> Audit sécurité GCP 2026 — IAM, VPC Service Controls, Security Command Center et Cloud Armor pour sécuriser les clouds GCP des organisations françaises NIS 2.

En septembre 2024, lors d'un audit de sécurité d'une scale-up française ayant migré l'intégralité de son infrastructure sur Google Cloud Platform (GCP), notre équipe a découvert des erreurs de configuration IAM critiques : 23 comptes de service disposaient du rôle **Owner** au niveau du projet (équivalent d'un accès root total), les **VPC Service Controls** n'étaient pas configurés permettant l'exfiltration de données BigQuery depuis n'importe quelle IP, et les **Cloud Audit Logs** (Admin Activity, Data Access) n'étaient pas activés sur 40% des projets GCP. Cette situation — malheureusement typique des migrations cloud rapides sans contrôle de sécurité — exposait l'entreprise à un risque majeur de compromission de données clients. En 18 mois de fonctionnement, aucune alerte de sécurité n'avait été générée malgré plusieurs activités suspectes visibles rétrospectivement dans les logs Cloud Audit qui avaient été activés. Mon avis est sans appel : GCP dispose des outils de sécurité natifs parmi les plus avancés du marché — IAM granulaire, **Security Command Center (SCC)**, **Chronicle SIEM**, **VPC Service Controls** — mais ils nécessitent une configuration experte et une connaissance approfondie du modèle de responsabilité partagée GCP pour être efficaces. Ce guide technique approfondi couvre l'audit de sécurité d'une infrastructure GCP en 2026 : analyse des IAM bindings et des comptes de service, configuration des VPC Service Controls, utilisation du Security Command Center Enterprise, intégration de Chronicle SIEM, protection avec Cloud Armor, et détection des misconfigurations avec les outils natifs GCP pour les organisations françaises soumises à NIS 2.

À RETENIR

À retenir

• Le modèle **IAM GCP** est basé sur des rôles (primitive, prédéfinis, personnalisés) assignés à des principals (comptes utilisateurs, groupes, comptes de service, identités fédérées) sur des ressources (projet, dossier, organisation) — éviter les rôles primitifs Owner/Editor au profit des rôles prédéfinis granulaires

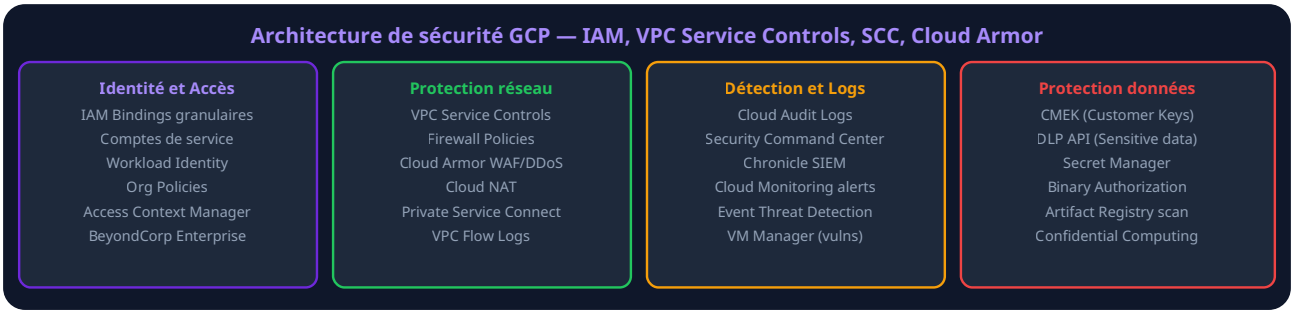
• **VPC Service Controls** créent un périmètre de sécurité autour des services GCP (BigQuery, Cloud Storage, Cloud SQL) qui empêche l'exfiltration de données même avec des credentials IAM compromis — le contrôle de sécurité le plus important pour les données sensibles GCP

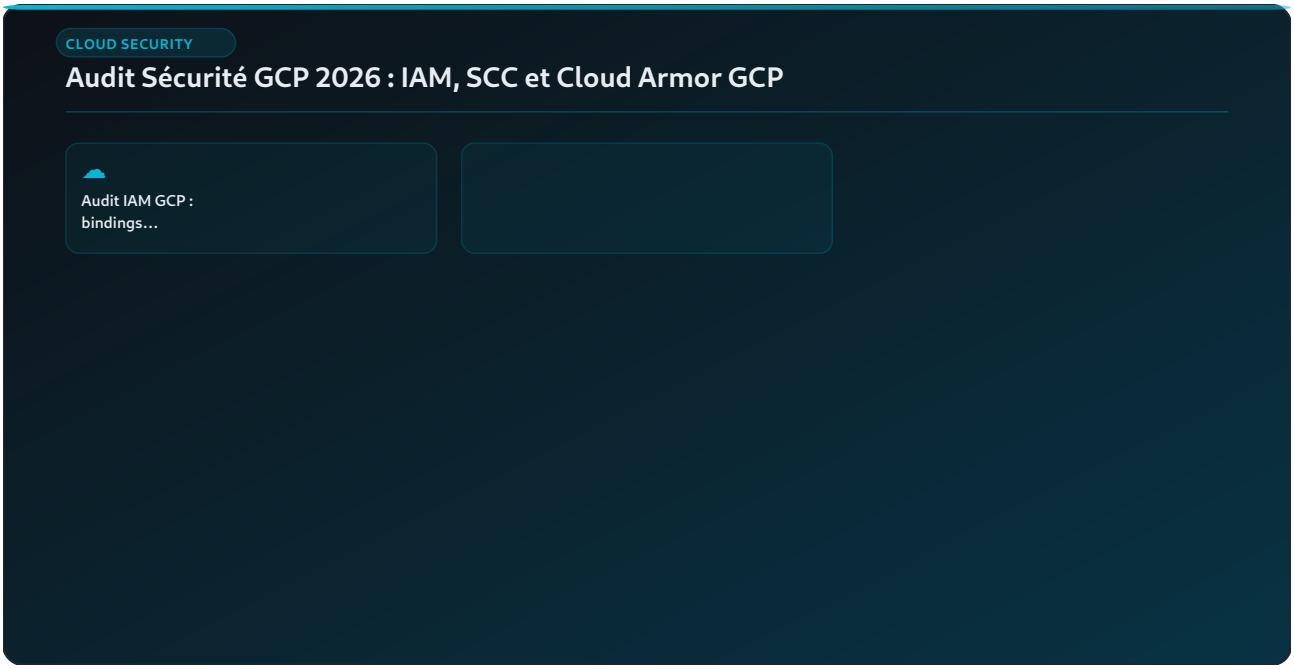
• **Security Command Center (SCC) Enterprise** avec Chronicle SIEM intégré offre une détection des menaces unifiée pour GCP, incluant la détection des misconfigurations (Posture), des menaces actives (Threat Detection), et la gestion des vulnérabilités (VM Manager)

