Checklist Sécurité GOOGLE CHROME ENTERPRISE

Ayi NEDJIMI Consultants
ayinedjimi-consultants.fr
v| — | 2026-04-04 | · 222 controles

Sommaire

Section 1 — MISES À JOUR & VERSIONING

1.1 Gestion des Versions et Canaux de Mise à Jour
1.2 Surveillance et Reporting des Versions
1.3 Gestion du Cycle de Vie des Versions

Section 2 — GESTION DES POLITIQUES GPO/INTUNE

2.1 Configuration et Déploiement des Modèles ADMX
2.2 Stratégies de Groupe et Objets GPO
2.3 Microsoft Intune et Gestion Mobile
2.4 Chrome Browser Cloud Management (CBCM)

Section 3 — NAVIGATION SÉCURISÉE

3.1 Google Safe Browsing et Protection Avancée
3.2 Protection contre les Malwares
3.3 Filtrage et Blocage de Contenu
3.4 Protection Avancée contre les Menaces
3.5 Analyse et Forensique de Navigation

Section 4 — GESTION DES MOTS DE PASSE

4.1 Configuration du Gestionnaire de Mots de Passe Chrome
4.2 Politiques d'Auto-Complétion et de Saisie
4.3 Intégration avec les Gestionnaires d'Entreprise
4.4 Détection et Prévention des Fuites de Credentials

Section 5 — COOKIES & DONNÉES DE NAVIGATION

5.1 Gestion des Cookies Tiers et Tracking
5.2 Protection des Données de Navigation
5.3 Mode Navigation Privée et Incognito

Section 6 — EXTENSIONS & ADD-ONS

6.1 Gestion de l'Installation d'Extensions
6.2 Contrôle des Permissions d'Extensions

Section 7 — CERTIFICATS & TLS

7.0 CERTIFICATS & TLS
7.1 Configuration TLS et Chiffrement

Section 8 — CONFIDENTIALITÉ & TÉLÉMÉTRIE

8.0 CONFIDENTIALITÉ & TÉLÉMÉTRIE
8.1 Contrôle de la Collecte de Données

Section 9 — ISOLATION DES SITES & SANDBOXING

9.0 ISOLATION DES SITES & SANDBOXING
9.1 Configuration de l'Isolation Avancée

Section 10 — TÉLÉCHARGEMENTS & FICHIERS

10.0 TÉLÉCHARGEMENTS & FICHIERS
10.1 Contrôle des Téléchargements

Section 11 — JAVASCRIPT & CONTENU WEB

11.0 JAVASCRIPT & CONTENU WEB
11.1 Contrôle de l'Exécution JavaScript

Section 12 — DNS & RÉSEAU

12.0 DNS & RÉSEAU
12.1 Configuration DNS Sécurisée

Section 13 — AUTHENTIFICATION & IDENTITÉ

13.0 AUTHENTIFICATION & IDENTITÉ
13.1 Intégration SSO et Authentification

Section 14 — MODE KIOSK & RESTRICTIONS

14.0 MODE KIOSK & RESTRICTIONS
14.1 Restrictions d'Utilisation

Section 15 — CHROME ENTERPRISE FEATURES

15.0 CHROME ENTERPRISE FEATURES
15.1 Fonctionnalités Avancées Enterprise

Section 16 — DEVTOOLS & DEBUG

16.0 DEVTOOLS & DEBUG
16.1 Restriction des Outils de Développement

Section 17 — JOURNALISATION & AUDIT

17.0 JOURNALISATION & AUDIT

17.1 Configuration des Logs de Sécurité

Section 18 — CONFORMITÉ & GOUVERNANCE

18.0 CONFORMITÉ & GOUVERNANCE

18.1 Mise en Conformité Réglementaire

Annexe : Checklist

Section 1 — MISES À JOUR & VERSIONING

1.1 — Gestion des Versions et Canaux de Mise à Jour

1.1.1 *Configuration du Canal de Mise à Jour Stable*

MITRE ATT&CK : T1190

DESCRIPTION :

Chrome doit être configuré sur le canal Stable pour recevoir uniquement les mises à jour de sécurité validées. Les canaux Beta, Dev ou Canary exposent à des vulnérabilités non corrigées et ne doivent pas être utilisés en production.

```
# Vérification du canal via registre
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Update" -Name "UpdateDefault" -ErrorAction SilentlyContinue
# Valeur attendue: 1 (Stable)
chrome --version
```

REMÉDIATION :

1. Configurer via GPO : Configuration ordinateur → Modèles administratifs → Google → Google Update → Applications → Google Chrome
2. Définir "Politique de mise à jour par défaut" sur "Mises à jour activées"
3. Registry : `New-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Update" -Name "UpdateDefault" -Value 1 -PropertyType DWord`

VALEUR PAR DÉFAUT :

Canal Stable activé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.1.2 *Activation des Mises à Jour Automatiques*

MITRE ATT&CK : T1190, T1203

DESCRIPTION :

Les mises à jour automatiques de Chrome doivent être activées pour assurer la correction rapide des vulnérabilités de sécurité. Le délai entre la publication et l'installation ne doit pas excéder 7 jours.

```
# Vérification des mises à jour automatiques
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AutoUpdateCheckPeriodMinutes"
# Vérifier chrome://policy
Get-Service "GoogleUpdateService*" | Select-Object Name, Status
```

REMÉDIATION :

1. GPO : Modèles administratifs → Google → Google Chrome → Mises à jour automatiques
2. Activer "Vérification automatique des mises à jour"
3. Registry : `Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AutoUpdateCheckPeriodMinutes" -Value 60`
4. Redémarrer le service Google Update

VALEUR PAR DÉFAUT :

Mises à jour automatiques activées

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.1.3 *Contrôle de Version Minimum Autorisée*

MITRE ATT&CK : T1190

DESCRIPTION :

Définir une version minimum de Chrome autorisée pour empêcher l'utilisation de versions obsolètes contenant des vulnérabilités connues. La version doit être mise à jour mensuellement.

```
# Vérification version minimum
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "MinimumVersionRequired"
# Comparer avec chrome://version
```

REMÉDIATION :

1. Définir via GPO : Google Chrome → "Version minimum requise"
2. Registry : `Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "MinimumVersionRequired" -Value "120.0.6099.0"`
3. Mettre à jour la version mensuelle selon les releases Chrome

VALEUR PAR DÉFAUT :

Aucune restriction de version

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.1.4 *Blocage des Versions de Développement*

MITRE ATT&CK : T1190

DESCRIPTION :

Empêcher l'installation et l'utilisation des versions Beta, Dev, ou Canary de Chrome qui contiennent des fonctionnalités expérimentales et des vulnérabilités non corrigées.

```
# Vérifier absence de versions développement
Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -like "*Chrome*"} | Select-Object Name, Version
Get-ChildItem -Path "C:\Program Files\Google" -Directory | Where-Object {$_.Name -like "*Chrome*"}
```

REMÉDIATION :

1. Utiliser AppLocker pour bloquer les exécutables Chrome non-officiels
2. GPO Software Restriction : Interdire l'exécution depuis les dossiers de développement
3. Supprimer les installations existantes de versions développement

VALEUR PAR DÉFAUT :

Toutes versions autorisées

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.1.5 *Gestion des Rollbacks de Version*

MITRE ATT&CK : T1562

DESCRIPTION :

Contrôler la capacité des utilisateurs à revenir à des versions antérieures de Chrome pour éviter l'utilisation de versions vulnérables après une mise à jour corrective.

```
# Vérifier la politique de rollback
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AllowVersionRollback"
```

REMÉDIATION :

1. GPO : Désactiver "Autoriser le rollback de version"
2. Registry : `Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AllowVersionRollback" -Value 0`

VALEUR PAR DÉFAUT :

Rollback autorisé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.1.6 *Configuration Canary Channel Monitoring pour Early Warning*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Monitoring canal Canary pour détection précoce vulnérabilités

AUDIT :

:

- chrome://policy/ → TargetChannel configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

1.1.7 *Beta Channel Security Testing Integration*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Tests sécurité automatisés sur canal Beta avant déploiement

AUDIT :

:

- chrome://policy/ → TargetChannel configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

1.2 — Surveillance et Reporting des Versions

1.2.1 *Monitoring des Versions Déployées*

MITRE ATT&CK : T1082

DESCRIPTION :

Mettre en place un système de monitoring pour identifier les versions de Chrome déployées dans l'environnement et détecter les installations non-autorisées ou obsolètes.

```
# Script de collecte des versions
Get-WmiObject -Class Win32_Product -ComputerName (Get-ADComputer -Filter *).Name |
Where-Object {$_.Name -eq "Google Chrome"} | Select-Object PSComputerName, Version
```

REMÉDIATION :

1. Déployer un script PowerShell de collecte via GPO
2. Utiliser Chrome Browser Cloud Management pour le reporting
3. Intégrer avec SCCM/Intune pour l'inventaire

VALEUR PAR DÉFAUT :

Pas de monitoring automatique

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.2.2 *Alertes de Sécurité pour Versions Vulnérables*

MITRE ATT&CK : T1190

DESCRIPTION :

Configurer des alertes automatiques lorsque des versions de Chrome vulnérables sont détectées dans l'environnement, basées sur les CVE et bulletins de sécurité Google.

```
# Vérifier configuration des alertes
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SecurityAlertsEnabled"
```

REMÉDIATION :

1. Activer Chrome Enterprise Reporting pour les alertes sécurité
2. Configurer l'intégration SIEM pour les événements Chrome
3. Automatiser les notifications via email/Slack

VALEUR PAR DÉFAUT :

Alertes désactivées

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.2.3 *Reporting de Conformité Version*

MITRE ATT&CK : T1082

DESCRIPTION :

Générer des rapports réguliers de conformité des versions Chrome déployées par rapport aux exigences de sécurité et aux versions supportées.

```
# Générer rapport de conformité
$ChromeVersions = Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -eq "Google Chrome"}
$ChromeVersions | Export-Csv -Path "ChromeVersionReport.csv"
```

REMÉDIATION :

1. Créer des rapports automatisés mensuels
2. Utiliser Power BI ou équivalent pour les dashboards
3. Inclure dans les rapports de conformité sécurité

VALEUR PAR DÉFAUT :

Pas de reporting automatique

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.2.4 *Gestion des Exceptions de Version*

MITRE ATT&CK : T1562

DESCRIPTION :

