Checklist Sécurité GOOGLE WORKSPACE

Ayi NEDJIMI Consultants
ayinedjimi-consultants.fr
v1.0 — 2026-04-04 · 176 controles

Sommaire

Section 1 — GESTION DES COMPTES & IDENTITÉS

1.0 — GESTION DES COMPTES & IDENTITÉS

1.1.1 *Configuration des rôles super-administrateur*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les comptes super-administrateur disposent d'un accès complet à tous les services Google Workspace. Une gestion stricte de ces comptes est essentielle pour prévenir les compromissions et maintenir la sécurité organisationnelle. Le principe du moindre privilège doit être appliqué.

REMÉDIATION :

1. Limiter le nombre de super-administrateurs à 2-4 maximum
2. Utiliser des comptes dédiés uniquement pour l'administration
3. Séparer les comptes d'administration des comptes utilisateurs standards

VALEUR PAR DÉFAUT :

Un super-administrateur est créé lors de l'inscription

1.1.2 *Authentification multifacteur pour super-administrateurs*

MITRE ATT&CK : T1078.004

DESCRIPTION :

L'authentification multifacteur est cruciale pour les comptes à privilèges élevés. Les super-administrateurs doivent utiliser des méthodes MFA robustes comme les clés de sécurité FIDO pour résister aux attaques de phishing avancées.

REMÉDIATION :

1. Console Admin > Sécurité > Authentification à 2 facteurs
2. Activer "Appliquer la validation en 2 étapes"
3. Configurer des clés de sécurité comme méthode principale

VALEUR PAR DÉFAUT :

MFA optionnel pour tous les utilisateurs

1.1.3 *Comptes de récupération configurés*

MITRE ATT&CK : T1098

DESCRIPTION :

Les comptes de récupération permettent de retrouver l'accès administratif en cas de compromission ou perte d'accès des comptes principaux. Ces comptes doivent être sécurisés et utilisés uniquement en cas d'urgence.

REMÉDIATION :

1. Configurer 1-2 comptes de récupération
2. Utiliser des adresses email externes sécurisées
3. Documenter la procédure de récupération

VALEUR PAR DÉFAUT :

Aucun compte de récupération configuré

1.1.4 *Délégation d'administration limitée*

MITRE ATT&CK : T1098.003

DESCRIPTION :

La délégation permet d'accorder des privilèges administratifs granulaires sans donner l'accès super-administrateur complet. Cette approche réduit la surface d'attaque et respecte le principe du moindre privilège.

REMÉDIATION :

1. Créer des rôles administratifs granulaires
2. Assigner les privilèges minimum nécessaires
3. Réviser régulièrement les attributions de rôles

VALEUR PAR DÉFAUT :

Rôles prédéfinis uniquement disponibles

1.1.5 *Audit des connexions administratives*

MITRE ATT&CK : T1078

DESCRIPTION :

Le monitoring des connexions administratives permet de détecter les accès suspects ou non autorisés. Les logs d'audit doivent être configurés pour tracer toutes les activités administratives critiques.

REMÉDIATION :

1. Activer les rapports d'audit administrateur
2. Configurer des alertes pour les connexions suspectes
3. Réviser mensuellement les logs d'accès

VALEUR PAR DÉFAUT :

Rapports d'audit activés par défaut

1.2.1 *Provisionnement automatique des utilisateurs*

MITRE ATT&CK : T1136

DESCRIPTION :

Le provisionnement automatique via LDAP, SAML ou API assure la cohérence entre les systèmes d'identité et réduit les erreurs manuelles. Cette approche améliore la sécurité et l'efficacité opérationnelle.

REMÉDIATION :

1. Configurer Google Cloud Directory Sync (GCDS) si LDAP
2. Implémenter SAML provisioning si SSO
3. Automatiser via Admin SDK API

VALEUR PAR DÉFAUT :

Création manuelle uniquement

1.2.2 *Désactivation automatique des comptes inactifs*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les comptes inactifs représentent un risque de sécurité car ils peuvent être compromis sans détection. Une politique de désactivation automatique après une période d'inactivité définie renforce la posture sécuritaire.

REMÉDIATION :

1. Définir une période d'inactivité (ex: 90 jours)
2. Configurer la suspension automatique
3. Implémenter un processus de révision avant suppression

VALEUR PAR DÉFAUT :

Aucune suspension automatique

1.2.3 *Gestion du cycle de vie des comptes*

MITRE ATT&CK : T1098

DESCRIPTION :

Un processus formalisé de gestion du cycle de vie (création, modification, suspension, suppression) garantit la traçabilité et la cohérence des opérations sur les comptes utilisateurs.

REMÉDIATION :

1. Documenter les procédures de cycle de vie
2. Implémenter des workflows d'approbation
3. Auditer régulièrement les changements de comptes

VALEUR PAR DÉFAUT :

Gestion manuelle sans workflow

1.2.4 *Attribution des licences par unité organisationnelle*

MITRE ATT&CK : T1069.003

DESCRIPTION :

L'attribution granulaire des licences selon l'unité organisationnelle permet un contrôle précis des fonctionnalités disponibles et optimise les coûts tout en maintenant la sécurité.

REMÉDIATION :

1. Créer des unités organisationnelles par fonction/département
2. Attribuer les licences selon les besoins métier
3. Réviser trimestriellement l'utilisation des licences

VALEUR PAR DÉFAUT :

Attribution manuelle des licences

1.3.1 *Structure des unités organisationnelles*

MITRE ATT&CK : T1069.003

DESCRIPTION :

Une structure d'unités organisationnelles bien conçue facilite l'application de politiques de sécurité granulaires et simplifie la gestion des utilisateurs et des ressources.

REMÉDIATION :

1. Concevoir une hiérarchie logique (département/fonction)
2. Limiter la profondeur à 3-4 niveaux maximum
3. Documenter la structure et les responsabilités

VALEUR PAR DÉFAUT :

Unité organisationnelle racine uniquement

1.3.2 *Héritage des politiques par OU*

MITRE ATT&CK : T1069.003

DESCRIPTION :
L'héritage des politiques permet d'appliquer des configurations de sécurité cohérentes à travers l'organisation tout en permettant des exceptions justifiées pour des unités spécifiques.

REMÉDIATION :
1. Configurer l'héritage par défaut des politiques
2. Justifier et documenter les exceptions
3. Réviser régulièrement les surcharges de politiques

VALEUR PAR DÉFAUT :
Héritage activé par défaut

1.3.3 *Séparation des environnements par OU*

MITRE ATT&CK : T1078.002

DESCRIPTION :
La séparation des environnements (production, test, développement) via les unités organisationnelles renforce l'isolation et permet l'application de politiques de sécurité différenciées.

REMÉDIATION :
1. Créer des OU distinctes par environnement
2. Appliquer des politiques restrictives à la production
3. Limiter les permissions inter-environnements

VALEUR PAR DÉFAUT :
Aucune séparation d'environnements

1.4.1 *Politique de mots de passe renforcée*

MITRE ATT&CK : T1110.001

DESCRIPTION :
Des politiques de mots de passe robustes constituent la première ligne de défense contre les attaques par force brute et les compromissions de comptes. La complexité doit être équilibrée avec l'utilisabilité.

REMÉDIATION :
1. Longueur minimum 12 caractères
2. Expiration tous les 180 jours maximum
3. Interdire la réutilisation des 12 derniers mots de passe

VALEUR PAR DÉFAUT :
8 caractères minimum, pas d'expiration

1.4.2 *Historique et réutilisation des mots de passe*

MITRE ATT&CK : T1110.001

DESCRIPTION :
L'historique des mots de passe empêche la réutilisation de mots de passe précédents, réduisant les risques liés aux mots de passe compromis ou devinés.

REMÉDIATION :
1. Conserver l'historique des 12 derniers mots de passe
2. Empêcher la réutilisation immédiate
3. Éduquer les utilisateurs sur la création de mots de passe forts

VALEUR PAR DÉFAUT :
Historique de 1 mot de passe

1.4.3 *Verrouillage de compte après échecs*

MITRE ATT&CK : T1110

DESCRIPTION :
Le verrouillage automatique des comptes après plusieurs tentatives de connexion infructueuses protège contre les attaques par force brute et les tentatives de compromission automatisées.

REMÉDIATION :
1. Verrouiller après 5 tentatives échouées
2. Durée de verrouillage: 15-30 minutes
3. Alerter l'administrateur en cas de verrouillages répétés

VALEUR PAR DÉFAUT :
Verrouillage après 100 tentatives

1.5.1 *Révision périodique des comptes utilisateurs*

MITRE ATT&CK : T1078.002

DESCRIPTION :
La révision régulière des comptes utilisateurs permet d'identifier les comptes orphelins, inactifs ou surdimensionnés en termes de privilèges, contribuant à maintenir une posture sécuritaire optimale.

REMÉDIATION :
1. Planifier des révisions trimestrielles
2. Identifier les comptes inactifs >90 jours
3. Valider la nécessité métier de chaque compte

VALEUR PAR DÉFAUT :
Aucune révision automatique

1.5.2 *Audit des attributions de groupes*

MITRE ATT&CK : T1069.003

DESCRIPTION :
L'appartenance aux groupes détermine les accès et privilèges des utilisateurs. Un audit régulier garantit que les permissions restent alignées avec les responsabilités actuelles des utilisateurs.

REMÉDIATION :
1. Auditer mensuellement les groupes à privilèges
2. Valider l'appartenance avec les responsables métier
3. Supprimer les membres non autorisés

VALEUR PAR DÉFAUT :
Aucun audit automatique des groupes

1.5.3 *Monitoring des changements de privilèges*

MITRE ATT&CK : T1098.003

DESCRIPTION :
La surveillance en temps réel des modifications de privilèges permet de détecter les élévations suspectes de droits et de réagir rapidement aux compromissions potentielles.

REMÉDIATION :
1. Configurer des alertes pour les changements de privilèges
2. Réviser immédiatement toute élévation non planifiée
3. Maintenir un log d'approbation des changements

VALEUR PAR DÉFAUT :
Aucune alerte automatique

1.6.1 *Comptes de service sécurisés*

MITRE ATT&CK : T1078.003

DESCRIPTION :
Les comptes de service automatisent les tâches mais représentent un risque s'ils sont mal sécurisés. Ils nécessitent une gestion stricte avec des privilèges minimaux et une rotation régulière des clés.

REMÉDIATION :
1. Créer des comptes de service dédiés par application
2. Appliquer le principe du moindre privilège
3. Rotation des clés tous les 90 jours

VALEUR PAR DÉFAUT :
Gestion manuelle des comptes de service

1.6.2 *Authentification par clés API sécurisées*

MITRE ATT&CK : T1552.001

DESCRIPTION :
Les clés API permettent l'accès programmatique aux services Google Workspace. Leur compromission peut entraîner un accès non autorisé étendu. Une gestion sécurisée est critique.

REMÉDIATION :
1. Restreindre l'utilisation des clés API par IP/domaine
2. Rotation automatique tous les 60 jours
3. Auditer régulièrement l'utilisation des clés

VALEUR PAR DÉFAUT :
Clés API sans restriction d'usage

1.6.3 *Monitoring de l'utilisation des comptes de service*

MITRE ATT&CK : T1078.003

DESCRIPTION :

Le monitoring de l'activité des comptes de service permet de détecter les utilisations anormales ou non autorisées et de maintenir une visibilité sur les accès automatisés.

REMÉDIATION :

1. Configurer des alertes pour l'usage inhabituel
2. Réviser mensuellement les logs d'accès
3. Corréler avec les déploiements d'applications

VALEUR PAR DÉFAUT :

Aucun monitoring spécifique des comptes de service

1.7.1 *Processus d'offboarding formalisé*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Un processus d'offboarding structuré garantit la révocation complète des accès lors des départs d'employés et la sécurisation des données, réduisant les risques de fuite ou d'accès malveillant post-départ.

REMÉDIATION :

1. Checklist d'offboarding standardisée
2. Suspension immédiate à la notification de départ
3. Transfert des données vers le manager sous 48h

VALEUR PAR DÉFAUT :

Processus manuel non formalisé

1.7.2 *Transfert sécurisé des données utilisateur*

MITRE ATT&CK : T1005

DESCRIPTION :

Le transfert des données utilisateur lors des départs doit être sécurisé et audité pour préserver la continuité métier tout en empêchant les fuites de données sensibles.

REMÉDIATION :

1. Utiliser l'outil de transfert natif Google
2. Approuver les transferts par le management
3. Auditer le contenu transféré

VALEUR PAR DÉFAUT :

Aucun transfert automatique configuré

1.0 — GESTION DES COMPTES & IDENTITÉS

1.1.1 *Configuration des rôles super-administrateur*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les comptes super-administrateur disposent d'un accès complet à tous les services Google Workspace. Une gestion stricte de ces comptes est essentielle pour prévenir les compromissions et maintenir la sécurité organisationnelle. Le principe du moindre privilège doit être appliqué.

AUDIT :

- Console Admin > Comptes > Rôles d'administrateur
- API: GET https://admin.googleapis.com/admin/directory/v1/roleAssignments
- gam print adminroles

REMÉDIATION :

1. Limiter le nombre de super-administrateurs à 2-4 maximum
2. Utiliser des comptes dédiés uniquement pour l'administration
3. Séparer les comptes d'administration des comptes utilisateurs standards

VALEUR PAR DÉFAUT :

Un super-administrateur est créé lors de l'inscription

1.1.2 *Authentification multifacteur pour super-administrateurs*

MITRE ATT&CK : T1078.004

DESCRIPTION :

L'authentification multifacteur est cruciale pour les comptes à privilèges élevés. Les super-administrateurs doivent utiliser des méthodes MFA robustes comme les clés de sécurité FIDO pour résister aux attaques de phishing avancées.

AUDIT :

- Console Admin > Sécurité > Authentification à 2 facteurs
- API: GET https://admin.googleapis.com/admin/directory/v1/users/{userKey}
- gam info user admin@domain.com

REMÉDIATION :

1. Console Admin > Sécurité > Authentification à 2 facteurs
2. Activer "Appliquer la validation en 2 étapes"
3. Configurer des clés de sécurité comme méthode principale

VALEUR PAR DÉFAUT :

MFA optionnel pour tous les utilisateurs

1.1.3 *Comptes de récupération configurés*

MITRE ATT&CK : T1098

DESCRIPTION :

Les comptes de récupération permettent de retrouver l'accès administratif en cas de compromission ou perte d'accès des comptes principaux. Ces comptes doivent être sécurisés et utilisés uniquement en cas d'urgence.

AUDIT :

- Console Admin > Comptes > Récupération de compte administrateur
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}/orgunits
- gam print orgs

REMÉDIATION :

1. Configurer 1-2 comptes de récupération
2. Utiliser des adresses email externes sécurisées
3. Documenter la procédure de récupération

VALEUR PAR DÉFAUT :

Aucun compte de récupération configuré

1.1.4 *Délégation d'administration limitée*

MITRE ATT&CK : T1098.003

DESCRIPTION :

La délégation permet d'accorder des privilèges administratifs granulaires sans donner l'accès super-administrateur complet. Cette approche réduit la surface d'attaque et respecte le principe du moindre privilège.

AUDIT :

- Console Admin > Comptes > Rôles d'administrateur > Rôles personnalisés
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}/roles
- gam print adminroles

REMÉDIATION :

1. Créer des rôles administratifs granulaires
2. Assigner les privilèges minimum nécessaires
3. Réviser régulièrement les attributions de rôles

VALEUR PAR DÉFAUT :

Rôles prédéfinis uniquement disponibles

1.1.5 *Audit des connexions administratives*

MITRE ATT&CK : T1078

DESCRIPTION :

Le monitoring des connexions administratives permet de détecter les accès suspects ou non autorisés. Les logs d'audit doivent être configurés pour tracer toutes les activités administratives critiques.

AUDIT :

- Console Admin > Rapports > Rapports d'audit > Connexion administrateur
- API: GET https://admin.googleapis.com/admin/reports/v1/activity/users/{userKey}/applications/admin
- gam report admin start -30d end today

REMÉDIATION :

1. Activer les rapports d'audit administrateur
2. Configurer des alertes pour les connexions suspectes
3. Réviser mensuellement les logs d'accès

VALEUR PAR DÉFAUT :

Rapports d'audit activés par défaut

1.2.1 *Provisionnement automatique des utilisateurs*

MITRE ATT&CK : T1136

DESCRIPTION :

Le provisionnement automatique via LDAP, SAML ou API assure la cohérence entre les systèmes d'identité et réduit les erreurs manuelles. Cette approche améliore la sécurité et l'efficacité opérationnelle.