• Les **Cloud Audit Logs GCP** ont trois types : Admin Activity (activé par défaut, gratuit), Data Access (désactivé par défaut, payant), et System Events — activer les Data Access logs pour les services critiques est indispensable pour toute investigation forensique GCP

• **Cloud Armor** est le WAF/DDoS managé de GCP qui protège les Load Balancers via des règles préconfigurées (OWASP Top 10) et des règles personnalisées CEL (Common Expression Language) pour bloquer le trafic malveillant avant qu'il n'atteigne les applications

• Les **Org Policies GCP** permettent d'imposer des contraintes de sécurité au niveau de l'organisation qui s'appliquent à tous les projets et dossiers enfants, indépendamment des permissions IAM des administrateurs de projets individuels





L'**IAM GCP (Identity and Access Management)** utilise un modèle de contrôle d'accès basé sur des bindings qui associent un principal (identité) à un rôle sur une ressource. Les trois types de rôles sont : les rôles **primitifs** (Owner, Editor, Viewer) hérités de l'ancienne console Google Cloud — à éviter absolument en production car trop permissifs, les rôles **prédéfinis** (plus de 900 rôles granulaires comme `roles/bigquery.dataViewer`, `roles/compute.instanceAdmin.v1`) permettant le principe du moindre privilège, et les rôles **personnalisés** (Custom Roles) pour des combinaisons de permissions très spécifiques non couvertes par les rôles prédéfinis. L'audit des bindings IAM s'effectue avec la commande `gcloud projects get-iam-policy [PROJECT_ID] --`

`format=json` pour un projet, ou avec `gcloud organizations get-iam-policy [ORG_ID]` pour l'organisation entière.

Les **comptes de service GCP** (Service Accounts) sont des identités non-humaines utilisées par les applications et les workloads GCP pour s'authentifier aux APIs Google. Un compte de service est représenté par une adresse email (`[name]@[project-id].iam.gserviceaccount.com`) et peut disposer de clés JSON (à éviter — préférer Workload Identity) ou utiliser le mécanisme de métadonnées des instances Compute Engine. L'audit des comptes de service doit vérifier : l'absence de rôles Owner/Editor sur les comptes de service (signe de sur-privilégiation), l'absence de clés de compte de service avec une date de création ancienne (> 90 jours sans rotation), et l'absence de comptes de service disposant de l'IAM policy binding `iam.serviceAccountTokenCreator` sur eux-mêmes (privilege escalation path). L'outil **IAM Recommender** de GCP analyse les permissions utilisées et recommande des réductions de permissions basées sur l'activité réelle sur les 90 derniers jours, facilitant l'application du principe du moindre privilège à grande échelle.

Org Policies GCP : contraintes de sécurité organisationnelles

Les **Org Policies GCP** (Organization Policies) permettent d'imposer des contraintes de configuration qui s'appliquent à l'ensemble de l'organisation GCP, ou à des dossiers et projets spécifiques, indépendamment des permissions IAM des administrateurs individuels. Ces contraintes peuvent **refuser** des configurations dangereuses spécifiques ou **imposer** des configurations de sécurité requises. Les Org Policies de sécurité les plus importantes pour un audit GCP incluent : `constraints/compute.requireShieldedVm` (impose Shielded VM pour toutes les instances Compute Engine), `constraints/compute.restrictCloudNATUsage` (contrôle l'usage de Cloud NAT), `constraints/iam.allowedPolicyMemberDomains` (restreint les domaines pouvant recevoir des bindings IAM, empêchant l'ajout accidentel de comptes Gmail personnels), et `constraints/storage.uniformBucketLevelAccess` (impose le contrôle d'accès unifié sur les buckets Cloud Storage, désactivant les ACLs héritées plus complexes à auditer).

⚡ **Retour terrain**

J'ai accompagné la mise en sécurité d'un environnement GCP pour un groupe média. Le principal risque identifié : des comptes de service avec des rôles Owner ou Editor au niveau projet, utilisés par des applications en production. L'inventaire des comptes de service et la migration vers des rôles personnalisés à moindres privilèges a pris 6 semaines — mais lors d'un incident ultérieur impliquant un secret volé, le rayon d'impact était limité à un seul microservice.