Établir un processus formel pour les demandes d'exception de version Chrome, incluant évaluation des risques et approbation de la sécurité.

```
# Vérifier les exceptions configurées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "VersionExceptions"
```

REMÉDIATION :

1. Créer un processus de demande d'exception documenté
2. Configurer des groupes AD spécifiques pour les exceptions
3. Limiter la durée de validité des exceptions (max 30 jours)

VALEUR PAR DÉFAUT :

Pas de gestion d'exceptions

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.2.5 *Tests de Régression Post-Mise à Jour*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Mettre en place des tests automatisés pour vérifier que les mises à jour Chrome n'introduisent pas de régressions de sécurité ou de fonctionnalité dans les applications critiques.

```
# Vérifier la configuration des tests automatisés
Test-NetConnection -ComputerName "test-environment" -Port 443
```

REMÉDIATION :

1. Déployer Chrome d'abord sur un groupe pilote
2. Automatiser les tests de fonctionnalité critique
3. Valider les politiques de sécurité après mise à jour

VALEUR PAR DÉFAUT :

Pas de tests automatisés

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.2.6 *Automated CVE Scanning pour Chrome Versions*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Scanning automatisé CVEs avec corrélation versions déployées

AUDIT :

:

- chrome://policy/ → VersionReporting configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

1.2.7 *Zero-Day Vulnerability Early Warning System*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Système alerte précoce vulnérabilités zero-day

AUDIT :

:

- chrome://policy/ → SafeBrowsingExtendedReportingEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

1.3 — Gestion du Cycle de Vie des Versions

1.3.1 *Planification des Déploiements de Version*

MITRE ATT&CK : T1562

DESCRIPTION :

Établir un processus de planification des déploiements de nouvelles versions Chrome avec phases de test, validation et déploiement progressif selon un calendrier défini.

```
# Vérifier la configuration de déploiement graduel
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Update" -Name "RolloutPercent"
```

REMÉDIATION :

1. Définir des groupes de déploiement (pilote, production)
2. Configurer le déploiement graduel via GPO
3. Documenter les fenêtres de maintenance autorisées

VALEUR PAR DÉFAUT :

Déploiement immédiat

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.3.2 *Validation Préalable des Versions*

MITRE ATT&CK : T1190

DESCRIPTION :

Mettre en place un processus de validation des nouvelles versions Chrome sur un environnement de test avant le déploiement en production, incluant tests de sécurité et de compatibilité.

```
# Vérifier l'environnement de test
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "TestEnvironmentEnabled"
```

REMÉDIATION :

1. Créer un environnement de test dédié
2. Automatiser les tests de régression sécurité
3. Valider les applications métier critiques

VALEUR PAR DÉFAUT :

Pas de validation préalable

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.3.3 *Gestion des Versions Critiques d'Urgence*

MITRE ATT&CK : T1190

DESCRIPTION :

Définir une procédure d'urgence pour le déploiement rapide de versions critiques de Chrome corrigeant des vulnérabilités zero-day ou activement exploitées.

```
# Vérifier la configuration de déploiement d'urgence
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Update" -Name "EmergencyUpdateEnabled"
```

REMÉDIATION :

1. Configurer un canal de mise à jour d'urgence
2. Définir les critères de déclenchement d'urgence
3. Établir une procédure de rollback d'urgence

VALEUR PAR DÉFAUT :

Pas de procédure d'urgence

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.3.4 *Documentation des Changements de Version*

MITRE ATT&CK : T1082

DESCRIPTION :

Maintenir une documentation complète des changements de version Chrome incluant impacts sécurité, nouvelles fonctionnalités et modifications de comportement.

```
# Vérifier l'historique des versions déployées
Get-EventLog -LogName Application -Source "Google Chrome" | Select-Object TimeGenerated, Message
```

REMÉDIATION :

1. Créer un registre des changements automatisé
2. Documenter les impacts sur les politiques de sécurité
3. Maintenir un changelog interne des déploiements

VALEUR PAR DÉFAUT :

Pas de documentation automatique

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

1.3.5 *Archivage et Rétention des Versions*

MITRE ATT&CK : T1562

DESCRIPTION :

Établir une politique d'archivage et de rétention des versions Chrome pour permettre le rollback contrôlé et l'analyse forensique en cas d'incident.

```
# Vérifier l'espace de stockage des versions archivées
Get-ChildItem -Path "C:\ChromeVersions" -Directory | Measure-Object
```

REMÉDIATION :

1. Configurer un repository interne des versions Chrome
2. Définir une politique de rétention (ex: 6 mois)
3. Automatiser l'archivage des versions déployées

VALEUR PAR DÉFAUT :

Pas d'archivage automatique

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

Section 2 — GESTION DES POLITIQUES GPO/INTUNE

2.1 — Configuration et Déploiement des Modèles ADMX

2.1.1 *Installation des Modèles ADMX Chrome Enterprise*

MITRE ATT&CK : T1484

DESCRIPTION :

Installer et maintenir les modèles administratifs ADMX officiels de Google Chrome Enterprise pour permettre la gestion centralisée via les stratégies de groupe. Les templates doivent être à jour avec la version Chrome déployée.

```
# Vérifier la présence des templates ADMX Chrome
Test-Path "C:\Windows\PolicyDefinitions\chrome.admx"
Test-Path "C:\Windows\PolicyDefinitions\fr-FR\chrome.adml"
Get-ChildItem "C:\Windows\PolicyDefinitions" | Where-Object {$_.Name -like "*chrome*"}
```

REMÉDIATION :

1. Télécharger les templates ADMX depuis Google Admin Console
2. Copier chrome.admx vers C:\Windows\PolicyDefinitions\
3. Copier chrome.adml vers C:\Windows\PolicyDefinitions\fr-FR\
4. Redémarrer le service de stratégie de groupe

VALEUR PAR DÉFAUT :

Templates non installés

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.1.2 *Validation de la Version des Templates ADMX*

MITRE ATT&CK : T1484

DESCRIPTION :

S'assurer que les templates ADMX utilisés correspondent à la version de Chrome déployée pour éviter les incompatibilités de politiques et les configurations non appliquées.

```
# Extraire la version du template ADMX
Select-String -Path "C:\Windows\PolicyDefinitions\chrome.admx" -Pattern "policyDefinitions.*revision"
# Comparer avec la version Chrome installée
(Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome").DisplayVersion
```

REMÉDIATION :

1. Vérifier la correspondance des versions trimestriellement
2. Mettre à jour les templates avec chaque release majeure Chrome
3. Tester les nouvelles politiques en environnement de test

VALEUR PAR DÉFAUT :

Templates potentiellement obsolètes

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.1.3 *Configuration du Magasin Central ADMX*

MITRE ATT&CK : T1484

DESCRIPTION :

Utiliser un magasin central ADMX pour centraliser la gestion des templates Chrome et assurer la cohérence des politiques sur tous les contrôleurs de domaine.

```
# Vérifier le magasin central ADMX
Test-Path "\\domain.local\SYSVOL\domain.local\Policies\PolicyDefinitions\chrome.admx"
Get-GPO -All | Where-Object {$_.DisplayName -like "*Chrome*"}
```

REMÉDIATION :

1. Créer le dossier PolicyDefinitions dans SYSVOL
2. Copier tous les templates ADMX vers le magasin central
3. Configurer la réplication SYSVOL pour synchroniser les templates

VALEUR PAR DÉFAUT :

Magasin local uniquement

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.1.4 *Gestion des Versions de Templates ADMX*

MITRE ATT&CK : T1484

DESCRIPTION :

Établir un processus de gestion des versions des templates ADMX Chrome incluant archivage, documentation des changements et procédure de rollback.

```
# Vérifier l'historique des versions ADMX
Get-ChildItem "C:\AdminTemplatesArchive\Chrome" | Sort-Object LastWriteTime
```

REMÉDIATION :

1. Créer un repository Git pour les templates ADMX
2. Documenter les changements de politique avec chaque version
3. Tester les nouveaux templates avant déploiement production

VALEUR PAR DÉFAUT :

Pas de gestion de versions

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.1.5 *Validation de l'Intégrité des Templates*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Valider l'intégrité cryptographique des templates ADMX téléchargés pour prévenir l'utilisation de templates modifiés ou compromis.

```
# Vérifier la signature numérique si disponible
Get-AuthenticodeSignature "C:\Windows\PolicyDefinitions\chrome.admx"
# Calculer le hash pour comparaison
Get-FileHash "C:\Windows\PolicyDefinitions\chrome.admx" -Algorithm SHA256
```

REMÉDIATION :

1. Télécharger uniquement depuis les sources officielles Google
2. Vérifier les checksums SHA256 des fichiers
3. Scanner les templates avec l'antivirus avant déploiement

VALEUR PAR DÉFAUT :

Pas de vérification d'intégrité

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.1.6 *ADMX Template Digital Signature Validation*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Validation signatures numériques templates ADMX

AUDIT :

:

- chrome://policy/ → CloudPolicyOverridesPlatformPolicy configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

2.1.7 *Central Store Replication Monitoring*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Monitoring réplication magasin central avec alertes

AUDIT :

:

- chrome://policy/ → CloudPolicyOverridesPlatformPolicy configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

2.2 — Stratégies de Groupe et Objets GPO

2.2.1 *Création d'une GPO Dédiée Chrome Sécurité*

MITRE ATT&CK : T1484

DESCRIPTION :

Créer une stratégie de groupe dédiée exclusivement aux politiques de sécurité Chrome pour faciliter la gestion, le dépannage et la séparation des responsabilités.

```
# Vérifier l'existence de la GPO Chrome Security
Get-GPO -Name "Chrome Security Policy" -ErrorAction SilentlyContinue
Get-GPOReport -Name "Chrome Security Policy" -ReportType Html -Path "ChromeGPOReport.html"
```

REMÉDIATION :

1. Créer une nouvelle GPO nommée "Chrome Security Policy"
2. Lier la GPO aux UO appropriées
3. Configurer l'ordre de priorité des GPO
4. Documenter les politiques appliquées

VALEUR PAR DÉFAUT :

Pas de GPO dédiée Chrome

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.2.2 *Configuration de la Priorité des GPO*

MITRE ATT&CK : T1484

DESCRIPTION :