AUDIT :

- Console Admin > Comptes > Synchronisation LDAP/Active Directory
- API: GET https://admin.googleapis.com/admin/directory/v1/users
- gam print users

REMÉDIATION :

1. Configurer Google Cloud Directory Sync (GCDS) si LDAP
2. Implémenter SAML provisioning si SSO
3. Automatiser via Admin SDK API

VALEUR PAR DÉFAUT :

Création manuelle uniquement

1.2.2 *Désactivation automatique des comptes inactifs*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les comptes inactifs représentent un risque de sécurité car ils peuvent être compromis sans détection. Une politique de désactivation automatique après une période d'inactivité définie renforce la posture sécuritaire.

AUDIT :

- Console Admin > Comptes > Paramètres utilisateur > Suspension automatique
- API: GET https://admin.googleapis.com/admin/directory/v1/users?query='isSuspended=false'
- gam print users suspended

REMÉDIATION :

1. Définir une période d'inactivité (ex: 90 jours)
2. Configurer la suspension automatique
3. Implémenter un processus de révision avant suppression

VALEUR PAR DÉFAUT :

Aucune suspension automatique

1.2.3 *Gestion du cycle de vie des comptes*

MITRE ATT&CK : T1098

DESCRIPTION :
Un processus formalisé de gestion du cycle de vie (création, modification, suspension, suppression) garantit la traçabilité et la cohérence des opérations sur les comptes utilisateurs.

AUDIT :
- Console Admin > Rapports > Rapports d'audit > Comptes
- API: GET https://admin.googleapis.com/admin/reports/v1/activity/users/all/applications/admin
- gam report admin filter='USER_CREATED,USER_DELETED,USER_SUSPENDED'

REMÉDIATION :
1. Documenter les procédures de cycle de vie
2. Implémenter des workflows d'approbation
3. Auditer régulièrement les changements de comptes

VALEUR PAR DÉFAUT :
Gestion manuelle sans workflow

1.2.4 *Attribution des licences par unité organisationnelle*

MITRE ATT&CK : T1069.003

DESCRIPTION :
L'attribution granulaire des licences selon l'unité organisationnelle permet un contrôle précis des fonctionnalités disponibles et optimise les coûts tout en maintenant la sécurité.

AUDIT :
- Console Admin > Facturation > Abonnements > Attribution des licences
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}/orgunits
- gam print licenses

REMÉDIATION :
1. Créer des unités organisationnelles par fonction/département
2. Attribuer les licences selon les besoins métier
3. Réviser trimestriellement l'utilisation des licences

VALEUR PAR DÉFAUT :
Attribution manuelle des licences

1.3.1 *Structure des unités organisationnelles*

MITRE ATT&CK : T1069.003

DESCRIPTION :
Une structure d'unités organisationnelles bien conçue facilite l'application de politiques de sécurité granulaires et simplifie la gestion des utilisateurs et des ressources.

AUDIT :
- Console Admin > Annuaire > Unités organisationnelles
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}/orgunits
- gam print orgs

REMÉDIATION :
1. Concevoir une hiérarchie logique (département/fonction)
2. Limiter la profondeur à 3-4 niveaux maximum
3. Documenter la structure et les responsabilités

VALEUR PAR DÉFAUT :
Unité organisationnelle racine uniquement

1.3.2 *Héritage des politiques par OU*

MITRE ATT&CK : T1069.003

DESCRIPTION :
L'héritage des politiques permet d'appliquer des configurations de sécurité cohérentes à travers l'organisation tout en permettant des exceptions justifiées pour des unités spécifiques.

AUDIT :
- Console Admin > Annuaire > Unités organisationnelles > [Sélectionner OU] > Héritage
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}/orgunits/{orgUnitPath}
- gam info org /Finance

REMÉDIATION :
1. Configurer l'héritage par défaut des politiques
2. Justifier et documenter les exceptions
3. Réviser régulièrement les surcharges de politiques

VALEUR PAR DÉFAUT :
Héritage activé par défaut

1.4.1 *Politique de mots de passe renforcée*

MITRE ATT&CK : T1110.001

DESCRIPTION :

Des politiques de mots de passe robustes constituent la première ligne de défense contre les attaques par force brute et les compromissions de comptes. La complexité doit être équilibrée avec l'utilisabilité.

AUDIT :

- Console Admin > Sécurité > Paramètres des mots de passe
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}/orgunits/{orgUnitPath}
- gam info domain domain.com

REMÉDIATION :

1. Longueur minimum 12 caractères
2. Expiration tous les 180 jours maximum
3. Interdire la réutilisation des 12 derniers mots de passe

VALEUR PAR DÉFAUT :

8 caractères minimum, pas d'expiration

1.5.1 *Révision périodique des comptes utilisateurs*

MITRE ATT&CK : T1078.002

DESCRIPTION :

La révision régulière des comptes utilisateurs permet d'identifier les comptes orphelins, inactifs ou surdimensionnés en termes de privilèges, contribuant à maintenir une posture sécuritaire optimale.

AUDIT :

- Console Admin > Rapports > Comptes > Activité des utilisateurs
- API: GET https://admin.googleapis.com/admin/reports/v1/usage/users/all/dates/{date}
- gam report users filter='accounts:last_login_time<2024-01-01'

REMÉDIATION :

1. Planifier des révisions trimestrielles
2. Identifier les comptes inactifs >90 jours
3. Valider la nécessité métier de chaque compte

VALEUR PAR DÉFAUT :

Aucune révision automatique

2.0 — AUTHENTIFICATION & MFA

2.1.1 *Authentification à deux facteurs obligatoire*

MITRE ATT&CK : T1078

DESCRIPTION :
L'authentification à deux facteurs (2FA/MFA) est essentielle pour protéger les comptes contre les compromissions par mot de passe. Elle doit être obligatoire pour tous les utilisateurs sans exception.

AUDIT :
- Console Admin > Sécurité > Authentification à 2 facteurs
- API: GET https://admin.googleapis.com/admin/directory/v1/users?projection=full
- gam info domain domain.com | grep 2sv

REMÉDIATION :
1. Console Admin > Sécurité > Authentification à 2 facteurs
2. Activer "Appliquer la validation en 2 étapes"
3. Définir une période de grâce de 1 semaine maximum

VALEUR PAR DÉFAUT :
MFA optionnel

2.1.2 *Méthodes MFA autorisées*

MITRE ATT&CK : T1111

DESCRIPTION :
Toutes les méthodes MFA ne présentent pas le même niveau de sécurité. Les clés de sécurité FIDO offrent la meilleure protection contre le phishing, tandis que les SMS sont vulnérables aux attaques SIM swapping.

AUDIT :
- Console Admin > Sécurité > Authentification à 2 facteurs > Méthodes autorisées
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}
- gam info domain domain.com settings

REMÉDIATION :
1. Privilégier les clés de sécurité FIDO/WebAuthn
2. Autoriser Google Authenticator en complément
3. Désactiver les SMS sauf cas d'usage justifiés

VALEUR PAR DÉFAUT :
Toutes les méthodes autorisées

2.1.3 *Codes de récupération sécurisés*

MITRE ATT&CK : T1078

DESCRIPTION :
Les codes de récupération permettent aux utilisateurs de retrouver l'accès en cas de perte du second facteur. Ils doivent être gérés de manière sécurisée et avoir une durée de vie limitée.

AUDIT :
- Console Admin > Sécurité > Authentification à 2 facteurs > Codes de secours
- API: GET https://admin.googleapis.com/admin/directory/v1/users/{userKey}
- gam info user user@domain.com | grep backup

REMÉDIATION :
1. Générer automatiquement 10 codes de récupération
2. Expirer les codes après 12 mois
3. Informer les utilisateurs du stockage sécurisé

VALEUR PAR DÉFAUT :
10 codes de récupération permanents

2.1.4 *Clés de sécurité pour comptes privilégiés*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les comptes administrateurs et privilégiés sont des cibles prioritaires. L'utilisation obligatoire de clés de sécurité FIDO offre une protection maximale contre les attaques de phishing avancées.

AUDIT :

- Console Admin > Sécurité > Authentification à 2 facteurs > Clés de sécurité uniquement
- API: GET https://admin.googleapis.com/admin/directory/v1/users?query='isAdmin=true'
- gam print users query 'isAdmin=true'

REMÉDIATION :

1. Exiger les clés FIDO pour tous les administrateurs
2. Désactiver les autres méthodes MFA pour ces comptes
3. Fournir des clés de sauvegarde

VALEUR PAR DÉFAUT :

Toutes méthodes MFA autorisées pour les admins

2.1.5 *Politique de session et timeout*

MITRE ATT&CK : T1185

DESCRIPTION :

La gestion des sessions limite l'exposition en cas d'abandon de session ou de compromission d'un poste de travail. Les timeouts doivent être équilibrés entre sécurité et productivité.

AUDIT :

- Console Admin > Sécurité > Paramètres de session > Durée de session
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}
- gam info domain domain.com settings

REMÉDIATION :

1. Configurer un timeout de session à 8 heures
2. Exiger une ré-authentification pour les actions sensibles
3. Configurer la déconnexion automatique en cas d'inactivité

VALEUR PAR DÉFAUT :

Session persistante jusqu'à 14 jours

2.2.1 *Configuration SSO/SAML sécurisée*

MITRE ATT&CK : T1078

DESCRIPTION :

Le Single Sign-On SAML centralise l'authentification et peut renforcer la sécurité s'il est correctement configuré. La validation des certificats et le chiffrement des assertions sont cruciaux.

AUDIT :

- Console Admin > Sécurité > Configuration SSO
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}
- gam info domain domain.com sso

REMÉDIATION :

1. Utiliser uniquement HTTPS pour les endpoints SAML
2. Valider les certificats X.509 du fournisseur d'identité
3. Chiffrer les assertions SAML

VALEUR PAR DÉFAUT :

SSO désactivé

2.2.2 *Fournisseur d'identité de confiance*

MITRE ATT&CK : T1078

DESCRIPTION :

Le fournisseur d'identité SSO doit être durci et maintenu à jour. Sa compromission affecterait l'ensemble de l'écosystème Google Workspace.

AUDIT :

- Console Admin > Sécurité > Configuration SSO > URL de connexion
- Vérification manuelle de la configuration du fournisseur d'identité
- Audit des logs du fournisseur d'identité

REMÉDIATION :

1. Appliquer les mises à jour sécurité du fournisseur d'identité
2. Configurer MFA sur le fournisseur d'identité
3. Auditer régulièrement les configurations

VALEUR PAR DÉFAUT :

Configuration selon le fournisseur d'identité

2.2.3 *Validation des certificats SAML*

MITRE ATT&CK : T1556.006

DESCRIPTION :

La validation stricte des certificats SAML empêche les attaques man-in-the-middle et garantit l'intégrité des échanges d'authentification.

AUDIT :

- Console Admin > Sécurité > Configuration SSO > Certificat de vérification
- Vérification de la chaîne de certificats
- Validation des dates d'expiration

REMÉDIATION :

1. Utiliser des certificats signés par une AC de confiance
2. Configurer la validation stricte des certificats
3. Planifier le renouvellement avant expiration

VALEUR PAR DÉFAUT :

Validation selon configuration

2.2.4 *Mappage des attributs SAML*

MITRE ATT&CK : T1078

DESCRIPTION :

Le mappage correct des attributs SAML garantit que les utilisateurs reçoivent les bonnes permissions et appartenances aux groupes lors de l'authentification SSO.

AUDIT :

- Console Admin > Sécurité > Configuration SSO > Mappage des attributs
- Vérification des groupes assignés automatiquement
- Test du provisionnement automatique

REMÉDIATION :

1. Mapper les attributs utilisateur essentiels (nom, email, groupes)
2. Tester le provisionnement avec des comptes de test
3. Valider les permissions assignées automatiquement

VALEUR PAR DÉFAUT :

Mappage basique email/nom

2.2.5 *Fallback d'authentification sécurisé*

MITRE ATT&CK : T1078

DESCRIPTION :

En cas de panne du fournisseur d'identité SSO, un mécanisme de fallback doit permettre l'accès d'urgence tout en maintenant la sécurité.

AUDIT :

- Console Admin > Sécurité > Configuration SSO > Comptes de contournement
- Test des comptes d'urgence
- Documentation des procédures de fallback

REMÉDIATION :

1. Configurer des comptes d'administrateur de contournement
2. Documenter les procédures d'urgence
3. Tester régulièrement les mécanismes de fallback

VALEUR PAR DÉFAUT :

Authentification Google Workspace native

2.3.1 *Restriction d'accès par géolocalisation*

MITRE ATT&CK : T1078

DESCRIPTION :

Les restrictions géographiques peuvent limiter l'exposition aux attaques depuis des pays à risque, bien qu'elles doivent être configurées avec précaution pour ne pas impacter les utilisateurs légitimes.

AUDIT :

- Console Admin > Sécurité > Accès et contrôle des données > Restriction géographique
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}
- Analyse des logs de connexion par pays

REMÉDIATION :

1. Identifier les pays d'opération légitimes
2. Bloquer les pays à haut risque si applicable
3. Configurer des alertes pour les connexions inhabituelles

VALEUR PAR DÉFAUT :

Aucune restriction géographique

2.3.2 *Contrôle d'accès par plages IP*

MITRE ATT&CK : T1078

DESCRIPTION :
La restriction par plages IP peut renforcer la sécurité pour certaines unités organisationnelles sensibles, en limitant l'accès aux réseaux d'entreprise approuvés.

AUDIT :
- Console Admin > Sécurité > Accès et contrôle des données > Plages IP autorisées
- API: GET https://admin.googleapis.com/admin/directory/v1/customer/{customer}/orgunits
- Test d'accès depuis différentes IP

REMÉDIATION :
1. Définir les plages IP de l'entreprise
2. Configurer des exceptions pour les utilisateurs mobiles
3. Prévoir une procédure de déblocage d'urgence

VALEUR PAR DÉFAUT :
Aucune restriction IP

2.3.3 *Context-Aware Access (Accès contextuel)*

MITRE ATT&CK : T1078

DESCRIPTION :
L'accès contextuel analyse plusieurs facteurs (localisation, appareil, réseau) pour autoriser ou refuser l'accès, offrant une sécurité adaptative sans friction excessive pour l'utilisateur.

AUDIT :
- Console Admin > Sécurité > Context-Aware Access
- Google Cloud Console > BeyondCorp Enterprise
- Analyse des niveaux d'accès configurés

REMÉDIATION :
1. Configurer des niveaux d'accès selon le contexte
2. Définir des politiques pour les appareils gérés/non-gérés
3. Implémenter progressivement par unité organisationnelle

VALEUR PAR DÉFAUT :
Context-Aware Access désactivé

2.3.4 *Gestion des appareils de confiance*

MITRE ATT&CK : T1078

DESCRIPTION :
L'identification et la gestion des appareils de confiance permettent d'appliquer des politiques de sécurité différenciées selon que l'appareil est géré par l'entreprise ou non.

AUDIT :
- Console Admin > Appareils > Appareils mobiles
- Console Admin > Appareils > Points de terminaison
- gam print mobile query 'status:APPROVED'

REMÉDIATION :
1. Inventorier tous les appareils accédant aux services
2. Configurer des politiques pour appareils gérés/non-gérés
3. Exiger l'enregistrement pour les appareils sensibles

VALEUR PAR DÉFAUT :
Tous les appareils autorisés par défaut

2.4.1 *Alertes de connexions suspectes*

MITRE ATT&CK : T1078

DESCRIPTION :
Les alertes automatiques pour les connexions inhabituelles (géolocalisation, horaires, appareils) permettent une détection rapide des compromissions de comptes.

AUDIT :
- Console Admin > Sécurité > Centre d'alertes > Alertes de connexion
- API: GET https://admin.googleapis.com/admin/alertcenter/v1beta1/alerts
- Configuration des notifications par email

REMÉDIATION :
1. Configurer les alertes pour connexions géographiquement anormales
2. Activer les alertes pour nouveaux appareils
3. Définir les destinataires des alertes de sécurité

VALEUR PAR DÉFAUT :
Alertes de base configurées

2.4.2 *Monitoring des échecs d'authentification*

MITRE ATT&CK : T1110

DESCRIPTION :
Le suivi des tentatives d'authentification échouées aide à identifier les attaques par force brute et les tentatives de compromission de comptes utilisateur.