La politique Org Policy la plus critique d'un point de vue sécurité est `constraints/compute.vmExternalIpAccess` qui restreint quelles instances Compute Engine peuvent avoir une adresse IP externe — une contrainte essentielle pour éviter l'exposition accidentelle de VMs sur Internet. Combinée avec `constraints/compute.restrictLoadBalancerCreationForTypes` (restreint les types de Load Balancers pouvant être créés), ces politiques créent un périmètre réseau organisationnel qui s'applique à tous les projets de l'organisation. L'audit des Org Policies actives s'effectue avec `gcloud resource-manager org-policies list --organization=[ORG_ID]` et la vérification de leur application effective avec la commande `gcloud resource-manager org-policies describe [CONSTRAINT] --organization=[ORG_ID]`. La documentation officielle de toutes les contraintes disponibles est maintenue sur le site de Google Cloud.

VPC Service Controls : périmètre de sécurité des données GCP

Les **VPC Service Controls** sont le mécanisme de protection le plus puissant et le plus souvent absent dans les déploiements GCP non sécurisés. Ils créent un *périmètre de service* autour des ressources GCP (projets entiers ou services spécifiques comme BigQuery, Cloud Storage, Cloud SQL) qui empêche l'accès aux données depuis l'extérieur du périmètre, même avec des credentials IAM valides. Concrètement, un attaquant disposant de clés de compte de service

volées ne peut pas extraire les données BigQuery protégées par VPC Service Controls depuis son infrastructure externe — la requête est bloquée par le périmètre même si les permissions IAM sont valides. Cette protection contre l'exfiltration de données est impossible à réaliser uniquement avec des règles IAM et représente une couche de sécurité indépendante des identités.

La configuration des VPC Service Controls s'effectue via l'**Access Context Manager** qui définit les niveaux d'accès (conditions pour accéder au périmètre : réseau IP, identité du device, géolocalisation) et l'Access Policy qui regroupe les périmètres de service. Un périmètre de service peut opérer en mode **Enforced** (bloquage effectif) ou en mode **Dry Run** (journalisation uniquement, sans blocage) — le mode Dry Run est recommandé pour la phase de configuration et de validation avant le passage en mode Enforced, car les VPC Service Controls peuvent bloquer des accès légitimes si mal configurés. L'analyse des violations en mode Dry Run s'effectue dans les Cloud Audit Logs (type `vpcServiceControls`) avec la commande `gcloud logging read "protoPayload.metadata.resourceType=vpcServiceControls" --project=[PROJECT_ID]` pour identifier les accès légitimes à autoriser avant l'enforcement.

Cloud Audit Logs GCP : activation et analyse forensique

Les **Cloud Audit Logs GCP** sont la source primaire d'informations pour l'investigation forensique et la détection des menaces dans GCP. Ils se décomposent en trois types : les logs **Admin Activity** (activés par défaut, gratuits, conservés 400 jours) qui journalisent les opérations administratives modifiant la configuration des ressources GCP (création/suppression de VMs, modification des politiques IAM, création de buckets Cloud Storage), les logs **Data Access** (désactivés par défaut, payants, à activer manuellement pour chaque service) qui journalisent les lectures et écritures de données (requêtes BigQuery, lecture de fichiers Cloud Storage, requêtes Cloud SQL), et les logs **System Events** (automatiques, gratuits) générés par les systèmes GCP eux-mêmes. Pour une investigation forensique GCP, l'absence de logs Data Access rend impossible la reconstruction des accès aux données sensibles.

L'activation des logs Data Access pour les services critiques s'effectue au niveau de l'organisation ou du projet via la mise à jour de la politique d'audit IAM : `gcloud projects set-iam-policy [PROJECT_ID] audit_policy.json` où le fichier JSON spécifie les services et types de logs à

activer. Pour BigQuery, l'activation se fait avec `auditLogConfig.logType: DATA_READ` et `DATA_WRITE`. Une recommandation pratique : activer les Data Access logs pour BigQuery, Cloud Storage, Cloud SQL, Secret Manager, et KMS (Cloud Key Management Service) en priorité, car ces services contiennent généralement les données les plus sensibles des organisations. L'export des Cloud Audit Logs vers BigQuery via un Log Sink permet l'analyse SQL des logs avec des requêtes complexes, ou vers Chronicle SIEM pour la détection de menaces et la corrélation avec d'autres sources de sécurité.

Security Command Center Enterprise : posture et menaces

Le **Security Command Center (SCC) Enterprise** est la plateforme de gestion de la posture de sécurité et de détection des menaces native de GCP. En 2026, SCC Enterprise intègre Chronicle SIEM et offre trois capacités principales : **Security Posture** (détection des misconfigurations de resources GCP via des règles de conformité NIST, CIS, PCI-DSS), **Threat Detection** (détection des menaces actives via des règles Event Threat Detection et Container Threat Detection), et **Vulnerability Management** (inventaire des vulnérabilités CVE dans les VMs via VM Manager). Les findings SCC sont classés par sévérité (CRITICAL, HIGH, MEDIUM, LOW) et catégorisés par type (MISCONFIGURATION, VULNERABILITY, OBSERVATION, THREAT). L'API SCC permet d'exporter les findings vers des outils ITSM ou SIEM externes pour centraliser la gestion des vulnérabilités cloud.

L'**Event Threat Detection (ETD)**, composant de SCC, analyse les Cloud Audit Logs et VPC Flow Logs en temps quasi-réel pour détecter des patterns d'attaque connus : `Defense Evasion: Modify VPC Service Control` (modification des périmètres de service par un attaquant), `Discovery: Service Account Self-Investigation` (un compte de service qui interroge ses propres permissions — signe de reconnaissance post-compromission), `Exfiltration: BigQuery Data Exfiltration` (export inhabituel de grandes quantités de données BigQuery), `Credential Access: External Member Added to Policy` (ajout d'un compte externe à une politique IAM sensible). Ces détections sont préconfigurées et s'activent automatiquement sans écriture de règles, couvrant les techniques ATT&CK pour GCP les plus critiques dès l'activation de SCC.