Configurer l'ordre de priorité des GPO pour s'assurer que les politiques de sécurité Chrome ont la precedence sur les autres stratégies potentiellement conflictuelles.

```
# Vérifier l'ordre des GPO liées
Get-GPInheritance -Target "OU=Workstations,DC=domain,DC=local"
(Get-GPO -Name "Chrome Security Policy").GpoStatus
```

REMÉDIATION :

1. Placer la GPO Chrome en priorité haute
2. Activer "Appliqué" et désactiver "Héritage"
3. Utiliser "Enforced" si nécessaire pour les politiques critiques

VALEUR PAR DÉFAUT :

Ordre par défaut des GPO

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.2.3 *Filtrage de Sécurité des GPO Chrome*

MITRE ATT&CK : T1484

DESCRIPTION :

Configurer le filtrage de sécurité pour appliquer les politiques Chrome uniquement aux groupes d'utilisateurs et ordinateurs appropriés selon le principe du moindre privilège.

```
# Vérifier le filtrage de sécurité
Get-GPPermissions -Name "Chrome Security Policy" -All
Get-ADGroupMember -Identity "Chrome-Users-Group"
```

REMÉDIATION :

1. Créer des groupes de sécurité spécifiques (Chrome-Users, Chrome-Admins)
2. Appliquer le filtrage de sécurité sur ces groupes
3. Retirer "Utilisateurs authentifiés" si nécessaire

VALEUR PAR DÉFAUT :

Application à tous les utilisateurs authentifiés

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.2.4 *Sauvegarde et Restauration des GPO Chrome*

MITRE ATT&CK : T1484

DESCRIPTION :

Mettre en place une procédure de sauvegarde automatisée des GPO Chrome pour permettre la restauration rapide en cas de corruption ou de modification non autorisée.

```
# Vérifier les sauvegardes GPO existantes
Get-ChildItem "C:\GPOBackups" | Where-Object {$_.Name -like "*Chrome*"}
Backup-GPO -Name "Chrome Security Policy" -Path "C:\GPOBackups"
```

REMÉDIATION :

1. Créer un script de sauvegarde automatique hebdomadaire
2. Stocker les sauvegardes sur un partage sécurisé
3. Tester la procédure de restauration mensuellement

VALEUR PAR DÉFAUT :

Pas de sauvegarde automatique

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.2.5 *Monitoring des Changements de GPO Chrome*

MITRE ATT&CK : T1484

DESCRIPTION :
Surveiller et auditer tous les changements apportés aux GPO Chrome pour détecter les modifications non autorisées et maintenir un historique complet.

```
# Vérifier les événements d'audit GPO
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=5136,5137,5141} |
Where-Object {$_.Message -like "*Chrome*"}
```

REMÉDIATION :
1. Activer l'audit des changements d'objets de stratégie
2. Configurer des alertes pour les modifications GPO Chrome
3. Intégrer avec SIEM pour centraliser les logs

VALEUR PAR DÉFAUT :
Audit basique activé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.3 — Microsoft Intune et Gestion Mobile

2.3.1 *Configuration des Profils Chrome dans Intune*

MITRE ATT&CK : T1484

DESCRIPTION :
Configurer des profils de configuration Chrome dans Microsoft Intune pour gérer les appareils mobiles et les PC non joints au domaine avec les mêmes standards de sécurité.

```
# Utiliser Microsoft Graph PowerShell
Connect-MgGraph -Scopes "DeviceManagementConfiguration.Read.All"
Get-MgDeviceManagementConfigurationPolicy | Where-Object {$_.Name -like "*Chrome*"}
```

REMÉDIATION :
1. Créer un profil de configuration personnalisé pour Chrome
2. Importer les paramètres ADMX via OMA-URI
3. Assigner le profil aux groupes d'appareils appropriés

VALEUR PAR DÉFAUT :
Pas de gestion Intune Chrome

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.3.2 *Synchronisation GPO-Intune pour Chrome*

MITRE ATT&CK : T1484

DESCRIPTION :
Assurer la cohérence des politiques de sécurité Chrome entre les appareils gérés par GPO (domaine) et ceux gérés par Intune (cloud) pour maintenir un niveau de sécurité uniforme.

```
# Comparer les politiques GPO et Intune
$GPOSettings = Get-GPRegistryValue -Name "Chrome Security Policy" -Key "HKLM\SOFTWARE\Policies\Google\Chrome"
$IntuneSettings = Get-MgDeviceManagementConfigurationPolicy | Where-Object {$_.Name -eq "Chrome Security"}
```

REMÉDIATION :
1. Documenter toutes les politiques Chrome dans un référentiel central
2. Utiliser des scripts pour synchroniser les configurations
3. Tester la parité des politiques régulièrement

VALEUR PAR DÉFAUT :
Configurations indépendantes

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.3.3 *Gestion des Applications Chrome via Intune*

MITRE ATT&CK : T1484

DESCRIPTION :
Utiliser Intune pour déployer et gérer Chrome comme application d'entreprise avec contrôle des versions, mises à jour et politiques de sécurité intégrées.

```
# Vérifier le déploiement Chrome via Intune
Get-MgDeviceAppManagementMobileApp | Where-Object {$_.DisplayName -like "*Chrome*"}
Get-MgDeviceAppManagementMobileAppAssignment -MobileAppId $ChromeAppId
```

REMÉDIATION :
1. Ajouter Chrome comme application Win32 dans Intune
2. Configurer les scripts d'installation et de détection
3. Définir les groupes de déploiement et calendrier

VALEUR PAR DÉFAUT :
Déploiement manuel ou via autres outils

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.3.4 *Conformité des Appareils Chrome-Intune*

MITRE ATT&CK : T1484

DESCRIPTION :
Définir des politiques de conformité Intune qui vérifient la configuration Chrome sur les appareils et bloquent l'accès aux ressources en cas de non-conformité.

```
# Vérifier les politiques de conformité Chrome
Get-MgDeviceManagementDeviceCompliancePolicy | Where-Object {$_.DisplayName -like "*Chrome*"}
Get-MgDeviceManagementDeviceComplianceDeviceStatus
```

REMÉDIATION :
1. Créer une politique de conformité Chrome spécifique
2. Définir les critères de conformité (version, configuration)
3. Configurer l'accès conditionnel basé sur la conformité

VALEUR PAR DÉFAUT :
Pas de vérification de conformité Chrome

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.3.5 *Reporting Intune pour Chrome Enterprise*

MITRE ATT&CK : T1484

DESCRIPTION :
Configurer le reporting Intune pour surveiller le déploiement, la conformité et l'utilisation de Chrome sur les appareils gérés avec des tableaux de bord dédiés.

```
# Générer des rapports Chrome via Intune
Get-MgDeviceManagementReport
Get-MgDeviceManagementManagedDevice | Where-Object {$_.OSVersion -and $_.DeviceName}
```

REMÉDIATION :
1. Configurer des rapports personnalisés pour Chrome
2. Créer des tableaux de bord Power BI intégrés
3. Automatiser les rapports de conformité mensuels

VALEUR PAR DÉFAUT :
Reporting standard Intune

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.4 — Chrome Browser Cloud Management (CBCM)

2.4.1 *Activation et Configuration CBCM*

MITRE ATT&CK : T1484

DESCRIPTION :
Activer Chrome Browser Cloud Management pour la gestion centralisée des politiques Chrome via Google Admin Console, particulièrement pour les environnements hybrides ou cloud-first.

```
# Vérifier l'inscription CBCM
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CloudManagementEnrollmentToken"
# Vérifier dans chrome://policy la gestion cloud
```

REMÉDIATION :
1. Générer un token d'inscription depuis Google Admin Console
2. Configurer la politique CloudManagementEnrollmentToken
3. Vérifier l'inscription des appareils dans la console Admin

VALEUR PAR DÉFAUT :
CBCM non configuré

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.4.2 *Politiques de Sécurité CBCM Enterprise*

MITRE ATT&CK : T1484

DESCRIPTION :
Configurer les politiques de sécurité Chrome via CBCM en alignement avec les standards d'entreprise et réglementaires, en utilisant les modèles de sécurité Google.

```
# Les vérifications se font dans Google Admin Console
# Exportation possible via Chrome Reporting API
```

REMÉDIATION :
1. Accéder à Google Admin Console → Appareils → Chrome → Paramètres
2. Appliquer le modèle "Sécurité d'entreprise"
3. Personnaliser selon les besoins organisationnels
4. Tester sur un groupe pilote avant déploiement global

VALEUR PAR DÉFAUT :
Politiques par défaut Google

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.4.3 *Intégration CBCM avec Identity Provider*

MITRE ATT&CK : T1484

DESCRIPTION :
Intégrer CBCM avec le fournisseur d'identité d'entreprise (AD FS, Azure AD, Okta) pour l'authentification unifiée et l'application de politiques basées sur l'identité.

```
# Vérifier la configuration SSO Chrome
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AuthServerWhitelist"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AuthNegotiateDelegateWhitelist"
```

REMÉDIATION :
1. Configurer SAML SSO dans Google Admin Console
2. Définir les serveurs d'authentification autorisés
3. Tester l'authentification automatique sur les sites d'entreprise

VALEUR PAR DÉFAUT :
Pas d'intégration SSO

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.4.4 *Monitoring et Analytics CBCM*

MITRE ATT&CK : T1484

DESCRIPTION :
Utiliser les outils de monitoring et analytics intégrés à CBCM pour surveiller l'utilisation, la sécurité et la performance de Chrome dans l'entreprise.

```
# Vérifier l'activation du reporting
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ChromeManagementService"
```

REMÉDIATION :
1. Activer Chrome Enterprise Reporting dans Admin Console
2. Configurer les métriques de sécurité à surveiller
3. Créer des alertes pour les événements critiques
4. Intégrer avec les outils SIEM existants

VALEUR PAR DÉFAUT :
Reporting basique activé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

2.4.5 *Sauvegarde et Réplication des Politiques CBCM*

MITRE ATT&CK : T1484

DESCRIPTION :
Établir une stratégie de sauvegarde et réplication des politiques CBCM pour assurer la continuité de service et la récupération en cas d'incident.

```
# Les sauvegardes CBCM sont gérées par Google
# Vérifier la documentation des politiques locales
Test-Path "C:\ChromePoliciesBackup\CBCM_Config.json"
```

REMÉDIATION :
1. Documenter toutes les politiques CBCM configurées
2. Exporter régulièrement la configuration via Admin SDK
3. Maintenir une copie locale des paramètres critiques
4. Tester la procédure de reconfiguration