AUDIT :
- Console Admin > Rapports > Rapports d'audit > Connexion
- API: GET https://admin.googleapis.com/admin/reports/v1/activity/users/all/applications/login
- gam report login start -7d | grep FAILED

REMÉDIATION :
1. Configurer des seuils d'alerte pour les échecs répétés
2. Analyser les patterns d'attaque
3. Bloquer automatiquement après X tentatives échouées

VALEUR PAR DÉFAUT :
Logs disponibles sans alertes automatiques

2.4.3 *Analyse des patterns de connexion*

MITRE ATT&CK : T1078

DESCRIPTION :
L'analyse comportementale des patterns de connexion (horaires, fréquence, géolocalisation) permet d'établir des baselines et de détecter les anomalies.

AUDIT :
- Console Admin > Rapports > Rapports d'audit > Connexion > Analyse des tendances
- Outils d'analyse des logs (Google Cloud Logging)
- Tableaux de bord de monitoring personnalisés

REMÉDIATION :
1. Établir des baselines comportementales par utilisateur
2. Configurer des alertes pour les déviations significatives
3. Corréler avec les événements de sécurité

VALEUR PAR DÉFAUT :
Aucune analyse comportementale automatique

2.5.1 *Gestion des sessions concurrentes*

MITRE ATT&CK : T1185

DESCRIPTION :
La limitation du nombre de sessions simultanées par utilisateur réduit les risques de partage de comptes et limite l'exposition en cas de compromission.

AUDIT :
- Console Admin > Sécurité > Paramètres de session > Sessions simultanées
- Monitoring des sessions actives par utilisateur
- Analyse des connexions multiples suspectes

REMÉDIATION :
1. Limiter à 3-5 sessions simultanées maximum par utilisateur
2. Configurer la déconnexion des sessions les plus anciennes
3. Alerter en cas de sessions simultanées géographiquement distantes

VALEUR PAR DÉFAUT :
Sessions simultanées illimitées

2.5.2 *Révocation de sessions à distance*

MITRE ATT&CK : T1185

DESCRIPTION :
La capacité de révoquer à distance les sessions actives est essentielle en cas de compromission suspected ou de perte d'appareil.

AUDIT :
- Console Admin > Comptes > Sélectionner utilisateur > Déconnecter de toutes les sessions
- API: POST https://admin.googleapis.com/admin/directory/v1/users/{userKey}/signOut
- gam user user@domain.com signout

REMÉDIATION :
1. Former les administrateurs à la révocation de sessions
2. Documenter les procédures d'urgence
3. Tester régulièrement la fonctionnalité

VALEUR PAR DÉFAUT :
Révocation manuelle disponible

2.6.1 *Audit des méthodes d'authentification*

MITRE ATT&CK : T1078

DESCRIPTION :

L'audit régulier des méthodes d'authentification configurées par les utilisateurs permet d'identifier les configurations faibles ou obsolètes.

AUDIT :

- Console Admin > Rapports > Comptes > Méthodes de vérification en 2 étapes
- API: GET https://admin.googleapis.com/admin/directory/v1/users?projection=full
- gam print users 2sv

REMÉDIATION :

1. Auditer mensuellement les méthodes MFA configurées
2. Identifier les utilisateurs utilisant uniquement des méthodes faibles
3. Forcer la mise à jour vers des méthodes plus sécurisées

VALEUR PAR DÉFAUT :

Aucun audit automatique

3.0 — GMAIL — SÉCURITÉ EMAIL

3.1.1 *Configuration SPF (Sender Policy Framework)*

MITRE ATT&CK : T1566.001

DESCRIPTION :
SPF authentifie les serveurs autorisés à envoyer des emails au nom du domaine, réduisant significativement le risque d'usurpation d'identité et de phishing. Une configuration stricte est essentielle.

AUDIT :

- Console Admin > Applications > Google Workspace > Gmail > Authentifier les emails
- nslookup -type=TXT domain.com | grep 'v=spf1'
- dig TXT domain.com | grep SPF

REMÉDIATION :

1. Configurer un enregistrement SPF strict avec '-all'
2. Inclure uniquement les serveurs email autorisés
3. Tester avec des outils de validation SPF

VALEUR PAR DÉFAUT :
SPF non configuré par défaut

3.1.2 *Configuration DKIM (DomainKeys Identified Mail)*

MITRE ATT&CK : T1566.001

DESCRIPTION :
DKIM signe cryptographiquement les emails sortants, permettant aux destinataires de vérifier l'intégrité et l'authenticité des messages. Cette signature empêche la modification en transit.

AUDIT :

- Console Admin > Applications > Google Workspace > Gmail > Authentifier les emails > DKIM
- nslookup -type=TXT google._domainkey.domain.com
- Vérification de la signature DKIM sur emails envoyés

REMÉDIATION :

1. Activer DKIM pour tous les domaines
2. Générer des clés DKIM de 2048 bits minimum
3. Publier les clés publiques dans les enregistrements DNS

VALEUR PAR DÉFAUT :
DKIM désactivé par défaut

3.1.3 *Configuration DMARC stricte*

MITRE ATT&CK : T1566.001

DESCRIPTION :
DMARC utilise SPF et DKIM pour définir la politique de traitement des emails non authentifiés. Une politique 'reject' strict empêche la livraison d'emails usurpés.

AUDIT :

- Console Admin > Applications > Google Workspace > Gmail > Authentifier les emails > DMARC
- nslookup -type=TXT _dmarc.domain.com
- Analyse des rapports DMARC

REMÉDIATION :

1. Commencer par 'p=none' pour collecter des données
2. Progresser vers 'p=quarantine' puis 'p=reject'
3. Configurer des adresses de rapport RUA et RUF

VALEUR PAR DÉFAUT :
DMARC non configuré

3.1.4 *Authentification BIMI (Brand Indicators for Message Identification)*

MITRE ATT&CK : T1566.001

DESCRIPTION :
BIMI affiche le logo de l'entreprise dans les clients email pour les messages authentifiés, renforçant la reconnaissance de marque et la confiance des destinataires.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Authentifier les emails > BIMI
- nslookup -type=TXT default._bimi.domain.com
- Test d'affichage du logo dans Gmail

REMÉDIATION :
1. Obtenir un certificat VMC (Verified Mark Certificate)
2. Configurer l'enregistrement BIMI avec le logo SVG
3. Vérifier que DMARC est en mode 'quarantine' ou 'reject'

VALEUR PAR DÉFAUT :
BIMI non configuré

3.2.1 *Protection anti-phishing avancée*

MITRE ATT&CK : T1566.002

DESCRIPTION :
La protection anti-phishing utilise l'intelligence artificielle et l'analyse comportementale pour détecter les tentatives de hameçonnage sophistiquées, incluant les attaques de spear phishing ciblées.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Sécurité > Anti-phishing
- Console Admin > Centre d'alertes > Alertes de phishing
- Test avec des emails de phishing simulés

REMÉDIATION :
1. Activer la protection anti-phishing pour tous les utilisateurs
2. Configurer des alertes pour tentatives de phishing détectées
3. Former les utilisateurs à la reconnaissance du phishing

VALEUR PAR DÉFAUT :
Protection de base activée

3.2.2 *Analyse des pièces jointes malveillantes*

MITRE ATT&CK : T1566.001

DESCRIPTION :
L'analyse des pièces jointes en temps réel détecte les malwares et les documents malveillants avant leur ouverture par les utilisateurs, utilisant des techniques de sandboxing.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Sécurité > Protection contre les programmes malveillants
- Test avec des fichiers de test EICAR
- Analyse des logs de détection

REMÉDIATION :
1. Activer l'analyse en temps réel des pièces jointes
2. Configurer la mise en quarantaine automatique
3. Bloquer les types de fichiers à haut risque

VALEUR PAR DÉFAUT :
Analyse de base activée

3.2.3 *Protection des liens malveillants*

MITRE ATT&CK : T1566.002

DESCRIPTION :
La réécriture et l'analyse des liens en temps réel protègent contre les sites web malveillants et les tentatives de redirection vers des pages de phishing.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Sécurité > Protection des liens
- Test avec des liens malveillants connus
- Vérification de la réécriture des URL

REMÉDIATION :
1. Activer la réécriture de tous les liens
2. Configurer l'analyse en temps réel au clic
3. Bloquer l'accès aux sites de réputation douteuse

VALEUR PAR DÉFAUT :
Protection de base des liens

3.2.4 *Quarantaine administrative*

MITRE ATT&CK : T1566

DESCRIPTION :
La quarantaine administrative permet de retenir les messages suspects pour analyse manuelle avant livraison, offrant un contrôle granulaire sur les emails potentiellement dangereux.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Conformité > Quarantaine administrative
- Interface de gestion de la quarantaine
- Statistiques des messages en quarantaine

REMÉDIATION :
1. Configurer des règles de quarantaine pour messages suspects
2. Définir des reviewers autorisés
3. Établir des SLA de review (ex: 2h max)

VALEUR PAR DÉFAUT :
Quarantaine manuelle uniquement

3.3.1 *Règles DLP pour emails sensibles*

MITRE ATT&CK : T1041

DESCRIPTION :
Les règles de prévention des fuites de données (DLP) détectent et bloquent l'envoi d'informations sensibles par email, protégeant la confidentialité et la conformité réglementaire.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Conformité > Prévention contre la perte de données
- Test avec des données sensibles fictives
- Analyse des violations DLP détectées

REMÉDIATION :
1. Configurer des règles pour numéros de cartes bancaires, SSN
2. Détecter les documents confidentiels en pièce jointe
3. Bloquer ou alerter selon le niveau de sensibilité

VALEUR PAR DÉFAUT :
Aucune règle DLP configurée

3.3.2 *Chiffrement des emails sensibles*

MITRE ATT&CK : T1041

DESCRIPTION :
Le chiffrement automatique des emails contenant des données sensibles garantit la confidentialité en transit et au repos, même si les messages sont interceptés.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Conformité > Chiffrement des emails
- Test d'envoi d'emails avec données sensibles
- Vérification du chiffrement côté destinataire

REMÉDIATION :
1. Activer le chiffrement automatique pour données réglementées
2. Configurer S/MIME pour les emails externes
3. Utiliser le mode confidentiel Gmail pour données très sensibles

VALEUR PAR DÉFAUT :
Chiffrement TLS uniquement

3.3.3 *Mode confidentiel Gmail*

MITRE ATT&CK : T1041

DESCRIPTION :
Le mode confidentiel permet de contrôler l'accès aux emails sensibles avec expiration, restriction de copie/impression et authentification du destinataire.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Paramètres utilisateur > Mode confidentiel
- Test d'envoi en mode confidentiel
- Vérification des contrôles d'accès

REMÉDIATION :
1. Activer le mode confidentiel pour tous les utilisateurs
2. Former les utilisateurs à son utilisation appropriée
3. Configurer des modèles pour emails récurrents sensibles

VALEUR PAR DÉFAUT :
Mode confidentiel disponible mais optionnel

3.3.4 *Étiquetage automatique des emails*

MITRE ATT&CK : T1041

DESCRIPTION :
L'étiquetage automatique classifie les emails selon leur niveau de sensibilité, facilitant l'application de politiques de sécurité appropriées et la traçabilité.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Conformité > Classification des contenus
- Vérification des étiquettes appliquées automatiquement
- Statistiques de classification

REMÉDIATION :
1. Configurer des règles de classification par contenu
2. Utiliser des étiquettes visuelles claires (Confidentiel, Public, etc.)
3. Intégrer avec les politiques DLP

VALEUR PAR DÉFAUT :
Aucun étiquetage automatique

3.4.1 *Restrictions de transfert externe*

MITRE ATT&CK : T1041

DESCRIPTION :
Les restrictions de transfert limitent l'envoi d'emails vers des domaines externes spécifiques, réduisant les risques de fuite de données accidentelle ou malveillante.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Conformité > Règles de routage
- Test d'envoi vers domaines bloqués/autorisés
- Logs des emails bloqués

REMÉDIATION :
1. Créer une liste blanche de domaines partenaires autorisés
2. Bloquer l'envoi vers des domaines de messagerie gratuite
3. Configurer des alertes pour tentatives de contournement

VALEUR PAR DÉFAUT :
Aucune restriction de transfert

3.4.2 *Validation des destinataires externes*

MITRE ATT&CK : T1041

DESCRIPTION :
La validation des destinataires externes avertit les utilisateurs lors de l'envoi vers des adresses externes et peut exiger une confirmation pour les emails sensibles.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Conformité > Avertissements externes
- Test d'envoi d'emails vers destinataires externes
- Configuration des messages d'avertissement

REMÉDIATION :
1. Activer les avertissements pour tous les destinataires externes
2. Exiger une double confirmation pour emails avec pièces jointes
3. Personnaliser les messages d'avertissement

VALEUR PAR DÉFAUT :
Aucun avertissement configuré

3.4.3 *Archivage et rétention des emails*

MITRE ATT&CK : T1005

DESCRIPTION :
Les politiques d'archivage et de rétention garantissent la conservation appropriée des emails pour la conformité réglementaire et la récupération en cas de litige.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Paramètres utilisateur > Rétention des emails
- Google Vault > Règles de rétention
- Vérification de l'application des politiques

REMÉDIATION :
1. Définir des périodes de rétention selon le type d'email
2. Configurer l'archivage automatique dans Vault
3. Documenter les politiques de conservation

VALEUR PAR DÉFAUT :
Conservation illimitée dans Gmail

3.5.1 *Journalisation des emails*

MITRE ATT&CK : T1005

DESCRIPTION :

La journalisation capture automatiquement tous les emails entrants et sortants pour audit, investigation et conformité réglementaire.

AUDIT :

- Console Admin > Applications > Google Workspace > Gmail > Conformité > Journalisation des emails
- Vérification des emails journalisés
- Configuration du compte de réception des journaux

REMÉDIATION :

1. Activer la journalisation pour tous les emails
2. Configurer un compte dédié sécurisé pour les journaux
3. Définir les règles de rétention des journaux

VALEUR PAR DÉFAUT :

Journalisation désactivée

3.5.2 *Monitoring des patterns d'emails suspects*

MITRE ATT&CK : T1566

DESCRIPTION :

L'analyse des patterns d'emails (volume anormal, destinataires inhabituels, horaires suspects) permet de détecter les compromissions de comptes et les attaques internes.

AUDIT :

- Console Admin > Rapports > Gmail > Activité Gmail
- Google Cloud Security Command Center (si configuré)
- Analyse des logs d'audit Gmail

REMÉDIATION :

1. Configurer des seuils d'alerte pour volumes anormaux
2. Détecter les envois en masse inhabituels
3. Analyser les patterns temporels suspects

VALEUR PAR DÉFAUT :

Aucun monitoring automatique des patterns

3.5.3 *Alertes de sécurité Gmail*

MITRE ATT&CK : T1566

DESCRIPTION :

Les alertes de sécurité Gmail notifient proactivement les administrateurs des événements de sécurité critiques liés à la messagerie électronique.

AUDIT :

- Console Admin > Centre d'alertes > Gmail
- Configuration des notifications par email
- Test des alertes avec des événements simulés

REMÉDIATION :

1. Configurer des alertes pour détection de phishing
2. Activer les notifications de malware détecté
3. Définir les destinataires appropriés pour chaque type d'alerte

VALEUR PAR DÉFAUT :

Alertes de base configurées

3.6.1 *Signature email obligatoire*

MITRE ATT&CK : T1566.001

DESCRIPTION :

Les signatures email standardisées renforcent l'identité de l'expéditeur et peuvent inclure des éléments de sécurité comme des disclaimers légaux.

AUDIT :

- Console Admin > Applications > Google Workspace > Gmail > Paramètres utilisateur > Signatures email
- Vérification de l'application automatique des signatures
- Contrôle de la conformité des signatures

REMÉDIATION :

1. Créer des modèles de signature standardisés
2. Forcer l'application automatique des signatures
3. Inclure des disclaimers de confidentialité

VALEUR PAR DÉFAUT :

Signatures optionnelles et manuelles

3.6.2 *Désactivation du transfert automatique externe*

MITRE ATT&CK : T1114.003

DESCRIPTION :
Le transfert automatique vers des adresses externes peut entraîner des fuites de données massives. Cette fonctionnalité doit être strictement contrôlée ou désactivée.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Paramètres utilisateur > Transfert d'emails
- Audit des règles de transfert configurées par les utilisateurs
- gam print users delegate

REMÉDIATION :
1. Désactiver le transfert automatique vers adresses externes
2. Auditer les règles de transfert existantes
3. Configurer des alertes pour nouvelles règles de transfert

VALEUR PAR DÉFAUT :
Transfert automatique autorisé

3.6.3 *Contrôle des délégations de boîtes mail*

MITRE ATT&CK : T1114.002

DESCRIPTION :
Les délégations permettent à d'autres utilisateurs d'accéder à une boîte mail. Ces permissions doivent être contrôlées et auditées régulièrement.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Paramètres utilisateur > Délégation
- gam print users delegate
- Audit périodique des délégations actives

REMÉDIATION :
1. Limiter les délégations au strict nécessaire
2. Exiger une approbation managériale pour les délégations
3. Réviser trimestriellement toutes les délégations

VALEUR PAR DÉFAUT :
Délégations autorisées sans restriction

3.7.1 *Configuration S/MIME pour chiffrement email*

MITRE ATT&CK : T1041

DESCRIPTION :
S/MIME fournit un chiffrement de bout en bout et une signature numérique pour les emails les plus sensibles, offrant une protection cryptographique forte.