Chronicle SIEM GCP : détection et investigation cloud-native

Chronicle SIEM (anciennement Backstory, désormais intégré dans la plateforme Google SecOps) est le SIEM cloud-native de Google conçu pour ingérer et analyser des volumes massifs de logs de sécurité avec une rétention d'un an incluse dans le coût (modèle de tarification basé sur le nombre d'utilisateurs et non sur le volume de données — une différence fondamentale avec les SIEMs traditionnels comme Splunk). Chronicle utilise le langage de requête **YARA-L 2.0** pour écrire des règles de détection (Rules), similaire à YARA mais adapté aux événements de sécurité tabulaires, et le **UDM (Unified Data Model)** pour normaliser les events de toutes les sources en un schéma commun. Pour les organisations full-GCP, Chronicle ingère automatiquement les Cloud Audit Logs, VPC Flow Logs, et les findings SCC sans configuration supplémentaire.

L'avantage de Chronicle pour les investigations GCP est la capacité de rétro-recherche (Retrohunt) : exécuter une règle de détection sur l'intégralité des logs de l'année passée pour identifier si une technique d'attaque récemment documentée s'est déjà produite dans l'environnement avant sa détection. Cette capacité est particulièrement précieuse pour la réponse aux incidents où l'analyste doit déterminer si l'attaquant était déjà présent dans l'environnement avant la date de détection initiale. Chronicle dispose également d'un graphe d'entités (Entity Graph) qui agrège automatiquement les informations sur les adresses IP, domaines, fichiers, et utilisateurs à travers tous les événements pour faciliter l'investigation. Notre service RSSI externalisé inclut la configuration et la gestion de Chronicle SIEM pour les organisations françaises sur GCP.

Cloud Armor : WAF managé et protection DDoS GCP

Cloud Armor est le service de protection applicative (WAF/DDoS) managé de GCP qui s'intègre aux Load Balancers HTTP(S) pour filtrer le trafic malveillant avant qu'il n'atteigne les applications. Cloud Armor propose des **règles préconfigurées** pour la protection OWASP Top 10 (injection SQL, XSS, LFI/RFI, scanner detection) disponibles en un clic, et des règles

personnalisées en **CEL (Common Expression Language)** pour des logiques de filtrage spécifiques à l'application. La protection DDoS L3/L4 de Cloud Armor utilise l'infrastructure anycast mondiale de Google pour absorber les attaques volumétriques avant qu'elles n'atteignent la région GCP cible — Google bénéficiant d'une capacité d'absorption DDoS de plusieurs Tbps grâce à son infrastructure réseau globale.

La configuration de Cloud Armor s'effectue via des **Security Policies** attachées aux Backend Services du Load Balancer. Une Security Policy combine des règles avec des conditions CEL (`request.path.matches('/admin/.*') && !inIpRange(origin.ip, '10.0.0.0/8')` pour bloquer les accès à l'interface d'administration depuis des IPs non privées) et des actions (allow, deny, redirect, rate-based ban). Le mode **Adaptive Protection** de Cloud Armor utilise le machine learning pour détecter automatiquement les attaques DDoS L7 émergentes et suggérer des règles de mitigation en temps réel. Pour les applications exposant des APIs REST, la limitation de débit via Cloud Armor (`throttle action` avec un seuil de requêtes par IP par minute) prévient les attaques par brute-force et les abus d'API. Notre service d'audit de sécurité cloud couvre également GCP et inclut la revue de configuration Cloud Armor.

Binary Authorization : contrôle de la chaîne d'approvisionnement

Binary Authorization est un service GCP qui impose des politiques de contrôle sur les images de containers déployées dans GKE (Google Kubernetes Engine) et Cloud Run. Chaque image déployée doit disposer d'une ou plusieurs **attestations** cryptographiques signées par des *attestors* autorisés, prouvant qu'elle a passé des étapes de validation définies dans la politique : scan de vulnérabilités avec un score inférieur à un seuil, signature par l'équipe DevSecOps, ou validation par un pipeline CI/CD approuvé. Sans l'attestation requise, Binary Authorization bloque le déploiement du container — même si l'opérateur dispose des permissions IAM pour déployer sur GKE. Cette protection est cruciale pour prévenir les attaques de la chaîne d'approvisionnement logicielle (supply chain attacks) où un attaquant compromet un registre de containers ou injecte du code malveillant dans une image.

La configuration de Binary Authorization s'effectue en trois étapes : création d'un attestor avec une clé de signature KMS, configuration de la politique Binary Authorization du cluster GKE

pour exiger l'attestation de cet attestor pour tous les déploiements, et intégration dans le pipeline CI/CD pour créer automatiquement l'attestation après le scan de vulnérabilités réussi. Un mode **Dry Run** permet de tester la politique sans blocage effectif, en journalisant les déploiements qui auraient été bloqués dans Cloud Audit Logs. Binary Authorization s'intègre nativement avec Google Artifact Registry (scan automatique des images avec les CVEs connues au moment du push) et avec les pipelines Cloud Build pour créer des attestations après les étapes de validation réussies dans le pipeline CI/CD.