VALEUR PAR DÉFAUT :
Sauvegarde automatique Google

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

Section 3 — NAVIGATION SÉCURISÉE

3.1 — Google Safe Browsing et Protection Avancée

3.1.1 *Activation de Safe Browsing Standard*

MITRE ATT&CK : T1566, T1204

DESCRIPTION :

Activer Google Safe Browsing pour protéger contre les sites de phishing, malware et téléchargements dangereux. Cette fonctionnalité doit être configurée au minimum en mode standard pour tous les utilisateurs.

```
# Vérifier l'activation de Safe Browsing
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SafeBrowsingEnabled"
# Valeur attendue: 1 (activé)
# Vérifier dans chrome://settings/security
```

REMÉDIATION :

1. GPO : Configuration ordinateur → Google → Google Chrome → Safe Browsing
2. Activer "Activer la navigation sécurisée"
3. Registry : `Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SafeBrowsingEnabled" -Value 1`

VALEUR PAR DÉFAUT :

Safe Browsing activé par défaut

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.1.2 *Configuration de Safe Browsing Protection Renforcée*

MITRE ATT&CK : T1566, T1204

DESCRIPTION :

Configurer Safe Browsing en mode Protection Renforcée (Enhanced Protection) pour les utilisateurs à haut risque, offrant une protection plus proactive contre les menaces émergentes.

```
# Vérifier le mode Protection Renforcée
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SafeBrowsingProtectionLevel"
# Valeur attendue: 2 (Enhanced Protection)
```

REMÉDIATION :

1. GPO : Google Chrome → "Niveau de protection Safe Browsing"
2. Sélectionner "Protection renforcée"
3. Registry : `Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SafeBrowsingProtectionLevel" -Value 2`

VALEUR PAR DÉFAUT :

Protection standard (niveau 1)

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.1.3 *Blocage des Téléchargements Dangereux*

MITRE ATT&CK : T1566.001, T1204.002

DESCRIPTION :

Configurer Chrome pour bloquer automatiquement les téléchargements identifiés comme dangereux par Safe Browsing, sans possibilité de contournement par l'utilisateur.

```
# Vérifier le blocage des téléchargements dangereux
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SafeBrowsingForTrustedSourcesEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DownloadRestrictions"
```

REMÉDIATION :

1. Désactiver "Safe Browsing pour sources fiables" : `SafeBrowsingForTrustedSourcesEnabled = 0`
2. Configurer restrictions téléchargement : `DownloadRestrictions = 1` (bloquer fichiers dangereux)
3. Tester avec des fichiers test EICAR

VALEUR PAR DÉFAUT :

Avertissement avec possibilité de contournement

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.1.4 *Configuration des Alertes Phishing*

MITRE ATT&CK : T1566.002

DESCRIPTION :

Configurer Chrome pour afficher des alertes claires et blocantes lors de la détection de tentatives de phishing, avec impossibilité de contournement par les utilisateurs standards.

```
# Vérifier la configuration anti-phishing
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SafeBrowsingExtendedReportingOptInAllowed"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SafeBrowsingWhitelistDomains"
```

REMÉDIATION :

1. Interdire l'opt-out du reporting étendu : `SafeBrowsingExtendedReportingOptInAllowed = 0`
2. Éviter les domaines en whitelist sauf cas justifiés
3. Sensibiliser les utilisateurs aux alertes phishing

VALEUR PAR DÉFAUT :

Reporting étendu optionnel

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.1.5 *Monitoring des Événements Safe Browsing*

MITRE ATT&CK : T1566

DESCRIPTION :

Activer la collecte et le monitoring des événements Safe Browsing pour analyser les tentatives d'attaque et améliorer la posture de sécurité organisationnelle.

```
# Vérifier l'activation du reporting sécurité
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SecurityEventReporting"
```

REMÉDIATION :

1. Activer Chrome Enterprise Security Reporting
2. Configurer l'intégration avec le SIEM
3. Créer des alertes pour les détections répétées

VALEUR PAR DÉFAUT :

Reporting local uniquement

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.1.6 *Configuration de la Protection contre les URLs Suspectes*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Blocage automatique des domaines lookalike et phishing connus

AUDIT :

:

- chrome://policy/ → LookalikeWarningAllowlistDomains configuré
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Définir liste blanche domaines connus + monitoring tentatives accès lookalike
- Documentation procédures d'exception
- Formation équipes techniques

3.1.7 *Activation de la Protection Renforcée des Mots de Passe*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Détection réutilisation mot de passe sur sites potentiellement malveillants

AUDIT :

:

- chrome://policy/ → PasswordProtectionWarningTrigger = 1 (PHISHING_REUSE)
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Activer protection + intégration base données compromissions + alertes temps réel
- Documentation procédures d'exception
- Formation équipes techniques

3.1.8 *Configuration du Scanning Avancé des Téléchargements*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Scanning cloud avancé fichiers téléchargés + analyse comportementale

AUDIT :

:

- chrome://policy/ → SafeBrowsingExtendedReportingEnabled = true
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

2.4.6 *Configuration Chrome Enterprise Connectors*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: DLP connectors pour scanning contenu temps réel

AUDIT :

:

- chrome://policy/ → OnFileAttachedEnterpriseConnector configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

2.4.7 *Real-time URL Check Enterprise*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Vérification URLs temps réel avec threat intelligence

AUDIT :

:

- chrome://policy/ → OnSecurityEventEnterpriseConnector configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques
- Activer reporting étendu + définir seuils détection + quarantaine auto
- Documentation procédures d'exception
- Formation équipes techniques

3.1.9 *Blocage des Connexions Non-Sécurisées*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Interdiction contenu mixte HTTP/HTTPS sauf exceptions métier documentées

AUDIT :

:

- chrome://policy/ → InsecureContentAllowedForUrls vide ou URLs légitimes uniquement
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Audit applications legacy + migration HTTPS + exceptions temporaires documentées
- Documentation procédures d'exception
- Formation équipes techniques

3.1.10 *Protection contre les Attaques de Redirection Malveillante*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Blocage pop-ups, redirections forcées et manipulations UI malveillantes

AUDIT :

:

- chrome://policy/ → AbusiveExperienceInterventionEnforce = true
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Enforcement strict + monitoring tentatives contournement + éducation utilisateurs
- Documentation procédures d'exception
- Formation équipes techniques

3.2 — Protection contre les Malwares

3.2.1 *Scanning Antimalware Intégré*

MITRE ATT&CK : T1204.002

DESCRIPTION :

Activer le scanning antimalware intégré de Chrome pour analyser tous les téléchargements en temps réel avant exécution ou ouverture des fichiers.

```
# Vérifier l'activation du scanner intégré
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AdvancedProtectionAllowed"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CheckContentCompliance"
```

REMÉDIATION :

1. Activer Advanced Protection : `AdvancedProtectionAllowed = 1`
2. Forcer la vérification de contenu : `CheckContentCompliance = 1`
3. Intégrer avec Windows Defender ou autre antivirus

VALEUR PAR DÉFAUT :

Scanner basique activé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.2.2 *Quarantaine des Fichiers Suspects*

MITRE ATT&CK : T1204.002

DESCRIPTION :

Configurer Chrome pour mettre en quarantaine automatiquement les fichiers suspects détectés lors des téléchargements, en attendant une analyse approfondie.

```
# Vérifier la configuration de quarantaine
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DownloadDirectory"
Get-ChildItem "C:\Users\*\Downloads" -File | Where-Object {$_.Name -like "*.crdownload"}
```

REMÉDIATION :

1. Configurer un dossier de quarantaine dédié
2. Intégrer avec l'antivirus d'entreprise
3. Automatiser l'analyse des fichiers en quarantaine

3.1.11 *Protection Avancée contre Social Engineering*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Détection tentatives social engineering et manipulations utilisateur

AUDIT :

:

- Monitoring patterns social engineering + baseline comportement + alertes
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- ML détection + training utilisateurs + incident response + forensique
- Documentation procédures d'exception
- Formation équipes techniques

3.1.12 *Intégration Threat Intelligence Feeds*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Alimentation automatique IoCs et threat intelligence externe

AUDIT :

:

- Flux threat intel + corrélation IoCs + effectiveness metrics + update frequency
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- API threat intel + automated blocking + correlation + metrics + tuning
- Documentation procédures d'exception
- Formation équipes techniques

VALEUR PAR DÉFAUT :

Téléchargements directs sans quarantaine

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.2.3 *Blocage des Extensions Malveillantes*

MITRE ATT&CK : T1176

DESCRIPTION :

Empêcher l'installation d'extensions identifiées comme malveillantes par Safe Browsing et maintenir une liste noire actualisée des extensions compromises.

```
# Vérifier le blocage des extensions malveillantes
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallBlacklist"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallWhitelist"
```

REMÉDIATION :

1. Utiliser `ExtensionInstallBlacklist` avec la valeur "*" pour bloquer toutes les extensions par défaut
2. Autoriser uniquement les extensions approuvées via `ExtensionInstallWhitelist`
3. Maintenir la liste noire à jour avec les IOC

VALEUR PAR DÉFAUT :

Installation libre depuis Chrome Web Store

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.2.4 *Protection contre les Scripts Malveillants*

MITRE ATT&CK : T1059.007

DESCRIPTION :

Configurer Chrome pour détecter et bloquer l'exécution de scripts malveillants, particulièrement les cryptojackers et scripts de minage cryptocurrency.

```
# Vérifier la protection contre les scripts malveillants
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "JavaScriptAllowed"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DefaultJavaScriptSetting"
```

REMÉDIATION :

1. Configurer la politique JavaScript sur "Ask" pour les sites non-fiables
2. Bloquer les domaines connus de cryptojacking
3. Utiliser Content Security Policy pour limiter l'exécution de scripts

VALEUR PAR DÉFAUT :

JavaScript autorisé partout

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.2.5 *Surveillance des Indicateurs de Compromission*

MITRE ATT&CK : T1204

DESCRIPTION :

Mettre en place une surveillance active des indicateurs de compromission (IOC) liés aux malwares dans l'historique de navigation et les téléchargements Chrome.

```
# Vérifier la collecte d'IOC
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "MetricsReportingEnabled"
Get-ChildItem "C:\Users\*\AppData\Local\Google\Chrome\User Data\Default" -File
```