AUDIT :
- Console Admin > Applications > Google Workspace > Gmail > Conformité > S/MIME
- Vérification de l'installation des certificats utilisateur
- Test d'envoi d'emails chiffrés S/MIME

REMÉDIATION :
1. Déployer des certificats S/MIME pour utilisateurs sensibles
2. Configurer les politiques de chiffrement automatique
3. Former les utilisateurs à l'usage de S/MIME

VALEUR PAR DÉFAUT :
S/MIME non configuré

4.0 — GOOGLE DRIVE & PARTAGE

4.1.1 *Restrictions de partage externe*

MITRE ATT&CK : T1567.002

DESCRIPTION :
Le partage externe non contrôlé représente un risque majeur de fuite de données. Les restrictions doivent être configurées selon les besoins métier tout en maintenant la sécurité.

AUDIT :
- Console Admin > Applications > Google Workspace > Drive et Docs > Paramètres de partage
- Test de partage avec utilisateurs externes
- Audit des fichiers partagés externement

REMÉDIATION :
1. Restreindre le partage aux domaines approuvés uniquement
2. Désactiver le partage public par liens
3. Exiger une approbation pour le partage sensible

VALEUR PAR DÉFAUT :
Partage externe autorisé par défaut

4.1.2 *Contrôle des liens de partage*

MITRE ATT&CK : T1567.002

DESCRIPTION :
Les liens de partage permettent un accès facile mais peuvent être interceptés ou partagés involontairement. Leur contrôle est essentiel pour la sécurité des données.

AUDIT :
- Console Admin > Applications > Google Workspace > Drive et Docs > Paramètres de partage > Options de lien
- Analyse des liens publics existants
- Test de création de liens avec différents paramètres

REMÉDIATION :
1. Désactiver les liens publics 'Accessible à tous sur le web'
2. Exiger une authentification pour les liens partagés
3. Configurer l'expiration automatique des liens

VALEUR PAR DÉFAUT :
Tous types de liens autorisés

4.1.3 *Permissions par défaut restrictives*

MITRE ATT&CK : T1567.002

DESCRIPTION :
Les permissions par défaut doivent suivre le principe du moindre privilège, en accordant uniquement les accès minimaux nécessaires et en évitant les permissions d'édition par défaut.

AUDIT :
- Console Admin > Applications > Google Workspace > Drive et Docs > Paramètres de partage > Permissions par défaut
- Test de création de nouveaux documents
- Analyse des permissions couramment accordées

REMÉDIATION :
1. Configurer 'Lecteur' comme permission par défaut
2. Désactiver le partage automatique avec l'organisation
3. Exiger une action explicite pour accorder l'édition

VALEUR PAR DÉFAUT :
Permissions variables selon le contexte

4.1.4 *Avertissements de partage externe*

MITRE ATT&CK : T1567.002

DESCRIPTION :

Les avertissements sensibilisent les utilisateurs aux risques du partage externe et peuvent prévenir les fuites accidentelles de données sensibles.

AUDIT :

- Console Admin > Applications > Google Workspace > Drive et Docs > Paramètres de partage > Avertissements
- Test de partage avec utilisateurs externes
- Configuration des messages d'avertissement

REMÉDIATION :

1. Activer les avertissements pour tout partage externe
2. Personnaliser les messages selon le niveau de sensibilité
3. Exiger une confirmation explicite pour documents confidentiels

VALEUR PAR DÉFAUT :

Avertissements limités ou désactivés

4.2.1 *Classification et étiquetage des fichiers*

MITRE ATT&CK : T1005

DESCRIPTION :

La classification automatique des fichiers selon leur contenu permet d'appliquer des politiques de sécurité appropriées et de faciliter la gouvernance des données.

AUDIT :

- Console Admin > Applications > Google Workspace > Drive et Docs > Conformité > Classification des contenus
- Vérification des étiquettes appliquées automatiquement
- Test avec différents types de documents

REMÉDIATION :

1. Configurer des règles de classification par contenu
2. Utiliser des étiquettes visuelles standardisées
3. Intégrer avec les politiques DLP

VALEUR PAR DÉFAUT :

Aucune classification automatique

4.2.2 *Règles DLP pour Google Drive*

MITRE ATT&CK : T1567.002

DESCRIPTION :

Les règles DLP détectent et protègent les données sensibles stockées dans Drive, empêchant leur partage non autorisé ou leur fuite accidentelle.

AUDIT :

- Console Admin > Applications > Google Workspace > Drive et Docs > Conformité > Prévention contre la perte de données
- Test avec documents contenant des données sensibles
- Analyse des violations DLP détectées

REMÉDIATION :

1. Configurer des règles pour données personnelles (PII)
2. Détecter les documents financiers sensibles
3. Bloquer le partage externe de documents classifiés

VALEUR PAR DÉFAUT :

Aucune règle DLP configurée

4.2.3 *Chiffrement côté client (CSE)*

MITRE ATT&CK : T1005

DESCRIPTION :

Le chiffrement côté client offre une protection maximale en chiffrant les données avec des clés contrôlées par l'organisation avant leur stockage dans Drive.

AUDIT :

- Console Admin > Sécurité > Contrôle d'accès et des données > Chiffrement côté client
- Vérification de la configuration des fournisseurs de clés
- Test de création de fichiers chiffrés CSE

REMÉDIATION :

1. Configurer un service de gestion des clés externe
2. Activer CSE pour les unités organisationnelles sensibles
3. Former les utilisateurs à l'usage des fichiers chiffrés

VALEUR PAR DÉFAUT :

CSE non configuré

4.2.4 *Contrôle des téléchargements*

MITRE ATT&CK : T1567.002

DESCRIPTION :

La restriction des téléchargements limite les risques de fuite de données en empêchant l'extraction non contrôlée de documents sensibles.

AUDIT :

- Console Admin > Applications > Google Workspace > Drive et Docs > Paramètres de partage > Options de téléchargement
- Test de téléchargement avec différents types d'utilisateurs
- Vérification des restrictions par type de fichier

REMÉDIATION :

1. Désactiver les téléchargements pour documents très sensibles
2. Limiter les téléchargements aux utilisateurs internes
3. Configurer des alertes pour téléchargements en masse

VALEUR PAR DÉFAUT :

Téléchargements autorisés par défaut

4.3.1 *Gestion des drives partagés*

MITRE ATT&CK : T1074.002

DESCRIPTION :

Les drives partagés centralisent l'accès aux documents d'équipe mais nécessitent une gouvernance stricte pour maintenir la sécurité et éviter l'accumulation de données.

AUDIT :

- Console Admin > Applications > Google Workspace > Drive et Docs > Drives partagés
- Audit des drives partagés existants
- Analyse des permissions et de l'utilisation

REMÉDIATION :

1. Limiter la création de drives partagés aux managers
2. Définir des responsables pour chaque drive partagé
3. Auditer trimestriellement l'utilisation et les permissions

VALEUR PAR DÉFAUT :

Création libre de drives partagés

4.3.2 *Propriété et transfert des fichiers*

MITRE ATT&CK : T1074.002

DESCRIPTION :

La gestion appropriée de la propriété des fichiers garantit la continuité d'accès lors des départs d'employés et évite la perte de documents critiques.

AUDIT :

- Console Admin > Rapports > Applications > Drive > Propriété des fichiers
- Outils de transfert de données
- Identification des fichiers orphelins

REMÉDIATION :

1. Configurer le transfert automatique lors des départs
2. Identifier et réattribuer les fichiers orphelins
3. Encourager l'utilisation des drives partagés pour documents d'équipe

VALEUR PAR DÉFAUT :

Propriété individuelle des fichiers

4.3.3 *Quota et gestion de l'espace de stockage*

MITRE ATT&CK : T1074.002

DESCRIPTION :

La gestion des quotas évite l'accumulation excessive de données et peut limiter l'impact des attaques de déni de service par saturation de stockage.

AUDIT :

- Console Admin > Rapports > Applications > Drive > Utilisation du stockage
- Surveillance des quotas par utilisateur/unité organisationnelle
- Alertes de dépassement de quota

REMÉDIATION :

1. Définir des quotas appropriés par type d'utilisateur
2. Configurer des alertes avant dépassement
3. Nettoyer périodiquement les fichiers anciens

VALEUR PAR DÉFAUT :

Quotas selon le type de licence

4.4.1 *Restrictions d'installation d'add-ons*

MITRE ATT&CK : T1505.003

DESCRIPTION :

Les add-ons tiers peuvent introduire des vulnérabilités ou des fonctionnalités malveillantes. Leur installation doit être contrôlée et auditée.

AUDIT :

- Console Admin > Applications > Google Workspace > Drive et Docs > Applications et extensions
- Inventaire des add-ons installés
- Analyse des permissions accordées aux add-ons

REMÉDIATION :

1. Limiter l'installation aux add-ons approuvés
2. Auditer régulièrement les add-ons installés
3. Révoquer les add-ons non utilisés ou suspects

VALEUR PAR DÉFAUT :

Installation libre d'add-ons

4.4.2 *Contrôle des applications tierces*

MITRE ATT&CK : T1005

DESCRIPTION :

Les applications tierces connectées à Drive peuvent accéder aux données organisationnelles. Leurs permissions doivent être strictement contrôlées et régulièrement auditées.

AUDIT :

- Console Admin > Sécurité > Contrôles API > Applications connectées
- Audit des permissions accordées aux applications
- Analyse de l'utilisation des API Drive

REMÉDIATION :

1. Créer une liste blanche d'applications approuvées
2. Limiter les permissions accordées au strict nécessaire
3. Auditer mensuellement les accès des applications tierces

VALEUR PAR DÉFAUT :

Connexion libre des applications tierces

4.5.1 *Historique et versions des fichiers*

MITRE ATT&CK : T1005

DESCRIPTION :

L'historique des versions permet la récupération en cas de modification malveillante ou accidentelle, mais peut aussi conserver des données sensibles supprimées.

AUDIT :

- Console Admin > Applications > Google Workspace > Drive et Docs > Paramètres utilisateur > Historique des révisions
- Test de récupération de versions antérieures
- Politique de rétention des versions

REMÉDIATION :

1. Configurer une rétention limitée des versions (ex: 30 jours)
2. Former les utilisateurs à la gestion des versions
3. Purger régulièrement les versions anciennes de documents sensibles

VALEUR PAR DÉFAUT :

Rétention illimitée des versions

4.5.2 *Audit des activités de fichiers*

MITRE ATT&CK : T1005

DESCRIPTION :

L'audit des activités Drive permet de détecter les accès suspects, les modifications non autorisées et les téléchargements en masse de données.

AUDIT :

- Console Admin > Rapports > Rapports d'audit > Drive
- API: GET https://admin.googleapis.com/admin/reports/v1/activity/users/all/applications/drive
- gam report drive start -7d

REMÉDIATION :

1. Activer l'audit détaillé de toutes les actions Drive
2. Configurer des alertes pour activités suspectes
3. Analyser régulièrement les patterns d'accès anormaux

VALEUR PAR DÉFAUT :

Audit de base activé

4.5.3 *Détection d'accès anormaux*

MITRE ATT&CK : T1005

DESCRIPTION :
La détection d'accès anormaux (géolocalisation, horaires, volume) aide à identifier les compromissions de comptes et les fuites de données potentielles.

AUDIT :
- Console Admin > Centre d'alertes > Drive
- Configuration des seuils d'alerte
- Analyse des patterns d'accès utilisateurs

REMÉDIATION :
1. Configurer des alertes pour accès depuis nouvelles géolocalisations
2. Détecter les téléchargements de volume anormal
3. Alerter pour accès en dehors des heures habituelles

VALEUR PAR DÉFAUT :
Détection limitée d'anomalies

4.6.1 *Synchronisation Desktop sécurisée*

MITRE ATT&CK : T1005

DESCRIPTION :
La synchronisation Drive Desktop peut exposer les données organisationnelles sur les postes de travail. Elle doit être sécurisée et contrôlée.

AUDIT :
- Console Admin > Applications > Google Workspace > Drive et Docs > Paramètres utilisateur > Drive pour ordinateur
- Inventaire des appareils synchronisant Drive
- Contrôle des données synchronisées

REMÉDIATION :
1. Limiter la synchronisation aux appareils gérés
2. Chiffrer localement les données synchronisées
3. Configurer la suppression automatique lors du départ

VALEUR PAR DÉFAUT :
Drive Desktop autorisé sans restriction

4.6.2 *Contrôle des appareils mobiles*

MITRE ATT&CK : T1005

DESCRIPTION :
L'accès Drive depuis les appareils mobiles non gérés peut exposer les données. Des politiques strictes doivent être appliquées pour sécuriser l'accès mobile.

AUDIT :
- Console Admin > Appareils > Appareils mobiles > Paramètres Drive
- Politique d'accès par type d'appareil
- Audit des connexions mobiles

REMÉDIATION :
1. Exiger l'enregistrement MDM pour accès Drive mobile
2. Limiter les fonctionnalités sur appareils non gérés
3. Configurer la suppression à distance en cas de perte

VALEUR PAR DÉFAUT :
Accès mobile libre depuis tous appareils

4.7.1 *Backup et récupération des données Drive*

MITRE ATT&CK : T1485

DESCRIPTION :
Bien que Google assure la redondance des données, un backup indépendant peut être nécessaire pour la conformité et la protection contre les suppressions malveillantes.

AUDIT :
- Évaluation de la stratégie de backup organisationnelle
- Test de récupération de données supprimées
- Documentation des procédures de récupération

REMÉDIATION :
1. Évaluer le besoin de backup tiers selon les exigences
2. Configurer Google Vault pour la rétention légale
3. Tester régulièrement les procédures de récupération

VALEUR PAR DÉFAUT :
Redondance Google sans backup externe

5.0 — GOOGLE MEET & COMMUNICATION

5.1.1 *Restrictions d'accès aux réunions*

MITRE ATT&CK : T1200

DESCRIPTION :

Les réunions non protégées peuvent être infiltrées par des personnes malveillantes. Les contrôles d'accès appropriés préviennent le "zoombombing" et protègent les discussions sensibles.

AUDIT :

- Console Admin > Applications > Google Workspace > Google Meet > Paramètres de sécurité
- Test de création de réunions avec différents niveaux d'accès
- Vérification des options de salle d'attente

REMÉDIATION :

1. Activer la salle d'attente par défaut pour toutes les réunions
2. Limiter l'accès aux participants du domaine pour réunions sensibles
3. Désactiver l'entrée libre pour les invités externes

VALEUR PAR DÉFAUT :

Accès libre avec lien de réunion

5.1.2 *Authentification des participants externes*

MITRE ATT&CK : T1200

DESCRIPTION :

L'authentification des participants externes garantit l'identité des invités et empêche les accès non autorisés via des liens interceptés.

AUDIT :

- Console Admin > Applications > Google Workspace > Google Meet > Participants externes
- Test de participation avec comptes externes non authentifiés
- Configuration des exigences d'authentification

REMÉDIATION :

1. Exiger l'authentification Google pour tous les participants externes
2. Configurer l'approbation manuelle pour invités sensibles
3. Désactiver l'accès anonyme pour réunions confidentielles

VALEUR PAR DÉFAUT :

Accès autorisé sans authentification pour externes

5.1.3 *Contrôle des enregistrements*

MITRE ATT&CK : T1005

DESCRIPTION :

Les enregistrements de réunions peuvent contenir des informations sensibles. Leur création et stockage doivent être contrôlés pour éviter les fuites de données.