CMEK et Cloud KMS : gestion des clés de chiffrement client

Le **CMEK (Customer-Managed Encryption Keys)** permet aux organisations d'utiliser leurs propres clés de chiffrement gérées dans **Cloud KMS (Key Management Service)** pour chiffrer les données dans les services GCP (BigQuery, Cloud Storage, Cloud SQL, Compute Engine persistent disks, Pub/Sub). Avec CMEK, Google ne peut plus accéder aux données chiffrées sans l'utilisation des clés du client — contrairement au chiffrement par défaut Google Managed Encryption Keys où Google contrôle les clés. Pour les organisations françaises avec des données très sensibles (données de santé, données financières réglementées), CMEK sur les services GCP critiques répond à l'exigence de contrôle souverain des clés de chiffrement. Les clés CMEK peuvent être stockées dans Cloud KMS (géré par GCP mais les clés appartiennent au client), dans Cloud HSM (Hardware Security Module certifié FIPS 140-2 Level 3), ou via Cloud External Key Manager (CEKM) pour les clés gérées dans un HSM on-premise ou un KMS tiers externe à GCP.

L'audit CMEK dans une organisation GCP vérifie : l'activation du CMEK sur tous les services contenant des données classifiées (BigQuery datasets, Cloud Storage buckets, Cloud SQL instances), la rotation des clés KMS à intervalles définis (GCP supporte la rotation automatique configurable), les politiques d'accès aux clés KMS (qui peut utiliser les clés pour le chiffrement/déchiffrement via les rôles `roles/cloudkms.cryptoKeyEncrypter` et `roles/cloudkms.cryptoKeyDecrypter`), et la surveillance des opérations KMS dans les Cloud Audit Logs pour détecter des accès inhabituels aux clés. Un chiffrement CMEK peut être activé sur les

projets existants sans migration des données grâce à la re-encryption transparente de GCP, mais cette opération doit être planifiée avec soin pour les datasets BigQuery volumineux.

Sensitive Data Protection : découverte et classification des données

Le service **Sensitive Data Protection** (anciennement Cloud DLP) de GCP permet de découvrir, classifier, et protéger les données sensibles dans BigQuery, Cloud Storage, et Datastore. Pour un audit de sécurité GCP, la découverte des données sensibles est souvent le premier chantier car de nombreuses organisations ne savent pas précisément quelles données sensibles sont stockées dans leurs environnements cloud. Sensitive Data Protection peut scanner automatiquement tous les buckets Cloud Storage et tables BigQuery d'un projet pour détecter plus de 150 types d'informations prédéfinis (*infoTypes*) : numéros de cartes de crédit, numéros de sécurité sociale français, numéros de téléphone, adresses email, données médicales (diagnostic, numéros d'ordonnance), et identifiants spécifiques comme les numéros SIRET/SIREN français. Les résultats sont exportés dans BigQuery pour une analyse et un reporting de conformité.

La **découverte continue des données (Data Discovery)** de Sensitive Data Protection surveille en permanence les nouveaux buckets Cloud Storage et tables BigQuery créés dans l'organisation, les scannant automatiquement pour détecter les données sensibles dès leur création. Cette capacité est essentielle pour les grandes organisations cloud-native où de nouveaux datasets sont créés quotidiennement par des équipes data — sans découverte continue, des données sensibles peuvent rester non détectées et non protégées pendant des semaines. Les résultats de la découverte alimentent le **Data Risk Summary** de Security Command Center qui fournit une vue consolidée des données sensibles exposées avec leur niveau de risque (combinant la sensibilité des données et les problèmes IAM/VPC Service Controls associés). Notre service de diagnostic NIS 2 inclut une phase de découverte des données sensibles GCP pour les organisations françaises soumises aux exigences de protection des données personnelles.

VPC Flow Logs et réseau GCP : visibilité du trafic

Les **VPC Flow Logs** GCP enregistrent les flux réseau (IP 5-tuple : source IP, destination IP, source port, destination port, protocole) pour toutes les connexions transitant via les interfaces réseau des VMs Compute Engine, des noeuds GKE, et via Cloud Interconnect/VPN. Activés au niveau du subnet VPC, les VPC Flow Logs sont échantillonnés par défaut à 50% des flux (configurable entre 0 et 1) et exportés vers Cloud Logging depuis lequel ils peuvent être routés vers BigQuery pour analyse SQL, vers Cloud Storage pour archivage à long terme, ou vers Chronicle SIEM pour la détection de menaces. Pour un audit de sécurité GCP, la vérification de l'activation des VPC Flow Logs sur tous les subnets contenant des workloads critiques est une étape fondamentale car leur absence rend impossible toute reconstruction du trafic réseau lors d'une investigation forensique d'incident.

L'analyse des VPC Flow Logs dans BigQuery permet de détecter des patterns réseau suspects : communications vers des plages IP de réputation mauvaise (threat intelligence), volumes de données inhabituels sortants vers des IPs externes (exfiltration), scans de ports internes (reconnaissance réseau post-compromission), ou communications entre VPCs qui ne devraient pas interagir. Une requête BigQuery simple pour détecter les connexions sortantes vers des IPs non RFC-1918 depuis des VMs de production révèle immédiatement toute communication vers l'extérieur qui pourrait indiquer une compromission ou une mauvaise configuration de sécurité réseau. L'export des VPC Flow Logs vers Chronicle permet des corrélations avec les Cloud Audit Logs pour enrichir les investigations : une connexion réseau suspecte visible dans les VPC Flow Logs peut être corrélée avec une opération IAM suspecte dans les Audit Logs pour construire une timeline complète d'un incident.