REMÉDIATION :

1. Activer la collecte de métriques sécurisées
2. Configurer l'export vers les outils SIEM/EDR
3. Créer des règles de détection basées sur les IOC

VALEUR PAR DÉFAUT :

Collecte basique de métriques

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.3 — Filtrage et Blocage de Contenu

3.3.1 *Configuration du Filtrage URL Enterprise*

MITRE ATT&CK : T1566.002

DESCRIPTION :

Implémenter un système de filtrage URL comprehensive pour bloquer l'accès aux sites malveillants, de phishing et non-autorisés selon la politique d'entreprise.

```
# Vérifier la configuration du filtrage URL
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "URLBlacklist"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "URLWhitelist"
```

REMÉDIATION :

1. Configurer `URLBlacklist` avec les catégories dangereuses
2. Utiliser `URLWhitelist` pour les exceptions nécessaires
3. Intégrer avec la solution de filtrage web d'entreprise
4. Tester régulièrement l'efficacité du filtrage

VALEUR PAR DÉFAUT :

Pas de filtrage URL configuré

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.3.2 *Blocage des Contenus Mixtes HTTPS/HTTP*

MITRE ATT&CK : T1557.001

DESCRIPTION :

Bloquer le chargement de contenus HTTP sur des pages HTTPS pour prévenir les attaques de type mixed content et man-in-the-middle.

```
# Vérifier le blocage des contenus mixtes
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "InsecureContentAllowedForUrls"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "InsecureContentBlockedForUrls"
```

REMÉDIATION :

1. Minimiser l'utilisation d'`InsecureContentAllowedForUrls`
2. Configurer `InsecureContentBlockedForUrls` pour les domaines sensibles
3. Sensibiliser les développeurs aux bonnes pratiques HTTPS

VALEUR PAR DÉFAUT :

Avertissement mais autorisation du contenu mixte

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.3.3 *Restriction des Téléchargements par Type de Fichier*

MITRE ATT&CK : T1204.002

DESCRIPTION :

Configurer des restrictions granulaires sur les téléchargements de fichiers selon leur type et origine pour minimiser les risques d'infection par malware.

```
# Vérifier les restrictions de téléchargement
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DownloadRestrictions"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DefaultDownloadDirectory"
```

REMÉDIATION :

1. Configurer `DownloadRestrictions` : 1=bloquer dangereux, 2=bloquer potentiellement dangereux
2. Limiter les types de fichiers autorisés (.pdf, .txt, .docx, etc.)
3. Scanner automatiquement le dossier de téléchargement

VALEUR PAR DÉFAUT :

Tous téléchargements autorisés avec avertissement

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.3.4 *Blocage des Pop-ups et Redirections Malveillantes*

MITRE ATT&CK : T1566.002

DESCRIPTION :

Renforcer le blocage des pop-ups et redirections automatiques utilisées dans les campagnes de phishing et distribution de malware.

```
# Vérifier le blocage des pop-ups
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DefaultPopupsSetting"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PopupsBlockedForUrls"
```

REMÉDIATION :

1. Définir `DefaultPopupsSetting` à 2 (bloquer les pop-ups)
2. Utiliser `PopupsAllowedForUrls` uniquement pour les applications métier
3. Sensibiliser les utilisateurs aux techniques de social engineering

VALEUR PAR DÉFAUT :

Blocage standard des pop-ups

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.3.5 *Filtrage des Annonces et Trackers Malveillants*

MITRE ATT&CK : T1566.002

DESCRIPTION :

Activer le filtrage natif Chrome des annonces intrusives et configurer la protection contre les trackers malveillants pour réduire la surface d'attaque.

```
# Vérifier le filtrage des annonces
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AdsSettingForIntrusiveAdsSites"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "BlockThirdPartyCookies"
```

REMÉDIATION :

1. Activer le filtre anti-annonces intrusives par défaut
2. Bloquer les cookies tiers sauf exceptions métier
3. Évaluer l'utilisation d'extensions ad-block approuvées

VALEUR PAR DÉFAUT :

Filtre basic activé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.4 — Protection Avancée contre les Menaces

3.4.1 *Configuration de l'Isolation de Sites Avancée*

MITRE ATT&CK : T1055

DESCRIPTION :

Activer l'isolation de sites avancée pour empêcher les attaques cross-site et limiter l'impact des vulnérabilités d'exécution de code dans le moteur de rendu.

```
# Vérifier l'isolation de sites
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SitePerProcess"
# Vérifier dans chrome://process-internals
```

REMÉDIATION :

1. Activer `SitePerProcess` : valeur 1
2. Configurer `IsolateOrigins` pour les sites sensibles
3. Monitorer l'impact sur les performances

VALEUR PAR DÉFAUT :

Isolation partielle activée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.4.2 *Protection contre les Attaques Spectre/Meltdown*

MITRE ATT&CK : T1055.012

DESCRIPTION :

Configurer les mitigations Chrome contre les attaques de type Spectre/Meltdown via l'isolation stricte des processus et la désactivation des timers haute précision.

```
# Vérifier les mitigations Spectre
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "HighResolutionTimeApi"
# Vérifier dans chrome://flags les flags de sécurité
```

REMÉDIATION :

1. Désactiver les APIs de temps haute résolution si non nécessaires
2. Activer l'isolation stricte des sites
3. Maintenir Chrome à jour pour les dernières mitigations

VALEUR PAR DÉFAUT :

Mitigations de base activées

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.4.3 *Détection des Tentatives d'Exploitation*

MITRE ATT&CK : T1203

DESCRIPTION :

Configurer Chrome pour détecter et reporter les tentatives d'exploitation de vulnérabilités, incluant les crashes suspects et comportements anormaux.

```
# Vérifier la collecte de crashs
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "MetricsReportingEnabled"
Get-ChildItem "C:\Users\*\AppData\Local\Google\Chrome\User Data\Crashpad"
```

REMÉDIATION :

1. Activer la collecte de rapports de crash sécurisés
2. Configurer l'analyse automatique des patterns de crash
3. Intégrer avec les outils de détection d'incidents

VALEUR PAR DÉFAUT :

Rapports de crash basiques

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.4.4 *Protection contre les Attaques de Déni de Service*

MITRE ATT&CK : T1499.004

DESCRIPTION :

Configurer des limites de ressources pour prévenir les attaques DoS via des pages web consommant excessivement CPU, mémoire ou connexions réseau.

```
# Vérifier les limites de ressources
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "MemoryPressureOffPages"
```

REMÉDIATION :

1. Configurer des limites de mémoire par onglet
2. Activer la suspension automatique des onglets inactifs
3. Limiter le nombre de connexions simultanées par site

VALEUR PAR DÉFAUT :

Gestion automatique des ressources

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.4.5 *Réponse Automatisée aux Incidents de Sécurité*

MITRE ATT&CK : T1566

DESCRIPTION :

Mettre en place des mécanismes de réponse automatisée aux détections de sécurité Chrome, incluant isolation de session et notification des équipes sécurité.

3.2.6 *Advanced Persistent Threat (APT) Detection*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Détection APTs avec behavioral analysis avancée

AUDIT :

:

- chrome://policy/ → AdvancedProtectionAllowed configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

3.2.7 *Zero-Day Exploit Protection*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Protection exploits zero-day avec sandboxing

AUDIT :

:

- chrome://policy/ → SafeBrowsingExtendedReportingEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

Vérifier la configuration de réponse automatisée

Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SecurityEventActions"

3.5 — Analyse et Forensique de Navigation

3.5.1 *Conservation des Logs de Navigation Sécurisée*

MITRE ATT&CK : T1070.003

DESCRIPTION :

Configurer la conservation et la protection des logs de navigation pour l'analyse forensique et la détection d'incidents de sécurité post-compromission.

```
# Vérifier la configuration de logging
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ChromeCleanupReportingEnabled"
Get-ChildItem "C:\Users\*\AppData\Local\Google\Chrome\User Data\Default\History"
```

REMÉDIATION :

1. Activer la collecte de logs de sécurité détaillés
2. Configurer la rétention selon la politique d'entreprise
3. Chiffrer et protéger l'accès aux logs sensibles

VALEUR PAR DÉFAUT :

Logs basiques avec rétention limitée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.5.2 *Intégration avec les Outils SIEM/SOAR*

MITRE ATT&CK : T1566

DESCRIPTION :

Intégrer les événements de sécurité Chrome avec les plateformes SIEM et SOAR d'entreprise pour une détection et réponse centralisées aux incidents.

```
# Vérifier l'intégration SIEM
Get-Service "Splunk*","Elastic*" -ErrorAction SilentlyContinue
Test-NetConnection -ComputerName "siem.company.com" -Port 514
```

REMÉDIATION :

1. Configurer l'export des événements Chrome vers le SIEM
2. Créer des règles de corrélation spécifiques aux menaces web
3. Automatiser les réponses via playbooks SOAR

VALEUR PAR DÉFAUT :

Pas d'intégration SIEM

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.5.3 *Analyse Comportementale des Patterns de Navigation*

MITRE ATT&CK : T1566.002

DESCRIPTION :

Implémenter une analyse comportementale pour détecter les patterns de navigation anormaux indicateurs de compromission ou d'activité malveillante.

```
# Vérifier la collecte de métriques comportementales
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "UserDataSnapshotEnabled"
```

REMÉDIATION :

1. Activer la collecte anonymisée de patterns de navigation
2. Configurer des baselines comportementales par utilisateur/groupe
3. Créer des alertes pour les déviations significatives

VALEUR PAR DÉFAUT :

Pas d'analyse comportementale

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.5.4 *Threat Intelligence et IOC Feeding*

MITRE ATT&CK : T1566

DESCRIPTION :

Intégrer les flux de Threat Intelligence pour enrichir automatiquement les listes de blocage Chrome avec les derniers IOC et domaines malveillants identifiés.

```
# Vérifier les sources de threat intelligence configurées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ThreatIntelligenceSources"
```

REMÉDIATION :

1. S'abonner aux flux de TI pertinents (MISP, AlienVault, etc.)
2. Automatiser la mise à jour des listes de blocage Chrome
3. Configurer des feed-back loops vers les plateformes de TI

VALEUR PAR DÉFAUT :

Safe Browsing uniquement

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

3.5.5 *Reporting et Métriques de Sécurité Navigation*

MITRE ATT&CK : T1566

DESCRIPTION :

Générer des rapports périodiques sur les incidents de sécurité liés à la navigation, incluant métriques de détection, types de menaces et efficacité des contrôles.