AUDIT :

- Console Admin > Applications > Google Workspace > Google Meet > Enregistrement
- Vérification des permissions d'enregistrement par unité organisationnelle
- Audit des enregistrements stockés

REMÉDIATION :

1. Limiter l'enregistrement aux organisateurs de réunions
2. Configurer l'expiration automatique des enregistrements
3. Restreindre l'accès aux enregistrements selon la classification

VALEUR PAR DÉFAUT :

Enregistrement autorisé pour tous les participants

5.2.1 *Gestion des participants en cours de réunion*

MITRE ATT&CK : T1200

DESCRIPTION :

Les contrôles en cours de réunion permettent à l'organisateur de gérer les participants et d'éviter les perturbations ou l'écoute non autorisée.

AUDIT :

- Test des fonctionnalités de modération Meet
- Vérification des options de contrôle des participants
- Configuration des permissions par défaut

REMÉDIATION :

1. Activer les contrôles de modération par défaut
2. Permettre uniquement à l'organisateur de partager l'écran initialement
3. Configurer la mise en sourdine automatique à l'entrée

VALEUR PAR DÉFAUT :

Contrôles de base activés

5.3.1 *Intégrations et applications Meet*

MITRE ATT&CK : T1505.003

DESCRIPTION :

Les applications et intégrations tierces dans Meet peuvent introduire des vulnérabilités ou accéder à des données de réunion sensibles.

AUDIT :

- Console Admin > Applications > Google Workspace > Google Meet > Applications et extensions
- Inventaire des intégrations Meet autorisées
- Analyse des permissions accordées

REMÉDIATION :

1. Limiter les intégrations aux applications approuvées
2. Auditer régulièrement les permissions des applications
3. Désactiver les intégrations non utilisées

VALEUR PAR DÉFAUT :

Intégrations tierces autorisées

6.0 — GOOGLE CHAT & SPACES

6.1.1 *Restrictions de chat externe*

MITRE ATT&CK : T1566.003

DESCRIPTION :

Les conversations avec des utilisateurs externes peuvent exposer des informations sensibles ou être utilisées pour des attaques de social engineering.

AUDIT :

- Console Admin > Applications > Google Workspace > Google Chat > Paramètres de chat externe
- Test de communication avec utilisateurs externes
- Analyse des conversations externes existantes

REMÉDIATION :

1. Limiter le chat externe aux domaines approuvés
2. Configurer des avertissements pour conversations externes
3. Désactiver complètement si non nécessaire métier

VALEUR PAR DÉFAUT :

Chat externe autorisé avec avertissements

6.1.2 *Historique et rétention des conversations*

MITRE ATT&CK : T1005

DESCRIPTION :

L'historique des conversations doit être géré selon les politiques de conformité, tout en permettant l'investigation en cas d'incident de sécurité.

AUDIT :

- Console Admin > Applications > Google Workspace > Google Chat > Historique des conversations
- Paramètres de rétention par unité organisationnelle
- Configuration Google Vault pour Chat

REMÉDIATION :

1. Configurer des politiques de rétention appropriées
2. Activer la sauvegarde dans Vault si requis pour conformité
3. Former les utilisateurs sur la confidentialité des chats

VALEUR PAR DÉFAUT :

Historique conservé indéfiniment

6.2.1 *Gestion des espaces collaboratifs*

MITRE ATT&CK : T1074.002

DESCRIPTION :

Les espaces Google Chat centralisent la collaboration d'équipe mais nécessitent une gouvernance pour éviter la prolifération et maintenir la sécurité.

AUDIT :

- Audit des espaces existants dans l'organisation
- Analyse de l'appartenance aux espaces
- Vérification des permissions de création d'espaces

REMÉDIATION :

1. Limiter la création d'espaces aux managers/chefs d'équipe
2. Définir des propriétaires responsables pour chaque espace
3. Auditer trimestriellement l'utilisation des espaces

VALEUR PAR DÉFAUT :

Création libre d'espaces par tous utilisateurs

6.3.1 *Partage de fichiers dans Chat*

MITRE ATT&CK : T1567.002

DESCRIPTION :

Le partage de fichiers via Chat peut contourner les contrôles DLP habituels et doit être aligné avec les politiques de partage Drive.

AUDIT :

- Test de partage de fichiers sensibles via Chat
- Vérification de l'application des règles DLP
- Configuration des restrictions de partage

REMÉDIATION :

1. Aligner les politiques de partage Chat avec Drive
2. Appliquer les règles DLP aux fichiers partagés en chat
3. Sensibiliser les utilisateurs aux risques du partage informel

VALEUR PAR DÉFAUT :

Partage libre de fichiers via Chat

7.0 — GOOGLE CALENDAR

7.1.1 *Restrictions de partage d'agenda*

MITRE ATT&CK : T1005

DESCRIPTION :

Le partage d'agenda peut révéler des informations sensibles sur les activités organisationnelles et les participants aux réunions.

AUDIT :

- Console Admin > Applications > Google Workspace > Google Calendar > Paramètres de partage
- Audit des agendas partagés publiquement
- Test de partage avec utilisateurs externes

REMÉDIATION :

1. Désactiver le partage public d'agendas par défaut
2. Limiter le partage externe aux partenaires approuvés
3. Configurer des niveaux de visibilité granulaires

VALEUR PAR DÉFAUT :

Partage d'agenda autorisé avec restrictions de base

7.1.2 *Visibilité des événements par défaut*

MITRE ATT&CK : T1005

DESCRIPTION :

La visibilité par défaut des événements doit protéger les informations sensibles tout en permettant la coordination d'équipe nécessaire.

AUDIT :

- Configuration des niveaux de visibilité par défaut
- Test de création d'événements avec différents niveaux
- Vérification des permissions de visualisation

REMÉDIATION :

1. Configurer la visibilité 'Privé' par défaut pour événements sensibles
2. Former les utilisateurs sur les niveaux de confidentialité
3. Utiliser des libellés génériques pour événements confidentiels

VALEUR PAR DÉFAUT :

Visibilité selon les paramètres utilisateur

7.2.1 *Gestion des ressources et salles de réunion*

MITRE ATT&CK : T1005

DESCRIPTION :

Les réservations de ressources peuvent révéler des patterns d'activité organisationnels et nécessitent un contrôle d'accès approprié.

AUDIT :

- Console Admin > Annuaire > Ressources de bâtiment et calendrier
- Audit des permissions de réservation
- Configuration des politiques de réservation

REMÉDIATION :

1. Limiter la visibilité des ressources selon les besoins
2. Configurer des approbateurs pour ressources sensibles
3. Masquer les détails des réservations confidentielles

VALEUR PAR DÉFAUT :

Ressources visibles à tous les utilisateurs du domaine

7.3.1 *Invitations et participants externes*

MITRE ATT&CK : T1566.003

DESCRIPTION :

Les invitations à des participants externes peuvent exposer des informations organisationnelles et être utilisées pour des attaques de reconnaissance.

AUDIT :

- Console Admin > Applications > Google Workspace > Google Calendar > Partage avec des utilisateurs externes
- Test d'invitation de participants externes
- Configuration des avertissements

REMÉDIATION :

1. Configurer des avertissements pour invitations externes
2. Limiter les détails visibles aux participants externes
3. Exiger une approbation pour événements très sensibles

VALEUR PAR DÉFAUT :

Invitations externes autorisées avec avertissements de base

7.4.1 *Intégrations Calendar tierces*

MITRE ATT&CK : T1505.003

DESCRIPTION :

Les applications tierces intégrées à Calendar peuvent accéder aux données d'agenda et nécessitent un contrôle strict des permissions.

AUDIT :

- Console Admin > Sécurité > Contrôles API > Applications connectées filtrant Calendar
- Audit des intégrations Calendar autorisées
- Analyse des permissions accordées

REMÉDIATION :

1. Limiter les intégrations aux applications approuvées
2. Auditer régulièrement les accès aux données Calendar
3. Révoquer les intégrations non utilisées

VALEUR PAR DÉFAUT :

Intégrations tierces autorisées selon paramètres API

8.0 — APPAREILS & ENDPOINTS

8.1.1 *Configuration MDM (Mobile Device Management)*

MITRE ATT&CK : T1430

DESCRIPTION :
La gestion des appareils mobiles est essentielle pour contrôler l'accès aux données organisationnelles depuis les smartphones et tablettes. Un MDM bien configuré protège contre les appareils compromis.

AUDIT :
- Console Admin > Appareils > Appareils mobiles > Gestion
- Inventaire des appareils enregistrés
- Test d'enregistrement d'un nouvel appareil

REMÉDIATION :
1. Exiger l'enregistrement MDM pour accès à Workspace
2. Configurer des politiques de sécurité strictes (PIN, chiffrement)
3. Activer la suppression à distance en cas de perte/vol

VALEUR PAR DÉFAUT :
MDM optionnel

8.1.2 *Politiques de sécurité des appareils*

MITRE ATT&CK : T1430

DESCRIPTION :
Les politiques de sécurité appliquées aux appareils mobiles doivent inclure le chiffrement, les mots de passe forts et la protection contre le jailbreak/rooting.

AUDIT :
- Console Admin > Appareils > Appareils mobiles > Paramètres d'appareil
- Vérification de l'application des politiques
- Test de conformité sur différents types d'appareils

REMÉDIATION :
1. Exiger un code PIN/mot de passe complexe (6+ caractères)
2. Activer le chiffrement complet de l'appareil
3. Bloquer les appareils jailbreakés/rootés

VALEUR PAR DÉFAUT :
Politiques de base selon le système d'exploitation

8.1.3 *Gestion des applications mobiles*

MITRE ATT&CK : T1426

DESCRIPTION :
Le contrôle des applications installées sur les appareils gérés prévient l'installation de malwares et d'applications non autorisées pouvant compromettre la sécurité.

AUDIT :
- Console Admin > Appareils > Appareils mobiles > Applications approuvées
- Liste blanche/noire d'applications
- Monitoring des applications installées

REMÉDIATION :
1. Créer une liste blanche d'applications autorisées
2. Bloquer l'installation depuis des sources inconnues
3. Surveiller et alerter pour applications suspectes

VALEUR PAR DÉFAUT :
Installation libre d'applications

8.1.4 *Séparation des données professionnelles/personnelles*

MITRE ATT&CK : T1430

DESCRIPTION :

La conteneurisation sépare les données professionnelles des données personnelles, permettant la suppression sélective sans affecter les données personnelles de l'utilisateur.

AUDIT :

- Configuration des profils de travail Android/iOS
- Test de séparation des données
- Vérification de la suppression sélective

REMÉDIATION :

1. Activer les profils de travail pour BYOD
2. Configurer la séparation stricte des applications/données
3. Tester la suppression sélective des données professionnelles

VALEUR PAR DÉFAUT :

Pas de séparation configurée par défaut

8.2.1 *Politique BYOD (Bring Your Own Device)*

MITRE ATT&CK : T1430

DESCRIPTION :

Les politiques BYOD équilibrent flexibilité utilisateur et sécurité organisationnelle. Elles doivent être clairement définies et techniquement appliquées.

AUDIT :

- Documentation des politiques BYOD
- Configuration technique des restrictions BYOD
- Formation des utilisateurs sur les politiques

REMÉDIATION :

1. Documenter clairement les exigences BYOD
2. Implémenter techniquement les restrictions nécessaires
3. Former régulièrement les utilisateurs sur les bonnes pratiques

VALEUR PAR DÉFAUT :

BYOD autorisé sans restrictions particulières

8.2.2 *Contrôle d'accès par type d'appareil*

MITRE ATT&CK : T1430

DESCRIPTION :

Différents types d'appareils (gérés vs non-gérés) doivent avoir des niveaux d'accès différenciés selon leur niveau de sécurité et de conformité.

AUDIT :

- Console Admin > Sécurité > Context-aware access > Niveaux d'accès
- Configuration des politiques par type d'appareil
- Test d'accès avec appareils de différents types

REMÉDIATION :

1. Créer des niveaux d'accès selon le type d'appareil
2. Limiter l'accès aux données sensibles pour appareils non-gérés
3. Exiger des contrôles additionnels pour appareils personnels

VALEUR PAR DÉFAUT :

Accès uniforme tous types d'appareils

8.3.1 *Gestion des certificats d'appareils*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Les certificats d'appareil permettent une identification forte des endpoints et doivent être gérés de manière sécurisée avec rotation régulière.

AUDIT :

- Console Admin > Appareils > Certificats
- Inventaire des certificats déployés
- Vérification des dates d'expiration

REMÉDIATION :

1. Déployer des certificats d'appareil pour identification
2. Configurer la rotation automatique avant expiration
3. Révoquer immédiatement les certificats des appareils perdus

VALEUR PAR DÉFAUT :

Pas de gestion centralisée des certificats

8.4.1 *Endpoint Detection and Response (EDR)*

MITRE ATT&CK : T1057

DESCRIPTION :

L'intégration avec des solutions EDR permet la détection avancée de menaces sur les endpoints accédant à Google Workspace.

AUDIT :

- Intégration avec solutions EDR tierces
- Monitoring des activités suspectes sur endpoints
- Corrélation avec les événements Workspace

REMÉDIATION :

1. Déployer une solution EDR sur tous les endpoints
2. Intégrer les alertes EDR avec le SIEM organisationnel
3. Configurer des réponses automatiques aux menaces détectées

VALEUR PAR DÉFAUT :

Aucune intégration EDR native

9.0 — APPLICATIONS TIERCES & OAUTH

9.1.1 *Liste blanche d'applications OAuth*

MITRE ATT&CK : T1528

DESCRIPTION :
Les applications OAuth non contrôlées peuvent accéder massivement aux données organisationnelles. Une liste blanche stricte est essentielle pour maintenir la sécurité.

AUDIT :
- Console Admin > Sécurité > Contrôles API > Applications OAuth tierces
- Inventaire des applications autorisées
- Audit des permissions accordées

REMÉDIATION :
1. Créer une liste blanche d'applications approuvées uniquement
2. Bloquer toutes les autres applications OAuth par défaut
3. Processus d'approbation formel pour nouvelles applications

VALEUR PAR DÉFAUT :
Applications OAuth autorisées par défaut

9.1.2 *Révision des scopes OAuth accordés*

MITRE ATT&CK : T1528

DESCRIPTION :
Les scopes OAuth définissent les permissions accordées aux applications. Ils doivent être limités au strict nécessaire selon le principe du moindre privilège.

AUDIT :
- Analyse détaillée des scopes accordés par application
- Vérification de l'utilisation effective des permissions
- Audit des scopes sensibles (lecture/écriture Drive, Gmail, etc.)

REMÉDIATION :
1. Auditer trimestriellement tous les scopes accordés
2. Révoquer les permissions non utilisées ou excessives
3. Exiger une justification métier pour scopes sensibles

VALEUR PAR DÉFAUT :
Scopes accordés selon demande application

9.1.3 *Monitoring de l'activité des applications OAuth*

MITRE ATT&CK : T1528

DESCRIPTION :
Le monitoring continu des applications OAuth permet de détecter les utilisations anormales ou malveillantes des permissions accordées.

AUDIT :
- Console Admin > Rapports > Applications OAuth
- Analyse de l'activité API par application
- Détection d'utilisations suspectes

REMÉDIATION :
1. Configurer des alertes pour usage API anormal
2. Surveiller les applications accédant à de gros volumes de données
3. Corréler l'activité avec les événements de sécurité

VALEUR PAR DÉFAUT :
Monitoring limité de l'activité OAuth

9.2.1 *Restrictions d'accès au Marketplace*

MITRE ATT&CK : T1505.003

DESCRIPTION :

Le Google Workspace Marketplace propose de nombreuses applications dont certaines peuvent introduire des vulnérabilités ou accéder à des données sensibles.

AUDIT :

- Console Admin > Applications > Marketplace apps
- Configuration des restrictions d'installation
- Inventaire des apps installées depuis le Marketplace

REMÉDIATION :

1. Limiter l'installation aux administrateurs uniquement
2. Évaluer la sécurité avant installation d'applications Marketplace
3. Auditer régulièrement les applications installées

VALEUR PAR DÉFAUT :

Installation libre depuis le Marketplace

9.2.2 *Gestion des add-ons et extensions*

MITRE ATT&CK : T1505.003

DESCRIPTION :

Les add-ons pour Gmail, Drive, Docs peuvent étendre les fonctionnalités mais aussi introduire des risques de sécurité s'ils ne sont pas contrôlés.