Cloud IDS : détection des intrusions réseau sur GCP

Cloud IDS (Intrusion Detection System) est un service GCP géré de détection d'intrusions réseau qui analyse le trafic réseau en mode passif (mirroring des paquets via Packet Mirroring) pour détecter des menaces au niveau réseau : malwares, exploitations de vulnérabilités,

commandes et contrôle (C2), mouvements latéraux. Cloud IDS utilise les signatures de détection de *Palo Alto Networks* (le même moteur que le NGFW Palo Alto) appliquées sur le trafic réseau GCP, offrant des capacités de détection de menaces réseau au niveau IDS/IPS sans nécessiter le déploiement et la gestion d'appliances réseau physiques ou virtuelles. La sévérité des alertes Cloud IDS est alignée avec les catégories Palo Alto Networks : CRITICAL, HIGH, MEDIUM, LOW, INFORMATIONAL.

Le déploiement de Cloud IDS s'effectue en créant un Endpoint IDS dans la région souhaitée et en configurant le Packet Mirroring pour copier le trafic des VMs à surveiller vers cet endpoint. Une limitation importante à connaître pour le dimensionnement : Cloud IDS analyse le trafic décrypté — pour les flux HTTPS internes, le déchiffrement TLS doit être effectué par les Load Balancers GCP ou par des proxies dédiés avant l'envoi au Packet Mirroring pour une analyse applicative complète. Les alertes Cloud IDS apparaissent dans Cloud Logging et peuvent être exportées vers Chronicle SIEM ou vers Cloud Pub/Sub pour déclencher des réponses automatisées via Cloud Functions. Pour les organisations utilisant GCP comme infrastructure principale de production, Cloud IDS est un complément précieux aux détections Cloud-native de SCC Event Threat Detection qui se concentre sur les appels API GCP, là où Cloud IDS couvre les menaces au niveau réseau traditionnel.

Workload Identity Federation : accès GCP sans clés de service

Workload Identity Federation est le mécanisme GCP permettant à des workloads s'exécutant en dehors de GCP (AWS EC2, Azure VMs, GitHub Actions, GitLab CI, Jenkins, systèmes on-premise) d'accéder aux APIs GCP sans clé de compte de service JSON — éliminant la principale source de compromission de credentials GCP. Avec Workload Identity Federation, le workload externe s'authentifie auprès de son fournisseur d'identité natif (AWS STS, Azure AD token, GitHub OIDC token) et échange ce token contre des credentials GCP temporaires via le Service Account Impersonation. Les credentials GCP obtenus sont valides pour une courte durée (1 heure par défaut) et générés à la demande, éliminant les secrets longue durée à protéger et à faire pivoter.

La configuration de Workload Identity Federation s'effectue en créant un **Workload Identity Pool** et un **Provider** dans GCP qui définissent comment valider les tokens du fournisseur d'identité externe et quelles conditions (`attribute.repository == 'mon-org/mon-repo'` pour GitHub Actions) permettent l'impersonation du compte de service GCP cible. Pour les pipelines CI/CD GitHub Actions qui déploient sur GCP, Workload Identity Federation élimine complètement la nécessité de stocker des clés de compte de service JSON dans les secrets GitHub — une pratique risquée car les secrets GitHub peuvent être exposés accidentellement dans des logs CI/CD. L'audit des Workload Identity Pools et Providers existants vérifie que les conditions d'attributs sont suffisamment restrictives pour éviter l'impersonation de comptes de service par des workflows non autorisés.

Cloud Build et DevSecOps GCP : pipeline CI/CD sécurisé

Cloud Build est le service CI/CD managé de GCP qui exécute des pipelines de build, de test, et de déploiement dans des containers éphémères isolés. La sécurisation d'un pipeline Cloud Build implique : l'utilisation d'un compte de service Cloud Build dédié avec les permissions minimales nécessaires (pas le compte de service par défaut Cloud Build qui dispose du rôle Editor sur le projet), l'activation des **Private Pools** Cloud Build (workers dans le VPC du client plutôt que dans l'infrastructure partagée de GCP) pour les builds manipulant des secrets ou des données sensibles, et l'intégration du scan de vulnérabilités des images containers avec **Google Artifact Registry** qui scanne automatiquement les images pushées contre les CVEs connues de la base de données OSV (Open Source Vulnerabilities).

L'intégration du scan SAST (Static Application Security Testing) et SCA (Software Composition Analysis) dans les pipelines Cloud Build est recommandée pour les organisations soumises à NIS 2 : intégration de **Snyk**, **Semgrep**, ou des outils natifs Google (comme les règles Container Analysis pour l'analyse des dépendances) dans les étapes de build pour bloquer les déploiements d'images contenant des vulnérabilités critiques avant qu'elles n'atteignent les environnements de production GKE. Combined avec Binary Authorization qui vérifie les attestations de scan réussi avant tout déploiement GKE, ce pipeline DevSecOps GCP garantit que seules des images

validées et sécurisées arrivent en production, créant une véritable chaîne de confiance de la source code jusqu'au container en production.

Cloud Asset Inventory : visibilité complète des ressources GCP

Cloud Asset Inventory est le service GCP qui maintient un inventaire en temps réel de toutes les ressources et politiques IAM de l'organisation GCP, avec un historique des changements sur les 35 derniers jours. Pour un audit de sécurité GCP, Cloud Asset Inventory est le point de départ indispensable : la commande `gcloud asset search-all-resources --organization=[ORG_ID] --asset-types="storage.googleapis.com/Bucket"` liste immédiatement tous les buckets Cloud Storage de l'organisation avec leurs métadonnées, permettant d'identifier les buckets publics ou mal configurés. La commande `gcloud asset search-all-iam-policies --query="roles/owner"` liste tous les principals disposant du rôle Owner dans l'organisation entière en quelques secondes.