3.3.6 *Content Security Policy (CSP) Enforcement*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Enforcement CSP stricte avec nonces et hashes

AUDIT :

:

- chrome://policy/ → DefaultImagesSetting configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

3.3.7 *Subresource Integrity (SRI) Validation*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Validation intégrité sous-ressources avec SRI

AUDIT :

:

- chrome://policy/ → DefaultJavaScriptSetting configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

Section 4 — GESTION DES MOTS DE PASSE

4.1 — Configuration du Gestionnaire de Mots de Passe Chrome

4.1.1 *Activation Contrôlée du Gestionnaire Intégré*

MITRE ATT&CK : T1555.003

DESCRIPTION :

Configurer le gestionnaire de mots de passe intégré de Chrome selon la politique d'entreprise, en privilégiant les solutions d'entreprise dédiées lorsque disponibles.

```
# Vérifier la configuration du gestionnaire de mots de passe
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordManagerEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordLeakDetectionEnabled"
```

REMÉDIATION :

1. Évaluer si un gestionnaire d'entreprise est disponible (1Password, Bitwarden Business)
2. Si gestionnaire Chrome utilisé : `PasswordManagerEnabled = 1`
3. Activer la détection de fuites : `PasswordLeakDetectionEnabled = 1`
4. Configurer des politiques de complexité appropriées

VALEUR PAR DÉFAUT :

Gestionnaire activé par défaut

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.1.2 *Désactivation du Gestionnaire pour Solutions d'Entreprise*

MITRE ATT&CK : T1555.003

DESCRIPTION :

Désactiver le gestionnaire de mots de passe Chrome lorsqu'une solution d'entreprise dédiée est déployée pour éviter la fragmentation et maintenir la gouvernance centralisée.

```
# Vérifier la désactivation du gestionnaire Chrome
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordManagerEnabled"
# Vérifier la présence de gestionnaires d'entreprise
Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -like "*1Password*" -or $_.Name -like "*Bitwarden*"}
```

REMÉDIATION :

1. Désactiver le gestionnaire Chrome : `PasswordManagerEnabled = 0`
2. Bloquer l'enregistrement automatique : `AutofillAddressEnabled = 0`
3. Configurer l'extension du gestionnaire d'entreprise via force-install
4. Former les utilisateurs à la transition

VALEUR PAR DÉFAUT :

Gestionnaire Chrome activé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.1.3 *Configuration du Chiffrement Local des Mots de Passe*

MITRE ATT&CK : T1555.003

DESCRIPTION :

S'assurer que les mots de passe stockés localement par Chrome sont correctement chiffrés en utilisant les mécanismes de protection de données Windows (DPAPI).

```
# Vérifier le chiffrement des données Chrome
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "EncryptionKey"
Get-ChildItem "C:\Users\*\AppData\Local\Google\Chrome\User Data\Default" -File | Where-Object {$_.Name -eq "Login Data"}
```

REMÉDIATION :

1. Vérifier que DPAPI est utilisé pour le chiffrement
2. Configurer la protection renforcée des profils utilisateur
3. Activer BitLocker sur les postes pour protection au niveau disque
4. Sensibiliser sur les risques de partage de session

VALEUR PAR DÉFAUT :

Chiffrement DPAPI activé par défaut

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.1.4 *Audit des Mots de Passe Faibles et Compromis*

MITRE ATT&CK : T1110

DESCRIPTION :

Activer l'audit automatique des mots de passe pour détecter les mots de passe faibles, réutilisés ou compromis dans les bases de données de fuites connues.

```
# Vérifier l'activation de l'audit des mots de passe
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordCheckEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordLeakDetectionEnabled"
```

REMÉDIATION :

1. Activer la vérification des mots de passe : `PasswordCheckEnabled = 1`
2. Activer la détection de fuites : `PasswordLeakDetectionEnabled = 1`
3. Configurer des notifications pour les mots de passe compromis
4. Intégrer avec Have I Been Pwned API si nécessaire

VALEUR PAR DÉFAUT :

Vérification basique activée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.1.5 *Gestion de la Synchronisation des Mots de Passe*

MITRE ATT&CK : T1555.003

DESCRIPTION :

Contrôler strictement la synchronisation des mots de passe via Google Account pour prévenir l'exfiltration non autorisée des credentials d'entreprise.

```
# Vérifier la configuration de synchronisation
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SyncDisabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SyncTypesListDisabled"
```

REMÉDIATION :

1. Désactiver la sync globalement : `SyncDisabled = 1` ou
2. Désactiver uniquement les mots de passe : `SyncTypesListDisabled = ["passwords"]`
3. Si sync nécessaire, utiliser Google Workspace avec DLP
4. Auditer régulièrement les comptes Google connectés

VALEUR PAR DÉFAUT :

Synchronisation activée si utilisateur connecté

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.2 — Politiques d'Auto-Complétion et de Saisie

4.2.1 *Configuration de l'Auto-Complétion Sécurisée*

MITRE ATT&CK : T1555.003

DESCRIPTION :

Configurer l'auto-complétion pour équilibrer sécurité et usabilité, en restreignant l'auto-complétion sur les sites non-sécurisés et les champs sensibles.

```
# Vérifier la configuration d'auto-complétion
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AutofillAddressEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AutofillCreditCardEnabled"
```

REMÉDIATION :

1. Désactiver l'auto-complétion des cartes de crédit : `AutofillCreditCardEnabled = 0`
2. Restreindre l'auto-complétion des adresses selon les besoins
3. Configurer des exceptions pour les sites d'entreprise sécurisés
4. Sensibiliser sur les risques de shoulder surfing

VALEUR PAR DÉFAUT :

Auto-complétion activée pour la plupart des champs

3.4.6 *Machine Learning Threat Detection*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: ML détection menaces avec learning continu

AUDIT :

:

- chrome://policy/ → CloudPolicyOverridesPlatformPolicy configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

3.4.7 *Behavioral Analysis Engine*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Analyse comportementale avec detection déviations

AUDIT :

:

- chrome://policy/ → SafeBrowsingExtendedReportingEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.2.2 *Restriction sur Sites Non-HTTPS*

MITRE ATT&CK : T1557.001

DESCRIPTION :

Empêcher l'auto-complétion et la sauvegarde de mots de passe sur les sites non-sécurisés (HTTP) pour prévenir l'interception en transit.

```
# Vérifier les restrictions HTTP
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordProtectionWarningTrigger"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordProtectionLoginURLs"
```

REMÉDIATION :

1. Configurer l'avertissement pour les connexions non-HTTPS
2. Bloquer la sauvegarde de mots de passe sur HTTP
3. Sensibiliser sur l'importance de HTTPS
4. Utiliser HSTS pour forcer HTTPS sur les domaines d'entreprise

VALEUR PAR DÉFAUT :

Avertissement mais autorisation sur HTTP

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.2.3 *Gestion des Exceptions d'Auto-Complétion*

MITRE ATT&CK : T1555.003

DESCRIPTION :

Définir des règles d'exception pour l'auto-complétion basées sur les domaines, types de champs et niveau de sensibilité des données.

```
# Vérifier les exceptions configurées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AutofillAddressEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordManagerAllowlistUrls"
```

REMÉDIATION :

1. Créer une whitelist des domaines d'entreprise autorisés
2. Définir des règles par type de données (personnelles vs. professionnelles)
3. Documenter et réviser les exceptions trimestriellement
4. Tester l'impact sur l'expérience utilisateur

VALEUR PAR DÉFAUT :

Pas d'exceptions spécifiques configurées

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.2.4 *Protection contre les Attaques de Formulaires*

MITRE ATT&CK : T1566.002

DESCRIPTION :

Configurer des protections contre les attaques par formulaires malveillants conçus pour voler les credentials via l'auto-complétion ou la saisie manuelle.

```
# Vérifier les protections contre le phishing
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordProtectionWarningTrigger"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SafeBrowsingProtectionLevel"
```

REMÉDIATION :

1. Activer les alertes de phishing pour les formulaires de connexion
2. Configurer la protection renforcée Safe Browsing
3. Bloquer l'auto-complétion sur les sites suspects
4. Former les utilisateurs à identifier les formulaires frauduleux

VALEUR PAR DÉFAUT :

Protection basique contre le phishing

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.2.5 *Audit des Données d'Auto-Complétion*

MITRE ATT&CK : T1555.003

DESCRIPTION :
Mettre en place un audit régulier des données d'auto-complétion stockées pour identifier les informations sensibles et s'assurer de leur protection adéquate.

```
# Vérifier les données d'auto-complétion stockées
Get-ChildItem "C:\Users\*\AppData\Local\Google\Chrome\User Data\Default\Web Data"
# Script PowerShell pour analyser la base SQLite (nécessite outils)
```

REMÉDIATION :
1. Développer des scripts d'audit automatisés
2. Identifier et purger les données sensibles inappropriées
3. Créer des rapports de conformité réguliers
4. Sensibiliser les utilisateurs sur les données stockées

VALEUR PAR DÉFAUT :
Pas d'audit automatique des données stockées

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.3 — Intégration avec les Gestionnaires d'Entreprise

4.3.1 *Déploiement d'Extensions de Gestionnaires Certifiés*

MITRE ATT&CK : T1555.003

DESCRIPTION :
Déployer et configurer les extensions des gestionnaires de mots de passe d'entreprise certifiés (1Password Business, Bitwarden, LastPass Enterprise) via force-install.

```
# Vérifier les extensions force-installées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallForcelist"
Get-ChildItem "C:\Users\*\AppData\Local\Google\Chrome\User Data\Default\Extensions"
```

REMÉDIATION :
1. Identifier le gestionnaire d'entreprise standard
2. Configurer force-install via `ExtensionInstallForcelist`
3. Désactiver le gestionnaire Chrome intégré
4. Configurer les politiques spécifiques à l'extension

VALEUR PAR DÉFAUT :
Pas d'extension force-installée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.3.2 *Configuration de l'Authentification Unique (SSO)*

MITRE ATT&CK : T1556

DESCRIPTION :
Configurer l'intégration avec les solutions SSO d'entreprise (SAML, OAuth, ADFS) pour minimiser la gestion de mots de passe multiples.

```
# Vérifier la configuration SSO
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AuthServerWhitelist"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AuthNegotiateDelegateWhitelist"
```