AUDIT :

- Console Admin > Applications > Google Workspace > Drive et Docs > Applications et extensions
- Inventaire des add-ons installés par les utilisateurs
- Analyse des permissions des add-ons

REMÉDIATION :

1. Créer une liste d'add-ons approuvés
2. Bloquer l'installation d'add-ons non autorisés
3. Auditer mensuellement les add-ons installés

VALEUR PAR DÉFAUT :

Installation libre d'add-ons

9.3.1 *Contrôle de l'accès API par IP*

MITRE ATT&CK : T1071.001

DESCRIPTION :

La restriction de l'accès API par plages IP limite l'exposition et peut prévenir l'utilisation malveillante d'API keys compromises.

AUDIT :

- Console Admin > Sécurité > Contrôles API > Restrictions d'accès
- Configuration des plages IP autorisées
- Test d'accès API depuis différentes localisations

REMÉDIATION :

1. Définir les plages IP légitimes pour accès API
2. Bloquer l'accès depuis IP non autorisées
3. Configurer des alertes pour tentatives d'accès suspects

VALEUR PAR DÉFAUT :

Accès API autorisé depuis toutes IP

9.3.2 *Rotation des clés API et secrets*

MITRE ATT&CK : T1552.001

DESCRIPTION :

La rotation régulière des clés API et secrets limite l'impact d'une éventuelle compromission et constitue une bonne pratique sécuritaire.

AUDIT :

- Inventaire de toutes les clés API actives
- Vérification des dates de dernière rotation
- Processus documenté de rotation

REMÉDIATION :

1. Rotation automatique tous les 90 jours maximum
2. Processus de révocation immédiate en cas de compromission
3. Audit trimestriel de l'utilisation des clés

VALEUR PAR DÉFAUT :

Pas de rotation automatique configurée

10.0 — RÈGLES DLP & PROTECTION DONNÉES

10.1.1 *Classification automatique des données*

MITRE ATT&CK : T1005

DESCRIPTION :
La classification automatique identifie les données sensibles (PII, données financières, IP) pour appliquer les protections appropriées selon leur niveau de sensibilité.

AUDIT :
- Console Admin > Applications > Google Workspace > Drive et Docs > Conformité > Classification des contenus
- Test avec différents types de documents sensibles
- Vérification de l'application des étiquettes

REMÉDIATION :
1. Configurer des règles pour PII (numéros SS, cartes bancaires)
2. Détecter la propriété intellectuelle et documents financiers
3. Appliquer automatiquement les étiquettes de classification

VALEUR PAR DÉFAUT :
Aucune classification automatique configurée

10.1.2 *Règles DLP multi-services*

MITRE ATT&CK : T1041

DESCRIPTION :
Les règles DLP doivent être cohérentes à travers tous les services Workspace (Gmail, Drive, Chat) pour une protection uniforme des données sensibles.

AUDIT :
- Configuration DLP dans Gmail, Drive, Chat
- Test de cohérence des règles entre services
- Analyse des violations DLP par service

REMÉDIATION :
1. Harmoniser les règles DLP entre tous les services
2. Configurer des actions cohérentes (blocage, alerte, chiffrement)
3. Centraliser la gestion des politiques DLP

VALEUR PAR DÉFAUT :
Configuration DLP séparée par service

10.1.3 *Détection par reconnaissance optique (OCR)*

MITRE ATT&CK : T1005

DESCRIPTION :
L'OCR détecte les données sensibles dans les images et documents scannés, étendant la protection DLP au-delà du texte simple.

AUDIT :
- Console Admin > Règles DLP > Détection de contenu > OCR
- Test avec images contenant du texte sensible
- Vérification de la détection dans différents formats

REMÉDIATION :
1. Activer l'OCR pour toutes les règles DLP critiques
2. Tester avec différents formats d'images et PDF
3. Configurer des seuils de confiance appropriés

VALEUR PAR DÉFAUT :
OCR désactivé par défaut

10.2.1 *Actions automatisées sur violation DLP*

MITRE ATT&CK : T1041

DESCRIPTION :
Les actions automatisées (blocage, chiffrement, alerte) en réponse aux violations DLP permettent une protection en temps réel sans intervention manuelle.

AUDIT :
- Configuration des actions par type de violation
- Test du déclenchement automatique des actions
- Monitoring de l'efficacité des actions automatisées

REMÉDIATION :
1. Bloquer automatiquement les violations critiques
2. Chiffrer automatiquement les contenus sensibles
3. Alerter immédiatement les administrateurs sécurité

VALEUR PAR DÉFAUT :
Actions manuelles ou alertes uniquement

10.2.2 *Exceptions et surcharges DLP*

MITRE ATT&CK : T1041

DESCRIPTION :
Les exceptions DLP doivent être strictement contrôlées et auditées pour éviter les contournements non autorisés des protections.

AUDIT :
- Inventaire de toutes les exceptions DLP configurées
- Processus d'approbation des exceptions
- Audit régulier de l'utilisation des exceptions

REMÉDIATION :
1. Limiter les exceptions au strict minimum nécessaire
2. Exiger une approbation managériale pour toute exception
3. Réviser trimestriellement toutes les exceptions actives

VALEUR PAR DÉFAUT :
Pas de processus formel pour exceptions

10.3.1 *Intégration avec systèmes de classification externes*

MITRE ATT&CK : T1005

DESCRIPTION :
L'intégration avec des systèmes de classification d'entreprise (Microsoft Purview, etc.) permet une gouvernance uniforme des données.

AUDIT :
- Configuration des connecteurs de classification externes
- Test de synchronisation des étiquettes
- Vérification de la cohérence inter-systèmes

REMÉDIATION :
1. Configurer l'intégration avec le système de classification principal
2. Synchroniser les étiquettes et politiques
3. Maintenir la cohérence des classifications

VALEUR PAR DÉFAUT :
Aucune intégration externe configurée

10.4.1 *Monitoring et reporting DLP*

MITRE ATT&CK : T1041

DESCRIPTION :
Le monitoring continu et le reporting des violations DLP permettent l'amélioration continue des politiques et la détection de tentatives de contournement.

AUDIT :
- Console Admin > Rapports > Rapports de sécurité > DLP
- Configuration des alertes automatiques
- Tableaux de bord de violations DLP

REMÉDIATION :
1. Configurer des tableaux de bord temps réel
2. Alertes automatiques pour violations répétées
3. Rapports hebdomadaires de synthèse DLP

VALEUR PAR DÉFAUT :
Rapports de base disponibles

11.0 — VAULT & RÉTENTION

11.1.1 *Politiques de rétention par type de données*

MITRE ATT&CK : T1005

DESCRIPTION :
Les politiques de rétention doivent être différenciées selon le type de données et les exigences réglementaires, équilibrant conformité et performance.

AUDIT :
- Google Vault > Rétention > Règles de rétention
- Configuration par unité organisationnelle
- Test d'application des politiques

REMÉDIATION :
1. Définir des périodes selon les exigences légales
2. Séparer les politiques par type de contenu (email, drive, chat)
3. Documenter la justification de chaque période

VALEUR PAR DÉFAUT :
Rétention illimitée pour la plupart des services

11.1.2 *Configuration des holds légales*

MITRE ATT&CK : T1005

DESCRIPTION :
Les holds légales préservent les données pertinentes lors de litiges ou investigations, suspendant temporairement les politiques de rétention normales.

AUDIT :
- Google Vault > Holds > Gestion des conservations
- Test de création et application d'un hold
- Vérification de l'immunité aux suppressions

REMÉDIATION :
1. Documenter les procédures de création de holds
2. Former les équipes juridiques à l'utilisation de Vault
3. Auditer régulièrement les holds actifs

VALEUR PAR DÉFAUT :
Aucun hold configuré par défaut

11.1.3 *Recherche et export eDiscovery*

MITRE ATT&CK : T1005

DESCRIPTION :
Les fonctionnalités de recherche et d'export permettent de répondre aux demandes légales et investigations internes de manière efficace et sécurisée.

AUDIT :
- Google Vault > Recherche > Création de requêtes
- Test d'export de résultats
- Vérification des permissions d'accès

REMÉDIATION :
1. Former les équipes autorisées aux techniques de recherche
2. Configurer des templates de recherche pour cas récurrents
3. Auditer tous les exports effectués

VALEUR PAR DÉFAUT :
Fonctionnalités disponibles pour administrateurs Vault

11.2.1 *Accès et permissions Vault*

MITRE ATT&CK : T1005

DESCRIPTION :

L'accès à Vault doit être strictement contrôlé car il permet l'accès à toutes les données organisationnelles, incluant celles des dirigeants.

AUDIT :

- Google Vault > Paramètres > Privilèges Vault
- Audit des utilisateurs ayant accès à Vault
- Vérification des permissions granulaires

REMÉDIATION :

1. Limiter l'accès Vault aux équipes juridiques et conformité
2. Utiliser des permissions granulaires (lecture seule vs export)
3. Auditer mensuellement tous les accès Vault

VALEUR PAR DÉFAUT :

Accès Vault pour super-administrateurs uniquement

11.2.2 *Audit des activités Vault*

MITRE ATT&CK : T1005

DESCRIPTION :

Toutes les activités dans Vault doivent être loggées et auditées pour maintenir la traçabilité et détecter les abus potentiels.

AUDIT :

- Google Vault > Audit > Journal des activités
- Configuration des alertes pour actions sensibles
- Révision régulière des logs d'activité

REMÉDIATION :

1. Activer l'audit complet de toutes les actions Vault
2. Configurer des alertes pour exports volumineux
3. Réviser mensuellement les activités de recherche/export

VALEUR PAR DÉFAUT :

Audit de base des activités Vault

11.3.1 *Intégration avec systèmes d'archivage tiers*

MITRE ATT&CK : T1005

DESCRIPTION :

L'intégration avec des systèmes d'archivage d'entreprise peut être nécessaire pour la conformité et la gouvernance uniforme des données.

AUDIT :

- Configuration des exports automatiques vers systèmes tiers
- Vérification de l'intégrité des données archivées
- Test de récupération depuis archives externes

REMÉDIATION :

1. Évaluer les besoins d'archivage externe
2. Configurer les exports automatiques si requis
3. Tester régulièrement la récupération des archives

VALEUR PAR DÉFAUT :

Aucune intégration tierce configurée

12.0 — SÉCURITÉ DU DOMAINE

12.1.1 *Vérification de tous les domaines*

MITRE ATT&CK : T1590.001

DESCRIPTION :
Tous les domaines associés au tenant Google Workspace doivent être vérifiés pour éviter l'usurpation et garantir le contrôle administratif légitime.

AUDIT :
- Console Admin > Domaines > Gestion des domaines
- Statut de vérification pour chaque domaine
- Vérification des enregistrements TXT de validation

REMÉDIATION :
1. Vérifier immédiatement tous les domaines non vérifiés
2. Maintenir les enregistrements de vérification DNS
3. Surveiller l'ajout de nouveaux domaines non autorisés

VALEUR PAR DÉFAUT :
Domaine principal vérifié, secondaires peuvent ne pas l'être

12.1.2 *Configuration DMARC stricte pour tous domaines*

MITRE ATT&CK : T1566.001

DESCRIPTION :
DMARC doit être configuré en mode strict (p=reject) pour tous les domaines organisationnels afin d'empêcher l'usurpation d'emails.

AUDIT :
- nslookup -type=TXT _dmarc.domain.com pour chaque domaine
- Analyse des rapports DMARC
- Vérification de l'alignement SPF/DKIM

REMÉDIATION :
1. Configurer DMARC p=reject pour tous les domaines
2. Analyser régulièrement les rapports DMARC
3. Ajuster SPF/DKIM si nécessaire pour maintenir l'alignement

VALEUR PAR DÉFAUT :
DMARC non configuré pour domaines secondaires

12.1.3 *Protection des enregistrements DNS critiques*

MITRE ATT&CK : T1584.002

DESCRIPTION :
Les enregistrements DNS critiques (SPF, DKIM, DMARC, vérification domaine) doivent être protégés contre les modifications non autorisées.

AUDIT :
- Configuration DNSSEC pour les domaines
- Contrôles d'accès sur la gestion DNS
- Monitoring des changements DNS

REMÉDIATION :
1. Activer DNSSEC pour tous les domaines critiques
2. Limiter l'accès à la gestion DNS aux administrateurs autorisés
3. Configurer des alertes pour modifications DNS

VALEUR PAR DÉFAUT :
Protection DNS selon le registrar/hébergeur

12.2.1 *Alias de domaines sécurisés*

MITRE ATT&CK : T1566.001

DESCRIPTION :
Les alias de domaines doivent être gérés de manière cohérente avec les mêmes protections que le domaine principal.

AUDIT :
- Console Admin > Domaines > Alias de domaine
- Vérification de la configuration email pour alias
- Cohérence des politiques entre domaine principal et alias

REMÉDIATION :
1. Appliquer les mêmes politiques sécuritaires aux alias
2. Configurer SPF/DKIM/DMARC pour tous les alias
3. Limiter le nombre d'alias au strict nécessaire

VALEUR PAR DÉFAUT :
Alias créés sans configuration sécuritaire automatique

12.2.2 *Sous-domaines et délégations*

MITRE ATT&CK : T1584.001

DESCRIPTION :

Les sous-domaines et délégations DNS doivent être inventoriés et sécurisés pour éviter qu'ils deviennent des vecteurs d'attaque.

AUDIT :

- Inventaire complet des sous-domaines
- Vérification des délégations DNS autorisées
- Scan de sécurité des sous-domaines

REMÉDIATION :

1. Maintenir un inventaire à jour de tous les sous-domaines
2. Sécuriser ou supprimer les sous-domaines non utilisés
3. Appliquer les mêmes standards de sécurité aux sous-domaines

VALEUR PAR DÉFAUT :

Sous-domaines créés sans gouvernance centralisée

12.3.1 *Certificats SSL/TLS pour domaines*

MITRE ATT&CK : T1553.002

DESCRIPTION :

Les certificats SSL/TLS doivent être correctement configurés et maintenus pour tous les domaines et services exposés.

AUDIT :

- Vérification des certificats SSL pour tous les domaines
- Contrôle des dates d'expiration
- Validation de la chaîne de certification

REMÉDIATION :

1. Utiliser des certificats SSL valides pour tous les domaines
2. Configurer le renouvellement automatique
3. Surveiller les expirations et vulnérabilités SSL

VALEUR PAR DÉFAUT :

Certificats Google pour services Workspace, configuration manuelle pour autres services

13.0 — JOURNALISATION & AUDIT

13.1.1 *Audit des connexions administrateurs*

MITRE ATT&CK : T1078.004

DESCRIPTION :
Toutes les connexions et activités des comptes administrateurs doivent être loggées et monitorées pour détecter les compromissions et abus de privilèges.

AUDIT :
- Console Admin > Rapports > Rapports d'audit > Connexion administrateur
- Configuration des alertes pour connexions suspectes
- Rétention des logs administrateur

REMÉDIATION :
1. Activer l'audit complet des connexions admin
2. Configurer des alertes pour connexions géographiquement anormales
3. Réviser hebdomadairement les connexions administrateurs

VALEUR PAR DÉFAUT :
Audit de base des connexions activé

13.1.2 *Journalisation des modifications de configuration*

MITRE ATT&CK : T1098

DESCRIPTION :
Tous les changements de configuration administrative doivent être tracés pour maintenir la traçabilité et faciliter les investigations.

AUDIT :
- Console Admin > Rapports > Rapports d'audit > Admin
- API: GET https://admin.googleapis.com/admin/reports/v1/activity/users/all/applications/admin
- gam report admin start -30d filter='*_CHANGE'

REMÉDIATION :
1. Activer l'audit de toutes les modifications de configuration
2. Configurer des alertes pour changements critiques
3. Corréler les changements avec les tickets de changement

VALEUR PAR DÉFAUT :
Audit des modifications admin activé

13.1.3 *Monitoring des créations/suppressions de comptes*

MITRE ATT&CK : T1136

DESCRIPTION :
La création et suppression de comptes utilisateurs doit être étroitement surveillée car ces actions peuvent indiquer des compromissions ou des erreurs critiques.

AUDIT :
- Console Admin > Rapports > Rapports d'audit > Admin > Gestion des comptes
- Alertes configurées pour créations/suppressions
- Corrélation avec les processus HR

REMÉDIATION :
1. Alerter immédiatement pour toute création/suppression de compte
2. Corréler avec les processus RH et de provisionnement
3. Investiguer toute action non planifiée

VALEUR PAR DÉFAUT :
Logs disponibles sans alertes automatiques

13.2.1 *Audit des activités utilisateurs sensibles*

MITRE ATT&CK : T1005

DESCRIPTION :

Les activités utilisateurs sur les données sensibles (accès, téléchargement, partage) doivent être auditées pour détecter les comportements anormaux.