Le **Policy Analyzer** de Cloud Asset Inventory permet d'analyser les politiques IAM pour répondre à des questions complexes : "Quels principals ont accès à tel bucket Cloud Storage ?" ou "Quelles ressources ce compte de service peut-il accéder ?". Ces analyses sont cruciales pour les audits de droits d'accès requis par NIS 2. La **CAI Feed** (Cloud Asset Inventory Feed) permet de recevoir des notifications en temps réel lors de la création ou modification de ressources spécifiques via Cloud Pub/Sub, déclenchant des workflows d'audit automatisé : par exemple, une alerte immédiate si un bucket Cloud Storage devient public, si un rôle Owner est assigné à un compte externe, ou si un VPC Service Control est modifié. Notre service d'audit de sécurité cloud utilise Cloud Asset Inventory comme base de l'audit initial GCP.

Sécurité GKE : durcissement des clusters Kubernetes managés

La sécurité des clusters **GKE (Google Kubernetes Engine)** est un domaine à part entière qui combine les bonnes pratiques Kubernetes générales avec les spécificités GCP. Les configurations

GKE critiques pour la sécurité incluent : l'activation du **mode Autopilot** (qui applique automatiquement les meilleures pratiques de sécurité et réduit la surface d'attaque des workers nodes en rendant les nodes non-accessibles), l'activation des **Shielded Nodes** (vTPM, Secure Boot, Integrity Monitoring pour les workers GKE), l'utilisation de **Workload Identity** au lieu des clés de compte de service JSON pour l'authentification des workloads GKE aux APIs GCP, et l'activation de l'**audit logging Kubernetes** exporté vers Cloud Logging pour la visibilité sur les opérations kubectl et les API calls Kubernetes (création de pods, modifications de RBAC, accès aux secrets Kubernetes).

La détection des menaces spécifiques à GKE est assurée par **Container Threat Detection** de SCC Enterprise qui analyse les syscalls des containers en cours d'exécution pour détecter des comportements suspects : exécution de shells dans des containers qui ne devraient pas en avoir, tentatives de montage de volumes filesystem sensibles, communications réseau vers des IPs malveillantes depuis des pods, ou tentatives d'évasion de container via des vulnérabilités kernel. Container Threat Detection utilise des modules eBPF pour la surveillance des syscalls avec un impact minimal sur les performances des containers en production. Les findings Container Threat Detection apparaissent dans SCC avec les détails du pod, du namespace, et du cluster GKE concerné, permettant une investigation et une isolation rapide du workload compromis.

Service GCP	Rôle sécurité	Tier	Priorité audit
IAM + Org Policies	Contrôle d'accès	Gratuit	Critique
VPC Service Controls	Anti-exfiltration données	Payant	Critique
Cloud Audit Logs	Forensique et conformité	Partiel gratuit	Critique
Security Command Center	Posture + menaces	Standard/Premium	Élevée
Cloud Armor	WAF/DDoS protection	Payant	Élevée
Binary Authorization	Supply chain sécurité	Payant	Moyenne
Sensitive Data Protection	Découverte données sensibles	Payant	Moyenne

CIS Benchmarks GCP et outils d'audit automatisé

Les **CIS Benchmarks GCP** (Center for Internet Security) définissent 60+ contrôles de configuration recommandés pour les projets GCP, organisés en niveaux L1 (configuration de base sans impact fonctionnel) et L2 (configuration avancée avec possible impact opérationnel). Ces benchmarks couvrent IAM, Logging, Réseaux VPC, VMs Compute Engine, Cloud Storage, Cloud SQL, BigQuery, et KMS. Security Command Center Standard propose une vérification automatisée de la conformité aux CIS Benchmarks GCP via le module "Posture Management", générant des findings pour chaque contrôle CIS non respecté dans l'organisation. L'outil open-source **Forseti Security** (désormais intégré dans l'écosystème GCP) proposait également des audits de conformité automatisés, mais sa maintenance active a été transférée vers SCC qui couvre maintenant les mêmes cas d'usage.

Pour un audit GCP rapide et complet, les outils **Prowler** (open-source, disponible sur github.com/prowler-cloud/prowler) et **ScoutSuite** effectuent des audits de configuration multi-cloud incluant GCP avec des centaines de vérifications de sécurité organisées par service. Prowler GCP s'authentifie via les credentials Application Default Credentials et scanne tous les projets accessibles via l'API, produisant un rapport HTML ou JSON avec les findings classés par sévérité et mappés aux frameworks de conformité (CIS, NIS 2, ISO 27001). Un audit Prowler d'une organisation GCP de taille moyenne (50 projets) prend environ 20 à 40 minutes et produit une vue initiale complète des misconfigurations à corriger en priorité pour améliorer la posture de sécurité GCP.

IAM Conditions et contrôle d'accès contextuel GCP

Les **IAM Conditions GCP** permettent d'ajouter des contraintes contextuelles aux bindings IAM, transformant des accès permanents en accès conditionnels basés sur des attributs de la requête : timestamp (accès uniquement pendant les heures de bureau), adresse IP source (accès uniquement depuis le réseau d'entreprise), type de ressource (accès seulement aux ressources avec un label spécifique), ou attribut du device (accès depuis des appareils conformes

BeyondCorp). Un exemple pratique : un binding IAM avec condition temporelle pour les accès d'urgence (`request.time < timestamp('2026-07-15T00:00:00Z')`) permet d'accorder un accès temporaire à un consultant externe pour une intervention planifiée, avec révocation automatique à l'expiration de la condition sans action manuelle. Les IAM Conditions sont particulièrement utiles pour les accès just-in-time (JIT) qui remplacent les accès permanents à des comptes très privilégiés.