REMÉDIATION :
1. Configurer les serveurs d'authentification autorisés
2. Activer l'authentification intégrée Windows si approprié
3. Configurer les domaines de délégation Kerberos
4. Tester l'authentification automatique sur les applications métier

VALEUR PAR DÉFAUT :
Authentification manuelle par défaut

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.3.3 *Blocage des Gestionnaires Non-Autorisés*

MITRE ATT&CK : T1555.003

DESCRIPTION :
Bloquer l'installation et l'utilisation de gestionnaires de mots de passe non-autorisés par l'entreprise pour maintenir la gouvernance et éviter la fragmentation.

```
# Vérifier les blocages d'extensions
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallBlacklist"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallWhitelist"
```

3.5.6 *Digital Forensics Evidence Collection*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Collection preuves numériques avec chain of custody

AUDIT :

:

- chrome://policy/ → CloudReportingEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

3.5.7 *Incident Response Automation*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Réponse automatisée incidents avec playbooks

AUDIT :

:

- chrome://policy/ → SafeBrowsingExtendedReportingEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

REMÉDIATION :

1. Créer une blacklist des gestionnaires non-autorisés
2. Utiliser une whitelist restrictive pour les extensions
3. Surveiller les tentatives d'installation d'extensions bloquées
4. Sensibiliser sur les risques des solutions non-approuvées

VALEUR PAR DÉFAUT :

Installation libre depuis Chrome Web Store

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.3.4 *Monitoring des Accès aux Gestionnaires*

MITRE ATT&CK : T1555.003

DESCRIPTION :

Mettre en place un monitoring des accès et utilisations des gestionnaires de mots de passe pour détecter les comportements anormaux ou les tentatives d'accès non autorisé.

```
# Vérifier les logs d'accès aux extensions
Get-EventLog -LogName Application -Source "Chrome" | Where-Object {$_.Message -like "*password*"}
```

REMÉDIATION :

1. Activer les logs détaillés des extensions de mots de passe
2. Configurer des alertes pour les accès inhabituels
3. Intégrer avec le SIEM pour corrélation des événements
4. Créer des tableaux de bord d'utilisation

VALEUR PAR DÉFAUT :

Logging basique des extensions

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.3.5 *Sauvegarde et Récupération des Politiques de Mots de Passe*

MITRE ATT&CK : T1555.003

DESCRIPTION :

Établir des procédures de sauvegarde et récupération pour les configurations de gestion des mots de passe Chrome et les extensions associées.

```
# Vérifier les sauvegardes de configuration
Get-ChildItem "C:\Backups\ChromePasswordPolicies" -File
Test-Path "C:\Backups\ChromePasswordPolicies\ExtensionSettings.json"
```

REMÉDIATION :

1. Sauvegarder régulièrement les politiques GPO relatives aux mots de passe
2. Documenter les configurations des extensions de gestionnaires
3. Tester les procédures de restauration
4. Maintenir un inventaire des extensions approuvées

VALEUR PAR DÉFAUT :

Pas de sauvegarde spécifique des politiques de mots de passe

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.4 — Détection et Prévention des Fuites de Credentials

4.4.1 *Activation de la Détection de Fuites Google*

MITRE ATT&CK : T1110.001

DESCRIPTION :

Activer la fonctionnalité de détection de fuites de mots de passe de Google pour identifier proactivement les credentials compromis dans les bases de données publiques.

```
# Vérifier l'activation de la détection de fuites
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordLeakDetectionEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordCheckEnabled"
```

REMÉDIATION :

1. Activer la détection de fuites : `PasswordLeakDetectionEnabled = 1`
2. Configurer des notifications automatiques pour les utilisateurs
3. Intégrer avec les processus de gestion des incidents
4. Former les utilisateurs aux actions à prendre en cas de détection

VALEUR PAR DÉFAUT :

Détection activée par défaut

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.4.2 *Intégration avec Have I Been Pwned*

MITRE ATT&CK : T1110.001

DESCRIPTION :

Compléter la détection native Chrome avec des vérifications régulières contre la base de données Have I Been Pwned pour une couverture étendue des fuites.

```
# Vérifier l'intégration HIBP (généralement via scripts externes)
Test-Path "C:\Scripts\HIBPPasswordCheck.ps1"
Get-ScheduledTask | Where-Object {$_.TaskName -like "*HIBP*"}
```

REMÉDIATION :

1. Développer ou acquérir des outils d'intégration HIBP
2. Programmer des vérifications automatiques mensuelles
3. Créer des workflows de notification et remédiation
4. Respecter les limites d'API et politiques d'utilisation

VALEUR PAR DÉFAUT :

Pas d'intégration HIBP native

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.4.3 *Monitoring des Tentatives de Réutilisation*

MITRE ATT&CK : T1110.001

DESCRIPTION :

Surveiller et alerter sur les tentatives de réutilisation de mots de passe entre différents sites et services pour détecter les patterns à risque.

```
# Vérifier la surveillance de réutilisation
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordReuseDetectionEnabled"
```

REMÉDIATION :

1. Activer la détection de réutilisation native Chrome
2. Configurer des seuils d'alerte appropriés

4.1.6 *Password Breach Detection API*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: API détection mots de passe compromis temps réel

AUDIT :

:

- chrome://policy/ → PasswordProtectionChangePasswordURL configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

4.1.7 *Enterprise Password Policy Enforcement*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Enforcement politiques mots de passe entreprise

AUDIT :

:

- chrome://policy/ → PasswordManagerEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

1. Sensibiliser sur les risques de réutilisation
2. Promouvoir l'utilisation de gestionnaires pour mots de passe uniques

VALEUR PAR DÉFAUT :

Détection basique de réutilisation

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.4.4 *Blocage des Domaines de Phishing Connus*

MITRE ATT&CK : T1566.002

DESCRIPTION :

Maintenir une liste actualisée des domaines de phishing connus pour empêcher la saisie de credentials sur des sites frauduleux imitant les services légitimes.

```
# Vérifier la liste de blocage de domaines
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "URLBlacklist"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PasswordProtectionLoginURLs"
```

REMÉDIATION :

1. Maintenir une liste noire actualisée des domaines de phishing
2. Configurer des alertes spécifiques aux tentatives de connexion sur sites frauduleux
3. Utiliser les flux de threat intelligence pour les mises à jour
4. Bloquer proactivement les typosquatting des domaines d'entreprise

VALEUR PAR DÉFAUT :

Blocage basé sur Safe Browsing uniquement

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

4.4.5 *Réponse Automatisée aux Détections de Fuites*

MITRE ATT&CK : T1110.001

DESCRIPTION :

Mettre en place des réponses automatisées lorsque des fuites de credentials sont détectées, incluant notifications, blocages temporaires et procédures de réinitialisation.

```
# Vérifier les mécanismes de réponse automatisée
Get-ScheduledTask | Where-Object {$_.TaskName -like "*PasswordBreach*"}
Test-Path "C:\Scripts\PasswordBreachResponse.ps1"
```

REMÉDIATION :

1. Développer des playbooks de réponse automatisée
2. Configurer des notifications multicanales (email, SMS, Teams)
3. Intégrer avec les systèmes de gestion d'identité pour réinitialisation
4. Tester régulièrement les procédures de réponse

VALEUR PAR DÉFAUT :

Notifications manuelles uniquement

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

Section 5 — COOKIES & DONNÉES DE NAVIGATION

5.1 — Gestion des Cookies Tiers et Tracking

5.1.1 *Blocage des Cookies Tiers par Défaut*

MITRE ATT&CK : T1539

DESCRIPTION :

Configurer Chrome pour bloquer les cookies tiers par défaut afin de limiter le tracking cross-site et réduire la surface d'attaque pour les vols de session.

```
# Vérifier la politique des cookies tiers
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DefaultThirdPartyLockingEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "BlockThirdPartyCookies"
```

REMÉDIATION :

1. Activer le blocage des cookies tiers : `BlockThirdPartyCookies = 1`
2. Configurer des exceptions pour les applications métier nécessaires
3. Tester l'impact sur les applications d'entreprise
4. Documenter les exceptions approuvées

VALEUR PAR DÉFAUT :

Cookies tiers autorisés avec restrictions

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.1.2 *Configuration SameSite Cookie Policy*

MITRE ATT&CK : T1539, T1552.001

DESCRIPTION :

Enforcer la politique SameSite pour les cookies afin de prévenir les attaques CSRF et limiter la transmission de cookies dans les requêtes cross-site.

```
# Vérifier la configuration SameSite
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SameSiteByDefaultCookiesEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CookiesWithoutSameSiteMustBeSecureEnabled"
```

REMÉDIATION :

1. Activer SameSite par défaut : `SameSiteByDefaultCookiesEnabled = 1`
2. Forcer Secure pour cookies sans SameSite : `CookiesWithoutSameSiteMustBeSecureEnabled = 1`
3. Auditer les applications pour compatibilité SameSite
4. Former les développeurs sur les bonnes pratiques

VALEUR PAR DÉFAUT :

SameSite=Lax par défaut sur Chrome récent

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.1.3 *Gestion des Cookies de Session Sécurisés*

MITRE ATT&CK : T1539

DESCRIPTION :

S'assurer que les cookies de session sont correctement sécurisés avec les flags Secure et HttpOnly pour prévenir les vols de session via XSS ou interception réseau.

```
# Vérifier les politiques de cookies sécurisés
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CookiesSessionOnlyForUrls"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DefaultCookiesSetting"
```

REMÉDIATION :

1. Configurer les domaines nécessitant cookies sécurisés uniquement
2. Bloquer les cookies non-sécurisés sur HTTPS : `DefaultCookiesSetting = 4`
3. Auditer les applications pour usage correct des flags de sécurité
4. Implémenter des contrôles de durée de session

VALEUR PAR DÉFAUT :

Cookies persistants autorisés

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.1.4 *Limitation de la Durée de Vie des Cookies*

MITRE ATT&CK : T1539

DESCRIPTION :

Configurer des limites sur la durée de vie des cookies pour réduire la fenêtre d'opportunité en cas de vol de session ou d'accès non autorisé.

```
# Vérifier les limites de durée de cookies
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CookieExpirationLimit"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SessionCookieLimit"
```

REMÉDIATION :

1. Définir une durée maximale appropriée (ex: 24h pour les sessions critiques)
2. Configurer la suppression automatique des cookies expirés
3. Implémenter des timeouts de session côté application
4. Sensibiliser sur la fermeture de session explicite

VALEUR PAR DÉFAUT :

Pas de limite explicite sur la durée des cookies

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.1.5 *Monitoring des Anomalies de Cookies*

MITRE ATT&CK : T1539

DESCRIPTION :

Mettre en place une surveillance des patterns anormaux d'utilisation de cookies pour détecter les tentatives de hijacking de session ou d'exploitation.

