AYI NEDJIMI Consultants

Guide Complet d'Audit de Sécurité Google Workspace

Catégorie : Guides Rouges Lecture : 3 min Publié le : 22/03/2026 Auteur : Ayi NEDJIMI

Guide complet d'audit de sécurité Google Workspace 2026 : IAM, DLP, Vault, Device Management — 10 niveaux de contrôle, scripts Apps Script inclus.

Ce guide de référence pour l'**audit de sécurité Google Workspace** couvre 10 niveaux de contrôle — de la configuration *IAM (Identity and Access Management)* jusqu'à la conformité réglementaire RGPD et NIS2. Rédigé par **Ayi NEDJIMI**, expert en cybersécurité cloud et conformité, il détaille les méthodes d'audit des 47 domaines de configuration Google Workspace : gestion des utilisateurs et des groupes, politiques **MFA** et **SAML**, sécurité des applications tierces (OAuth), *Data Loss Prevention (DLP)*, Google Vault pour l'eDiscovery, **Mobile Device Management (MDM)**, audit des logs Admin, Chrome Enterprise, et intégration SIEM. Chaque domaine inclut les requêtes d'audit **Apps Script**, les APIs Admin SDK, les indicateurs de risque, et les remédiations recommandées — permettant de générer un rapport d'audit complet en moins de 8 heures.

Structure du Guide Audit Google Workspace

Le guide est organisé en cinq chapitres couvrant progressivement tous les vecteurs d'attaque Google Workspace :

- **Chapitre 1 — IAM et Gestion des Identités** : Super Admins, groupes de sécurité, MFA enforcement, fédération SAML/OIDC
- **Chapitre 2 — Sécurité Email et Collaboration** : Gmail security, Drive DLP, Meet, Chat, phishing protection
- **Chapitre 3 — Applications Tierces et APIs** : OAuth scope audit, marketplace apps, Connected Apps, service accounts GCP
- **Chapitre 4 — Gouvernance des Données** : Google Vault, classification, rétention, eDiscovery, RGPD
- **Chapitre 5 — Endpoints et Conformité** : Chrome Enterprise, MDM, Context-Aware Access, NIS2, audit trails

Points Clés — Audit Google Workspace 2026

- Auditez les comptes **Super Admin** en priorité : nombre total (idéalement 2-4), connexions récentes, absence de MFA — ces comptes donnent accès à l'intégralité du tenant
- Les applications OAuth tierces avec des *scopes sensibles* (Drive read/write, Gmail send, Admin SDK) sont le vecteur #1 de compromission cloud — auditez-les systématiquement
- Activez le **Context-Aware Access** pour les ressources critiques — bloque les connexions depuis des appareils non gérés ou des localisations suspectes
- La politique de **rétention Google Vault** doit couvrir toutes les données réglementées (7 ans pour la comptabilité, 5 ans pour les RH) — vérifiez les gaps de couverture
- Exportez et analysez les **Admin Audit Logs** hebdomadairement : tout changement de configuration de sécurité par un Super Admin doit être tracé et justifié

Pourquoi auditer Google Workspace régulièrement en 2026 ?

Google Workspace est devenu un vecteur d'attaque majeur : les attaques de type **Business Email Compromise (BEC)** via Google Workspace ont augmenté de 67% en 2025 selon le rapport Verizon DBIR. Les techniques de compromission incluent le vol de tokens OAuth, l'abus des délégations de domaine entier (*Domain-Wide Delegation*), et l'exploitation d'applications tierces malveillantes installées via le Google Marketplace.

La directive **NIS2**, applicable depuis octobre 2024, impose un audit annuel des systèmes d'information cloud pour les opérateurs essentiels. Notre guide NIS2 détaille les obligations spécifiques aux environnements Google Workspace. Pour les aspects Azure AD / Microsoft 365, notre guide de détection des attaques Azure AD est complémentaire.

Comment auditer les permissions OAuth des applications tierces ?

L'audit des applications **OAuth** connectées à Google Workspace est souvent négligé mais critique. Une application tierce avec le scope `https://www.googleapis.com/auth/gmail.readonly` accordé par un Super Admin peut exfiltrer tous les emails de l'organisation. Ce guide fournit le script **Apps Script** complet pour inventorier toutes les applications OAuth, leurs scopes, et les utilisateurs qui les ont autorisées — permettant d'identifier les applications à risque en quelques minutes.

Pour les environnements disposant également d'un locataire Azure, notre article sur les abus OAuth/OIDC et sécurité des consentements couvre les techniques d'attaque cross-cloud. Les fonctionnalités de sécurité Google Workspace et les bonnes pratiques d'audit Google Admin sont les références officielles de ce guide.

Comment implémenter un programme d'audit Google Workspace continu ?

Ce guide propose un programme d'audit en trois niveaux : audit hebdomadaire automatisé (logs Admin SDK, connexions suspectes, nouveaux OAuth), audit mensuel manuel (Super Admin MFA, groupes de sécurité, politique DLP), et audit trimestriel complet (intégralité des 47 domaines). Les scripts Apps Script fournis automatisent l'audit hebdomadaire et génèrent un rapport HTML envoyé par email aux responsables sécurité.

Pour les entreprises avec des obligations de conformité RGPD, l'intégration avec **Google Vault** et la politique de rétention des données est détaillée dans le chapitre 4. Notre article sur la sécurité des agents LLM couvre également les risques spécifiques liés à l'utilisation de **Gemini for Workspace** et des extensions IA Google.

Quels outils complémentaires à l'audit natif Google Workspace ?

Le tableau de bord d'administration Google offre des fonctionnalités d'audit natives, mais des outils spécialisés permettent d'approfondir l'analyse : **GAM (Google Apps Manager)** pour les requêtes d'audit en ligne de commande, **Google Workspace Alert Center** pour les alertes de sécurité temps réel, et **Chronicle SIEM** (Google) pour la corrélation des logs à l'échelle. Ce guide couvre l'intégration de ces outils dans un programme SOC existant, notamment via les connecteurs SIEM disponibles pour Microsoft Sentinel.

Sources et références : MITRE ATT&CK · ANSSI

Conclusion

Ce guide est mis à jour trimestriellement pour intégrer les nouvelles fonctionnalités de sécurité Google Workspace et les techniques d'attaque émergentes. La version PDF inclut les 47 checklists d'audit prêtes à l'emploi et les scripts Apps Script commentés.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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