L'**Access Context Manager** GCP permet de définir des niveaux d'accès (*Access Levels*) qui combinent plusieurs attributs contextuels (IP de la requête, conformité du device, appartenance à un groupe) en une condition réutilisable dans les IAM Conditions et les VPC Service Controls. Un access level "CorpNetworkCompliantDevice" peut combiner : plage IP du réseau d'entreprise ET appartenance au groupe Active Directory des utilisateurs ayant réalisé la formation sécurité de l'année ET device certifié par Chrome Device Management. Ce niveau d'accès contextuel, appliqué via les VPC Service Controls ou les IAM Conditions sur les ressources sensibles, crée un modèle Zero Trust GCP où chaque accès est évalué selon plusieurs facteurs de confiance simultanément, bien au-delà de la simple authentification par credentials. Notre service de mise en conformité NIS 2 recommande ce modèle d'accès contextuel pour les accès aux données les plus sensibles hébergées sur GCP.

Questions fréquentes sur la sécurité GCP

GCP est-il plus sécurisé qu'AWS ou Azure par défaut ?

GCP dispose de protections DDoS natives plus robustes grâce à l'infrastructure réseau de Google, et son modèle IAM avec Workload Identity et les comptes de service est généralement considéré comme mieux conçu que les IAM Roles AWS. Cependant, la sécurité d'une infrastructure cloud dépend avant tout de sa configuration et non de la plateforme choisie. Les trois hyperscalers ont des misconfigurations courantes différentes (buckets S3/GCS publics accidentels, Security Groups AWS trop permissifs, VMs Azure sans MFA) mais un niveau de sécurité comparable lorsque correctement configurés selon les recommandations CIS Benchmarks respectifs.

Comment auditer rapidement la sécurité d'un projet GCP ?

Le point de départ le plus rapide est l'activation du Security Command Center Standard (gratuit) qui génère instantanément des findings sur les misconfigurations IAM et réseau les plus critiques. L'outil open-source Forseti Security (maintenant intégré dans SCC) ou les scripts de l'outil **gcloud-policy-intelligence** permettent un audit plus approfondi des IAM bindings. La commande `gcloud asset search-all-iam-policies --query="roles/owner"` liste en quelques secondes tous les principals disposant du rôle Owner dans l'organisation entière.

Les VPC Service Controls sont-ils compatibles avec les architectures multi-cloud ?

Les VPC Service Controls sont spécifiques à GCP et ne contrôlent que les accès aux services GCP. Pour les architectures multi-cloud, des solutions tierces comme Prisma Cloud (Palo Alto), Wiz, ou Orca Security offrent une vue unifiée de la posture de sécurité sur AWS, GCP, et Azure avec un langage de politiques commun. L'accès depuis des ressources AWS ou Azure vers des services GCP protégés par VPC Service Controls nécessite la configuration d'Access Levels spécifiques dans l'Access Context Manager autorisant les plages IP des autres clouds.

Comment GCP se conforme-t-il aux exigences NIS 2 françaises ?

GCP France (régions europe-west9 et europe-west10) bénéficie des certifications ISO 27001, SOC 2 Type II, et C5 (Cloud Computing Compliance Controls Catalogue, le référentiel allemand equivalent à SecNumCloud). Google a également obtenu des certifications sectorielles HDS pour les données de santé et PCI DSS Level 1. Pour les entités essentielles et importantes NIS 2, l'ANSSI recommande de vérifier que les traitements critiques restent dans des régions EU et de documenter les mesures de sécurité mises en place conformément à l'article 21 de NIS 2.

Quelle est la différence entre SCC Standard et SCC Enterprise ?

SCC Standard (gratuit) offre la détection des misconfigurations de base et l'inventaire des assets GCP. SCC Premium ajoute Event Threat Detection, Container Threat Detection, et VM Manager pour les vulnérabilités. SCC Enterprise (la nouvelle offre 2024+) intègre Chronicle SIEM, la gestion multi-cloud (AWS et Azure), et Mandiant Threat Intelligence pour une plateforme

CNAPP (Cloud-Native Application Protection Platform) complète. Le choix entre Standard, Premium et Enterprise dépend du volume de projets GCP et du niveau de maturité SOC visé.

Comment protéger les secrets applicatifs dans GCP ?

La bonne pratique est d'utiliser **Secret Manager GCP** pour tous les secrets applicatifs (clés API, mots de passe de bases de données, certificats) plutôt que de les stocker dans des variables d'environnement, des fichiers de configuration, ou des buckets Cloud Storage. Secret Manager offre le versioning des secrets, la rotation automatique, les audit logs d'accès, et la réplication multi-région. Les accès aux secrets via IAM (`roles/secretmanager.secretAccessor`) doivent être accordés uniquement aux comptes de service spécifiques qui en ont besoin, avec activation des logs Data Access pour surveiller chaque accès aux secrets en production.

Accompagnement sécurité GCP : audit et mise en conformité NIS 2

La sécurisation d'une infrastructure GCP nécessite une expertise technique combinant la maîtrise du modèle IAM GCP, des services de sécurité natifs (SCC, VPC Service Controls, Cloud Armor), et des exigences réglementaires françaises (NIS 2, RGPD). Notre service de RSSI externalisé réalise des audits de sécurité GCP complets incluant la revue des IAM bindings, la configuration des Org Policies, l'activation et le paramétrage du Security Command Center, et la mise en place des contrôles VPC Service Controls pour vos données les plus sensibles.

Démarrez par notre diagnostic NIS 2 pour évaluer votre maturité de sécurité cloud GCP et identifier les lacunes prioritaires. Notre service de pentest peut également réaliser des simulations d'attaque sur votre infrastructure GCP (IAM privilege escalation, exfiltration depuis des buckets publics, SSRF vers les métadonnées GCP) pour valider l'efficacité des contrôles de sécurité mis en place et identifier les chemins d'attaque encore exploitables dans votre configuration actuelle.