AUDIT :

- Console Admin > Rapports > Rapports d'audit > Drive > Téléchargements
- Configuration d'alertes pour volumes anormaux
- Analyse des patterns d'accès

REMÉDIATION :

1. Auditer les téléchargements de gros volumes
2. Surveiller les accès aux documents très sensibles
3. Alerter pour activités en dehors des heures normales

VALEUR PAR DÉFAUT :

Audit de base des activités utilisateurs

13.2.2 *Logs de sécurité centralisés*

MITRE ATT&CK : T1562.002

DESCRIPTION :

Les logs de sécurité doivent être centralisés dans un SIEM ou une solution de monitoring pour analyse et corrélation avec d'autres sources.

AUDIT :

- Configuration d'export vers SIEM/log management
- API: Utilisation de l'Admin SDK pour export automatique
- Vérification de l'intégrité des logs exportés

REMÉDIATION :

1. Configurer l'export automatique vers le SIEM organisationnel
2. Maintenir l'intégrité et la complétude des logs
3. Configurer des alertes corrélées multi-sources

VALEUR PAR DÉFAUT :

Logs disponibles uniquement dans la console Workspace

13.2.3 *Rétention et archivage des logs*

MITRE ATT&CK : T1562.002

DESCRIPTION :

Les logs d'audit doivent être conservés selon les exigences réglementaires et de sécurité, avec une protection contre la modification.

AUDIT :

- Durée de rétention des logs par type
- Protection contre la modification des logs
- Procédures d'archivage long terme

REMÉDIATION :

1. Définir des périodes de rétention selon les exigences légales
2. Exporter et archiver les logs pour conservation long terme
3. Protéger l'intégrité des logs archivés

VALEUR PAR DÉFAUT :

Rétention 6 mois pour la plupart des logs

13.3.1 *Configuration du Centre d'alertes*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Le Centre d'alertes Google doit être configuré pour notifier proactivement les administrateurs des événements de sécurité critiques.

AUDIT :

- Console Admin > Centre d'alertes > Configuration
- Test des notifications par email/SMS
- Personnalisation des seuils d'alerte

REMÉDIATION :

1. Configurer toutes les alertes de sécurité disponibles
2. Définir les destinataires appropriés par type d'alerte
3. Tester régulièrement les mécanismes de notification

VALEUR PAR DÉFAUT :

Alertes de base configurées pour super-admins

13.3.2 *Alertes personnalisées via API*

MITRE ATT&CK : T1562.001

DESCRIPTION :

L'API d'alertes permet de créer des règles personnalisées et d'intégrer les alertes Google Workspace dans les systèmes de monitoring existants.

AUDIT :

- Configuration d'alertes via Admin SDK
- Intégration avec systèmes de ticketing
- API: GET https://admin.googleapis.com/admin/alertcenter/v1beta1/alerts

REMÉDIATION :

1. Créer des alertes personnalisées selon les besoins organisationnels
2. Intégrer avec le système de ticketing/ITSM
3. Automatiser les réponses aux alertes de routine

VALEUR PAR DÉFAUT :

Alertes standard uniquement, pas d'intégration API

13.4.1 *Monitoring de la performance et disponibilité*

MITRE ATT&CK : T1498

DESCRIPTION :

Le monitoring de la performance aide à détecter les attaques de déni de service et les anomalies d'utilisation pouvant indiquer des compromissions.

AUDIT :

- Console Admin > Rapports > Rapports d'utilisation
- Surveillance des pics d'utilisation anormaux
- Alertes pour dégradations de performance

REMÉDIATION :

1. Établir des baselines de performance normale
2. Configurer des alertes pour déviations significatives
3. Corréler les anomalies avec les événements de sécurité

VALEUR PAR DÉFAUT :

Rapports d'utilisation disponibles sans monitoring automatique

14.0 — GROUPES GOOGLE

14.1.1 *Contrôle de création des groupes*

MITRE ATT&CK : T1069.003

DESCRIPTION :
La création libre de groupes peut entraîner une prolifération incontrôlée et des risques de sécurité. Les permissions de création doivent être limitées.

AUDIT :
- Console Admin > Annuaire > Groupes > Paramètres de groupe
- Permissions de création par unité organisationnelle
- Audit des groupes créés récemment

REMÉDIATION :
1. Limiter la création aux managers et administrateurs
2. Exiger une justification métier pour nouveaux groupes
3. Réviser trimestriellement les groupes créés

VALEUR PAR DÉFAUT :
Création libre de groupes par tous utilisateurs

14.1.2 *Gestion des membres externes dans groupes*

MITRE ATT&CK : T1069.003

DESCRIPTION :
Les membres externes dans les groupes peuvent accéder à des informations sensibles partagées avec le groupe. Leur inclusion doit être strictement contrôlée.

AUDIT :
- Console Admin > Annuaire > Groupes > Paramètres membres externes
- Audit des groupes avec membres externes
- gam print groups members | grep -v '@domain.com'

REMÉDIATION :
1. Désactiver l'ajout de membres externes par défaut
2. Exiger une approbation administrative pour membres externes
3. Auditer mensuellement tous les groupes avec membres externes

VALEUR PAR DÉFAUT :
Membres externes autorisés avec approbation

14.1.3 *Permissions de publication dans groupes*

MITRE ATT&CK : T1566.003

DESCRIPTION :
Les permissions de publication déterminent qui peut envoyer des emails au groupe. Des permissions trop ouvertes peuvent permettre le spam ou le phishing.

AUDIT :
- Console Admin > Annuaire > Groupes > [Groupe] > Paramètres de publication
- Audit des groupes avec publication ouverte
- Test d'envoi depuis comptes non autorisés

REMÉDIATION :
1. Limiter la publication aux membres du groupe uniquement
2. Configurer la modération pour groupes sensibles
3. Désactiver la publication externe non modérée

VALEUR PAR DÉFAUT :
Publication limitée aux membres par défaut

14.2.1 *Archivage et historique des groupes*

MITRE ATT&CK : T1005

DESCRIPTION :
L'historique des discussions de groupe doit être géré selon les politiques de rétention et les exigences de conformité.

AUDIT :
- Paramètres d'archivage par groupe
- Configuration Vault pour groupes Google
- Politiques de rétention des messages de groupe

REMÉDIATION :
1. Configurer l'archivage selon les exigences légales
2. Appliquer les politiques de rétention appropriées
3. Former les utilisateurs sur la confidentialité des groupes

VALEUR PAR DÉFAUT :
Archivage selon paramètres individuels de groupe

14.3.1 *Groupes de sécurité vs groupes de distribution*

MITRE ATT&CK : T1069.003

DESCRIPTION :

La distinction entre groupes de sécurité et de distribution doit être claire, avec des usages et gouvernances différenciés.

AUDIT :

- Classification des groupes par usage
- Permissions différenciées selon le type
- Documentation des rôles de chaque groupe

REMÉDIATION :

1. Classifier tous les groupes selon leur usage
2. Appliquer des politiques distinctes par type
3. Documenter clairement le rôle de chaque groupe

VALEUR PAR DÉFAUT :

Pas de distinction formelle entre types de groupes

15.0 — CHROME ENTERPRISE & NAVIGATEUR

15.1.1 *Politiques de sécurité Chrome*

MITRE ATT&CK : T1185

DESCRIPTION :
Les politiques Chrome Enterprise permettent de sécuriser les navigateurs gérés et de contrôler l'accès aux ressources web depuis les appareils d'entreprise.

AUDIT :
- Console Admin > Appareils > Chrome > Paramètres utilisateur
- Configuration des politiques de sécurité navigateur
- Test d'application des politiques sur navigateurs gérés

REMÉDIATION :
1. Configurer Safe Browsing en mode renforcé
2. Bloquer les téléchargements de types de fichiers dangereux
3. Activer la protection contre les sites malveillants

VALEUR PAR DÉFAUT :
Politiques de sécurité de base selon Chrome standard

15.1.2 *Gestion des extensions Chrome*

MITRE ATT&CK : T1505.003

DESCRIPTION :
Les extensions Chrome peuvent introduire des vulnérabilités ou accéder à des données sensibles. Leur installation doit être contrôlée via des listes blanches.

AUDIT :
- Console Admin > Appareils > Chrome > Applications et extensions
- Liste des extensions autorisées/bloquées
- Audit des extensions installées par les utilisateurs

REMÉDIATION :
1. Créer une liste blanche d'extensions approuvées
2. Bloquer l'installation d'extensions non autorisées
3. Auditer régulièrement les extensions installées

VALEUR PAR DÉFAUT :
Installation libre d'extensions depuis Chrome Web Store

15.1.3 *Contrôle de l'accès aux sites web*

MITRE ATT&CK : T1071.001

DESCRIPTION :
Le filtrage web via Chrome Enterprise peut bloquer l'accès aux sites malveillants, de productivité douteuse ou non conformes aux politiques organisationnelles.

AUDIT :
- Console Admin > Appareils > Chrome > Paramètres utilisateur > Filtrage d'URL
- Configuration des listes blanches/noires de sites
- Test d'accès à différentes catégories de sites

REMÉDIATION :
1. Configurer le filtrage par catégories (malware, phishing, adult)
2. Créer des listes de sites bloqués/autorisés spécifiques
3. Permettre des demandes de déblocage justifiées

VALEUR PAR DÉFAUT :
Pas de filtrage web configuré par défaut

15.2.1 *Synchronisation Chrome sécurisée*

MITRE ATT&CK : T1005

DESCRIPTION :

La synchronisation Chrome doit être contrôlée pour éviter la fuite de données via l'historique, mots de passe ou favoris synchronisés sur appareils non gérés.

AUDIT :

- Console Admin > Appareils > Chrome > Paramètres utilisateur > Synchronisation
- Configuration des éléments synchronisés
- Restriction de synchronisation sur appareils non gérés

REMÉDIATION :

1. Limiter la synchronisation aux appareils gérés uniquement
2. Désactiver la synchronisation des mots de passe si non nécessaire
3. Contrôler la synchronisation de l'historique de navigation

VALEUR PAR DÉFAUT :

Synchronisation autorisée pour comptes Workspace

15.3.1 *Rapports d'utilisation Chrome*

MITRE ATT&CK : T1071.001

DESCRIPTION :

Les rapports Chrome Enterprise fournissent une visibilité sur l'utilisation des navigateurs et peuvent aider à détecter les comportements anormaux.

AUDIT :

- Console Admin > Rapports > Chrome > Navigateur
- Analyse des sites les plus visités
- Détection d'activités de navigation suspectes

REMÉDIATION :

1. Configurer des rapports réguliers d'utilisation Chrome
2. Analyser les patterns de navigation pour détecter les anomalies
3. Corréler avec les événements de sécurité

VALEUR PAR DÉFAUT :

Rapports de base disponibles selon configuration

16.0 — GOOGLE CLOUD IDENTITY

16.1.1 *Context-Aware Access avancé*

MITRE ATT&CK : T1078

DESCRIPTION :
Context-Aware Access utilise des signaux contextuels (appareil, localisation, réseau) pour prendre des décisions d'accès granulaires sans friction utilisateur.

AUDIT :
- Google Cloud Console > Identity & Access Management > Context-Aware Access
- Configuration des niveaux d'accès
- Test avec différents contextes d'accès

REMÉDIATION :
1. Définir des niveaux d'accès selon le contexte de risque
2. Configurer des politiques pour appareils non gérés
3. Implémenter progressivement par populations d'utilisateurs

VALEUR PAR DÉFAUT :
Context-Aware Access non configuré

16.1.2 *BeyondCorp Enterprise*

MITRE ATT&CK : T1078

DESCRIPTION :
BeyondCorp implémente un modèle de sécurité zero-trust, évaluant chaque requête d'accès indépendamment du réseau d'origine.

AUDIT :
- Google Cloud Console > BeyondCorp Enterprise
- Configuration des politiques d'accès zero-trust
- Intégration avec les ressources internes

REMÉDIATION :
1. Évaluer les besoins de déploiement BeyondCorp
2. Configurer l'accès conditionnel aux ressources sensibles
3. Migrer progressivement du modèle périmétrique vers zero-trust

VALEUR PAR DÉFAUT :
BeyondCorp non configuré par défaut

16.2.1 *Intégration LDAP/Active Directory*

MITRE ATT&CK : T1078.002

DESCRIPTION :
La synchronisation avec Active Directory ou LDAP doit être sécurisée pour maintenir la cohérence des identités sans exposer les infrastructures internes.

AUDIT :
- Google Cloud Directory Sync (GCDS) configuration
- Sécurité des communications LDAP/AD
- Audit des comptes synchronisés

REMÉDIATION :
1. Utiliser LDAPS (LDAP over SSL) pour la synchronisation
2. Limiter les permissions du compte de service GCDS
3. Auditer régulièrement la synchronisation et les erreurs

VALEUR PAR DÉFAUT :
Synchronisation manuelle ou non configurée

16.3.1 *Gestion des identités privilégiées*

MITRE ATT&CK : T1078.004

DESCRIPTION :

Les identités privilégiées nécessitent des protections renforcées incluant MFA obligatoire, accès temporaire et audit strict.

AUDIT :

- Inventaire de tous les comptes privilégiés
- Configuration MFA obligatoire pour comptes privilégiés
- Audit des activités des comptes privilégiés

REMÉDIATION :

1. Identifier et inventorier tous les comptes privilégiés
2. Appliquer MFA renforcé (clés FIDO obligatoires)
3. Implémenter l'accès privilégié temporaire (JIT)

VALEUR PAR DÉFAUT :

Gestion manuelle des privilèges

17.0 — RÉPONSE AUX INCIDENTS

17.1.1 *Procédures d'investigation*

MITRE ATT&CK : T1005

DESCRIPTION :

Des procédures d'investigation documentées permettent une réponse rapide et efficace aux incidents de sécurité, préservant les preuves et limitant l'impact.

AUDIT :

- Documentation des procédures d'investigation
- Formation des équipes de réponse aux incidents
- Outils d'investigation configurés (Vault, logs, etc.)

REMÉDIATION :

1. Documenter les procédures step-by-step d'investigation
2. Former les équipes IT/sécurité aux outils Google
3. Tester régulièrement les procédures avec des simulations

VALEUR PAR DÉFAUT :

Pas de procédures formalisées d'investigation

17.1.2 *Outils de réponse automatisée*

MITRE ATT&CK : T1562.001

DESCRIPTION :

L'automatisation de certaines réponses (suspension de comptes, révocation de sessions) permet une réaction rapide aux incidents critiques.

AUDIT :

- Configuration d'alertes automatiques
- Scripts de réponse automatisée via Admin SDK
- Intégration avec systèmes SOAR/SIEM

REMÉDIATION :

1. Configurer la suspension automatique pour comportements à risque
2. Développer des scripts de réponse via API Admin SDK
3. Intégrer avec les outils SOAR organisationnels

VALEUR PAR DÉFAUT :

Réponse manuelle uniquement aux incidents

17.2.1 *Récupération de comptes compromis*

MITRE ATT&CK : T1078

DESCRIPTION :

Les procédures de récupération de comptes compromis doivent permettre une restauration sécurisée sans laisser de backdoors aux attaquants.

AUDIT :

- Procédures documentées de récupération de comptes
- Test de la récupération avec comptes de test
- Formation des équipes support

REMÉDIATION :

1. Documenter les étapes de récupération sécurisée
2. Inclure la révocation de toutes les sessions et tokens
3. Former le support IT aux procédures de récupération

VALEUR PAR DÉFAUT :

Procédures de récupération basiques

17.3.1 *Communication de crise*

MITRE ATT&CK : T1566

DESCRIPTION :

Les plans de communication de crise définissent comment informer les utilisateurs et parties prenantes lors d'incidents de sécurité majeurs.

AUDIT :

- Plans de communication documentés
- Canaux de communication d'urgence configurés
- Templates de messages prêts à utiliser

REMÉDIATION :

1. Documenter les plans de communication par type d'incident
2. Préparer des templates de messages pour différents scenarii
3. Tester les canaux de communication d'urgence

VALEUR PAR DÉFAUT :

Communication ad-hoc lors d'incidents

18.0 — CONFORMITÉ & GOUVERNANCE

18.1.1 *Localisation des données*

MITRE ATT&CK : T1005

DESCRIPTION :
Le contrôle de la localisation des données peut être requis pour certaines réglementations (RGPD, souveraineté numérique).

AUDIT :
- Console Admin > Données > Localisation des données
- Vérification des régions de stockage configurées
- Compliance avec exigences réglementaires locales

REMÉDIATION :
1. Configurer les régions de stockage selon les exigences
2. Valider la conformité avec les réglementations applicables
3. Documenter la stratégie de localisation des données

VALEUR PAR DÉFAUT :
Stockage dans les datacenters Google globaux

18.1.2 *Transparence de l'accès*

MITRE ATT&CK : T1078.003

DESCRIPTION :
Access Transparency fournit des logs détaillés des accès Google aux données clients pour maintenance et support.

AUDIT :
- Console Admin > Sécurité > Access Transparency
- Configuration des notifications d'accès Google
- Analyse des logs de transparence

REMÉDIATION :
1. Activer Access Transparency si disponible dans l'édition
2. Configurer les alertes pour accès Google aux données
3. Réviser régulièrement les logs de transparence

VALEUR PAR DÉFAUT :
Access Transparency selon édition Workspace

18.2.1 *Certifications de conformité*

MITRE ATT&CK : N/A

DESCRIPTION :
La validation des certifications Google Workspace pertinentes (SOC2, ISO27001, etc.) assure l'alignement avec les standards de sécurité organisationnels.

AUDIT :
- Documentation des certifications Google applicables
- Mapping avec les exigences organisationnelles
- Validation périodique du maintien des certifications

REMÉDIATION :
1. Identifier les certifications requises par l'organisation
2. Valider la couverture par les certifications Google
3. Maintenir une veille sur les certifications Google

VALEUR PAR DÉFAUT :
Certifications Google disponibles selon l'édition

18.3.1 *Gouvernance des données*

MITRE ATT&CK : T1005

DESCRIPTION :
Une gouvernance des données structurée définit les responsabilités, processus et contrôles pour la gestion du cycle de vie des données.

AUDIT :
- Documentation de la gouvernance des données
- Rôles et responsabilités définis
- Processus de classification et gestion des données

REMÉDIATION :
1. Documenter la stratégie de gouvernance des données
2. Définir les rôles de Data Owner/Data Steward
3. Implémenter les processus de gestion du cycle de vie

VALEUR PAR DÉFAUT :
Pas de gouvernance formalisée des données

Annexe : Checklist (176 controles)

#	Recommandation	Niveau	Oui	Non	N/A
Section 1 — GESTION DES COMPTES & IDENTITÉS					
1.1.1	Configuration des rôles super-administrateur	●	☐	☐	☐
1.1.2	Authentification multifacteur pour super-administrateurs	●	☐	☐	☐
1.1.3	Comptes de récupération configurés	●	☐	☐	☐
1.1.4	Délégation d'administration limitée	●	☐	☐	☐
1.1.5	Audit des connexions administratives	●	☐	☐	☐
1.2.1	Provisionnement automatique des utilisateurs	●	☐	☐	☐
1.2.2	Désactivation automatique des comptes inactifs	●	☐	☐	☐
1.2.3	Gestion du cycle de vie des comptes	●	☐	☐	☐
1.2.4	Attribution des licences par unité organisationnelle	●	☐	☐	☐
1.3.1	Structure des unités organisationnelles	●	☐	☐	☐
1.3.2	Héritage des politiques par OU	●	☐	☐	☐
1.3.3	Séparation des environnements par OU	●	☐	☐	☐
1.4.1	Politique de mots de passe renforcée	●	☐	☐	☐
1.4.2	Historique et réutilisation des mots de passe	●	☐	☐	☐
1.4.3	Verrouillage de compte après échecs	●	☐	☐	☐
1.5.1	Révision périodique des comptes utilisateurs	●	☐	☐	☐
1.5.2	Audit des attributions de groupes	●	☐	☐	☐
1.5.3	Monitoring des changements de privilèges	●	☐	☐	☐
1.6.1	Comptes de service sécurisés	●	☐	☐	☐
1.6.2	Authentification par clés API sécurisées	●	☐	☐	☐
1.6.3	Monitoring de l'utilisation des comptes de service	●	☐	☐	☐
1.7.1	Processus d'offboarding formalisé	●	☐	☐	☐
1.7.2	Transfert sécurisé des données utilisateur	●	☐	☐	☐
Section 1 — GESTION DES COMPTES & IDENTITÉS					
1.1.1	Configuration des rôles super-administrateur	●	☐	☐	☐
1.1.2	Authentification multifacteur pour super-administrateurs	●	☐	☐	☐
1.1.3	Comptes de récupération configurés	●	☐	☐	☐
1.1.4	Délégation d'administration limitée	●	☐	☐	☐
1.1.5	Audit des connexions administratives	●	☐	☐	☐
1.2.1	Provisionnement automatique des utilisateurs	●	☐	☐	☐
1.2.2	Désactivation automatique des comptes inactifs	●	☐	☐	☐
1.2.3	Gestion du cycle de vie des comptes	●	☐	☐	☐
1.2.4	Attribution des licences par unité organisationnelle	●	☐	☐	☐
1.3.1	Structure des unités organisationnelles	●	☐	☐	☐
1.3.2	Héritage des politiques par OU	●	☐	☐	☐
1.4.1	Politique de mots de passe renforcée	●	☐	☐	☐
1.5.1	Révision périodique des comptes utilisateurs	●	☐	☐	☐
Section 2 — AUTHENTIFICATION & MFA					
2.1.1	Authentification à deux facteurs obligatoire	●	☐	☐	☐
2.1.2	Méthodes MFA autorisées	●	☐	☐	☐
2.1.3	Codes de récupération sécurisés	●	☐	☐	☐
2.1.4	Clés de sécurité pour comptes privilégiés	●	☐	☐	☐
2.1.5	Politique de session et timeout	●	☐	☐	☐
2.2.1	Configuration SSO/SAML sécurisée	●	☐	☐	☐
2.2.2	Fournisseur d'identité de confiance	●	☐	☐	☐
2.2.3	Validation des certificats SAML	●	☐	☐	☐
2.2.4	Mappage des attributs SAML	●	☐	☐	☐
2.2.5	Fallback d'authentification sécurisé	●	☐	☐	☐
2.3.1	Restriction d'accès par géolocalisation	●	☐	☐	☐
2.3.2	Contrôle d'accès par plages IP	●	☐	☐	☐
2.3.3	Context-Aware Access (Accès contextuel)	●	☐	☐	☐
2.3.4	Gestion des appareils de confiance	●	☐	☐	☐
2.4.1	Alertes de connexions suspectes	●	☐	☐	☐
2.4.2	Monitoring des échecs d'authentification	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
2.4.3	Analyse des patterns de connexion	●	☐	☐	☐
2.5.1	Gestion des sessions concurrentes	●	☐	☐	☐
2.5.2	Révocation de sessions à distance	●	☐	☐	☐
2.6.1	Audit des méthodes d'authentification	●	☐	☐	☐
Section 3 — GMAIL — SÉCURITÉ EMAIL					
3.1.1	Configuration SPF (Sender Policy Framework)	●	☐	☐	☐
3.1.2	Configuration DKIM (DomainKeys Identified Mail)	●	☐	☐	☐
3.1.3	Configuration DMARC stricte	●	☐	☐	☐
3.1.4	Authentification BIMI (Brand Indicators for Message Identification)	●	☐	☐	☐
3.2.1	Protection anti-phishing avancée	●	☐	☐	☐
3.2.2	Analyse des pièces jointes malveillantes	●	☐	☐	☐
3.2.3	Protection des liens malveillants	●	☐	☐	☐
3.2.4	Quarantaine administrative	●	☐	☐	☐
3.3.1	Règles DLP pour emails sensibles	●	☐	☐	☐
3.3.2	Chiffrement des emails sensibles	●	☐	☐	☐
3.3.3	Mode confidentiel Gmail	●	☐	☐	☐
3.3.4	Étiquetage automatique des emails	●	☐	☐	☐
3.4.1	Restrictions de transfert externe	●	☐	☐	☐
3.4.2	Validation des destinataires externes	●	☐	☐	☐
3.4.3	Archivage et rétention des emails	●	☐	☐	☐
3.5.1	Journalisation des emails	●	☐	☐	☐
3.5.2	Monitoring des patterns d'emails suspects	●	☐	☐	☐
3.5.3	Alertes de sécurité Gmail	●	☐	☐	☐
3.6.1	Signature email obligatoire	●	☐	☐	☐
3.6.2	Désactivation du transfert automatique externe	●	☐	☐	☐
3.6.3	Contrôle des délégations de boîtes mail	●	☐	☐	☐
3.7.1	Configuration S/MIME pour chiffrement email	●	☐	☐	☐
Section 4 — GOOGLE DRIVE & PARTAGE					
4.1.1	Restrictions de partage externe	●	☐	☐	☐
4.1.2	Contrôle des liens de partage	●	☐	☐	☐
4.1.3	Permissions par défaut restrictives	●	☐	☐	☐
4.1.4	Avertissements de partage externe	●	☐	☐	☐
4.2.1	Classification et étiquetage des fichiers	●	☐	☐	☐
4.2.2	Règles DLP pour Google Drive	●	☐	☐	☐
4.2.3	Chiffrement côté client (CSE)	●	☐	☐	☐
4.2.4	Contrôle des téléchargements	●	☐	☐	☐
4.3.1	Gestion des drives partagés	●	☐	☐	☐
4.3.2	Propriété et transfert des fichiers	●	☐	☐	☐
4.3.3	Quota et gestion de l'espace de stockage	●	☐	☐	☐
4.4.1	Restrictions d'installation d'add-ons	●	☐	☐	☐
4.4.2	Contrôle des applications tierces	●	☐	☐	☐
4.5.1	Historique et versions des fichiers	●	☐	☐	☐
4.5.2	Audit des activités de fichiers	●	☐	☐	☐
4.5.3	Détection d'accès anormaux	●	☐	☐	☐
4.6.1	Synchronisation Desktop sécurisée	●	☐	☐	☐
4.6.2	Contrôle des appareils mobiles	●	☐	☐	☐
4.7.1	Backup et récupération des données Drive	●	☐	☐	☐
Section 5 — GOOGLE MEET & COMMUNICATION					
5.1.1	Restrictions d'accès aux réunions	●	☐	☐	☐
5.1.2	Authentification des participants externes	●	☐	☐	☐
5.1.3	Contrôle des enregistrements	●	☐	☐	☐
5.2.1	Gestion des participants en cours de réunion	●	☐	☐	☐
5.3.1	Intégrations et applications Meet	●	☐	☐	☐
Section 6 — GOOGLE CHAT & SPACES					
6.1.1	Restrictions de chat externe	●	☐	☐	☐
6.1.2	Historique et rétention des conversations	●	☐	☐	☐
6.2.1	Gestion des espaces collaboratifs	●	☐	☐	☐
6.3.1	Partage de fichiers dans Chat	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
Section 7 — GOOGLE CALENDAR					
7.1.1	Restrictions de partage d'agenda	●	☐	☐	☐
7.1.2	Visibilité des événements par défaut	●	☐	☐	☐
7.2.1	Gestion des ressources et salles de réunion	●	☐	☐	☐
7.3.1	Invitations et participants externes	●	☐	☐	☐
7.4.1	Intégrations Calendar tierces	●	☐	☐	☐
Section 8 — APPAREILS & ENDPOINTS					
8.1.1	Configuration MDM (Mobile Device Management)	●	☐	☐	☐
8.1.2	Politiques de sécurité des appareils	●	☐	☐	☐
8.1.3	Gestion des applications mobiles	●	☐	☐	☐
8.1.4	Séparation des données professionnelles/personnelles	●	☐	☐	☐
8.2.1	Politique BYOD (Bring Your Own Device)	●	☐	☐	☐
8.2.2	Contrôle d'accès par type d'appareil	●	☐	☐	☐
8.3.1	Gestion des certificats d'appareils	●	☐	☐	☐
8.4.1	Endpoint Detection and Response (EDR)	●	☐	☐	☐
Section 9 — APPLICATIONS TIERCES & OAUTH					
9.1.1	Liste blanche d'applications OAuth	●	☐	☐	☐
9.1.2	Révision des scopes OAuth accordés	●	☐	☐	☐
9.1.3	Monitoring de l'activité des applications OAuth	●	☐	☐	☐
9.2.1	Restrictions d'accès au Marketplace	●	☐	☐	☐
9.2.2	Gestion des add-ons et extensions	●	☐	☐	☐
9.3.1	Contrôle de l'accès API par IP	●	☐	☐	☐
9.3.2	Rotation des clés API et secrets	●	☐	☐	☐
Section 10 — RÈGLES DLP & PROTECTION DONNÉES					
10.1.1	Classification automatique des données	●	☐	☐	☐
10.1.2	Règles DLP multi-services	●	☐	☐	☐
10.1.3	Détection par reconnaissance optique (OCR)	●	☐	☐	☐
10.2.1	Actions automatisées sur violation DLP	●	☐	☐	☐
10.2.2	Exceptions et surcharges DLP	●	☐	☐	☐
10.3.1	Intégration avec systèmes de classification externes	●	☐	☐	☐
10.4.1	Monitoring et reporting DLP	●	☐	☐	☐
Section 11 — VAULT & RÉTENTION					
11.1.1	Politiques de rétention par type de données	●	☐	☐	☐
11.1.2	Configuration des holds légales	●	☐	☐	☐
11.1.3	Recherche et export eDiscovery	●	☐	☐	☐
11.2.1	Accès et permissions Vault	●	☐	☐	☐
11.2.2	Audit des activités Vault	●	☐	☐	☐
11.3.1	Intégration avec systèmes d'archivage tiers	●	☐	☐	☐
Section 12 — SÉCURITÉ DU DOMAINE					
12.1.1	Vérification de tous les domaines	●	☐	☐	☐
12.1.2	Configuration DMARC stricte pour tous domaines	●	☐	☐	☐
12.1.3	Protection des enregistrements DNS critiques	●	☐	☐	☐
12.2.1	Alias de domaines sécurisés	●	☐	☐	☐
12.2.2	Sous-domaines et délégations	●	☐	☐	☐
12.3.1	Certificats SSL/TLS pour domaines	●	☐	☐	☐
Section 13 — JOURNALISATION & AUDIT					
13.1.1	Audit des connexions administrateurs	●	☐	☐	☐
13.1.2	Journalisation des modifications de configuration	●	☐	☐	☐
13.1.3	Monitoring des créations/suppressions de comptes	●	☐	☐	☐
13.2.1	Audit des activités utilisateurs sensibles	●	☐	☐	☐
13.2.2	Logs de sécurité centralisés	●	☐	☐	☐
13.2.3	Rétention et archivage des logs	●	☐	☐	☐
13.3.1	Configuration du Centre d'alertes	●	☐	☐	☐
13.3.2	Alertes personnalisées via API	●	☐	☐	☐
13.4.1	Monitoring de la performance et disponibilité	●	☐	☐	☐
Section 14 — GROUPES GOOGLE					
14.1.1	Contrôle de création des groupes	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
14.1.2	Gestion des membres externes dans groupes	●	☐	☐	☐
14.1.3	Permissions de publication dans groupes	●	☐	☐	☐
14.2.1	Archivage et historique des groupes	●	☐	☐	☐
14.3.1	Groupes de sécurité vs groupes de distribution	●	☐	☐	☐
Section 15 — CHROME ENTERPRISE & NAVIGATEUR					
15.1.1	Politiques de sécurité Chrome	●	☐	☐	☐
15.1.2	Gestion des extensions Chrome	●	☐	☐	☐
15.1.3	Contrôle de l'accès aux sites web	●	☐	☐	☐
15.2.1	Synchronisation Chrome sécurisée	●	☐	☐	☐
15.3.1	Rapports d'utilisation Chrome	●	☐	☐	☐
Section 16 — GOOGLE CLOUD IDENTITY					
16.1.1	Context-Aware Access avancé	●	☐	☐	☐
16.1.2	BeyondCorp Enterprise	●	☐	☐	☐
16.2.1	Intégration LDAP/Active Directory	●	☐	☐	☐
16.3.1	Gestion des identités privilégiées	●	☐	☐	☐
Section 17 — RÉPONSE AUX INCIDENTS					
17.1.1	Procédures d'investigation	●	☐	☐	☐
17.1.2	Outils de réponse automatisée	●	☐	☐	☐
17.2.1	Récupération de comptes compromis	●	☐	☐	☐
17.3.1	Communication de crise	●	☐	☐	☐
Section 18 — CONFORMITÉ & GOUVERNANCE					
18.1.1	Localisation des données	●	☐	☐	☐
18.1.2	Transparence de l'accès	●	☐	☐	☐
18.2.1	Certifications de conformité	●	☐	☐	☐
18.3.1	Gouvernance des données	●	☐	☐	☐