4.2.6 *Form Data Leak Prevention (DLP)*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: DLP formulaires avec détection données sensibles

AUDIT :

:

- chrome://policy/ → AutofillAddressEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

4.2.7 *Credit Card Data Protection Enhanced*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Protection renforcée données cartes crédit PCI-DSS

AUDIT :

:

- chrome://policy/ → AutofillCreditCardEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CookieMetricsEnabled"

5.2 — Protection des Données de Navigation

5.2.1 *Chiffrement du Stockage Local*

MITRE ATT&CK : T1555.003

DESCRIPTION :

S'assurer que toutes les données de navigation (historique, cookies, cache) sont correctement chiffrées au repos en utilisant les mécanismes de protection de données système.

```
# Vérifier le chiffrement des données utilisateur
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "UserDataSnapshotEnabled"
Get-ChildItem "C:\Users\*\AppData\Local\Google\Chrome\User Data" -Directory
```

REMÉDIATION :

1. Vérifier l'activation de DPAPI pour le chiffrement
2. Activer BitLocker sur tous les postes
3. Configurer des politiques de verrouillage automatique
4. Auditer les permissions d'accès aux profils utilisateur

VALEUR PAR DÉFAUT :

Chiffrement DPAPI activé par défaut

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.2.2 *Gestion de la Rétention d'Historique*

MITRE ATT&CK : T1070.003

DESCRIPTION :

Configurer des politiques de rétention appropriées pour l'historique de navigation balançant besoins d'audit sécurité et confidentialité des utilisateurs.

```
# Vérifier la configuration de rétention d'historique
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "HistoryDeletionEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "BrowsingDataLifetime"
```

REMÉDIATION :

1. Définir une durée de rétention selon la politique d'entreprise (ex: 90 jours)
2. Autoriser/interdire la suppression manuelle selon les besoins d'audit
3. Configurer l'archivage automatique pour la conformité
4. Équilibrer surveillance sécurité et respect de la vie privée

VALEUR PAR DÉFAUT :

Rétention illimitée avec suppression manuelle autorisée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.2.3 *Protection contre l'Exfiltration de Données*

MITRE ATT&CK : T1041

DESCRIPTION :

Implémenter des contrôles pour prévenir l'exfiltration des données de navigation via la synchronisation non autorisée ou l'export vers des services externes.

```
# Vérifier les contrôles d'exfiltration
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SyncDisabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CloudPrintProxyEnabled"
```

REMÉDIATION :

1. Désactiver la synchronisation non-contrôlée : `SyncDisabled = 1`
2. Bloquer les services d'impression cloud non-autorisés
3. Contrôler l'accès aux APIs d'export de données
4. Surveiller les tentatives de synchronisation externe

VALEUR PAR DÉFAUT :

Synchronisation autorisée si utilisateur connecté

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.2.4 *Audit des Accès aux Données Sensibles*

MITRE ATT&CK : T1555.003

DESCRIPTION :

Mettre en place un audit complet des accès aux données sensibles stockées par Chrome (mots de passe, certificats, données de formulaires) pour la détection d'intrusion.

```
# Vérifier l'audit d'accès aux données
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DataAuditEnabled"
Get-EventLog -LogName Security -Source "Chrome" | Select-Object -First 10
```

REMÉDIATION :

1. Activer l'audit détaillé des accès aux données Chrome
2. Configurer des alertes pour les accès inhabituels
3. Intégrer avec les outils SIEM pour corrélation
4. Créer des rapports d'audit réguliers

VALEUR PAR DÉFAUT :

Audit basique système activé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.2.5 *Nettoyage Automatique des Données Temporaires*

MITRE ATT&CK : T1070.003

DESCRIPTION :

Configurer le nettoyage automatique des données temporaires (cache, cookies temporaires, données de formulaires) pour réduire la surface d'attaque et les fuites de données.

```
# Vérifier le nettoyage automatique
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ClearBrowsingDataOnExit"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "BrowsingDataLifetime"
```

REMÉDIATION :

1. Configurer le nettoyage à la fermeture pour les données non-critiques
2. Définir des intervalles de nettoyage automatique appropriés
3. Préserver les données nécessaires aux applications métier
4. Documenter les exceptions de nettoyage

VALEUR PAR DÉFAUT :

Nettoyage manuel uniquement

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.2.6 *Encryption at Rest pour Données Navigation Enterprise*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Chiffrement données stockées localement avec clés enterprise

AUDIT :

:

- chrome://policy/ → DiskCacheSize configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

5.2.7 *Memory Protection contre Cold Boot Attacks*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Protection mémoire contre récupération données sensibles

AUDIT :

:

- chrome://policy/ → MemoryPressureThresholdMB configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

5.3 — Mode Navigation Privée et Incognito

5.3.1 *Contrôle d'Accès au Mode Incognito*

MITRE ATT&CK : T1070.003

DESCRIPTION :

Configurer l'accès au mode Incognito selon la politique d'entreprise, balançant besoins de confidentialité utilisateur et exigences d'audit sécurité.

```
# Vérifier la politique du mode Incognito
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "IncognitoModeAvailability"
```

REMÉDIATION :

1. Évaluer les besoins métier vs. exigences d'audit
2. Configurer selon la politique : 0=autorisé, 1=désactivé, 2=forcé
3. Documenter la justification de la configuration choisie
4. Sensibiliser sur les implications sécurité du mode privé

VALEUR PAR DÉFAUT :

Mode Incognito disponible

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.3.2 *Limitation des Extensions en Mode Privé*

MITRE ATT&CK : T1176

4.3.6 *Enterprise Vault Integration (CyberArk, HashiCorp)*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Intégration coffres-forts entreprise avec rotation auto

AUDIT :

:

- chrome://policy/ → PasswordManagerEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

4.3.7 *Privileged Access Management (PAM) Integration*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Intégration PAM pour comptes privilégiés

AUDIT :

:

- chrome://policy/ → ExtensionInstallForcelist configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

DESCRIPTION :

Contrôler quelles extensions peuvent s'exécuter en mode Incognito pour prévenir la collecte de données dans un contexte supposé privé.

```
# Vérifier les extensions autorisées en mode privé
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "IncognitoModeExtensions"
```

REMÉDIATION :

1. Définir une whitelist des extensions autorisées en mode privé
2. Bloquer par défaut toutes les extensions non-essentielles
3. Auditer les permissions des extensions autorisées
4. Documenter les exceptions et leur justification

VALEUR PAR DÉFAUT :

Extensions autorisées selon leurs paramètres individuels

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.3.3 *Monitoring des Sessions Privées*

MITRE ATT&CK : T1070.003

DESCRIPTION :

Mettre en place une surveillance appropriée des sessions privées pour détecter les abus tout en respectant les attentes de confidentialité.

```
# Vérifier la surveillance des sessions privées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "PrivateSessionMonitoring"
```

REMÉDIATION :

1. Définir les métriques de surveillance autorisées (fréquence, durée)
2. Éviter la collecte de contenu spécifique
3. Monitorer les patterns d'usage anormaux
4. Respecter les réglementations sur la confidentialité

VALEUR PAR DÉFAUT :

Surveillance limitée en mode privé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.3.4 *Protection contre les Fuites de Données Privées*

MITRE ATT&CK : T1041

DESCRIPTION :

S'assurer que les données des sessions privées ne fuient pas vers les sessions normales ou les services de synchronisation cloud.

```
# Vérifier l'isolation des données privées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "IncognitoDataIsolation"
```

REMÉDIATION :

1. Vérifier l'isolation stricte entre sessions privées et normales
2. S'assurer de la non-synchronisation des données privées
3. Auditer les mécanismes de nettoyage post-session privée
4. Tester l'absence de persistence des données privées

VALEUR PAR DÉFAUT :

Isolation des données privées activée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

5.3.5 *Éducation et Sensibilisation Mode Privé*

MITRE ATT&CK : T1070.003

DESCRIPTION :

Éduquer les utilisateurs sur les vraies capacités et limitations du mode Incognito pour éviter les fausses attentes de sécurité et anonymat.

```
# Vérifier les matériaux de formation
Test-Path "C:\Training\ChromePrivacyTraining.pdf"
Get-ScheduledTask | Where-Object {$_.TaskName -like "*Privacy*Training*"}
```

REMÉDIATION :

1. Créer des matériaux de formation clairs sur les limitations du mode privé
2. Expliquer ce qui est et n'est pas protégé en mode Incognito
3. Sensibiliser sur la visibilité réseau et des administrateurs système
4. Promouvoir l'utilisation d'outils appropriés pour la vraie anonymisation

VALEUR PAR DÉFAUT :

Pas de formation spécifique sur le mode privé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

Section 6 — EXTENSIONS & ADD-ONS

6.1 — Gestion de l'Installation d'Extensions

6.1.1 *Configuration de la Liste Blanche d'Extensions*

MITRE ATT&CK : T1176

DESCRIPTION :

Implémenter une liste blanche stricte des extensions autorisées pour empêcher l'installation d'extensions malveillantes ou non-validées qui pourraient compromettre la sécurité du navigateur.

```
# Vérifier la liste blanche d'extensions
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallWhitelist"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallBlacklist"
```

REMÉDIATION :

1. Configurer `ExtensionInstallBlacklist` avec "*" pour bloquer toutes les extensions par défaut
2. Définir `ExtensionInstallWhitelist` avec les ID des extensions approuvées uniquement
3. Documenter le processus d'approbation des nouvelles extensions
4. Réviser trimestriellement la liste des extensions autorisées

VALEUR PAR DÉFAUT :

Installation libre depuis Chrome Web Store

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

6.1.2 *Force-Installation des Extensions Critiques*

MITRE ATT&CK : T1176

DESCRIPTION :

Déployer automatiquement les extensions de sécurité critiques via force-install pour s'assurer que tous les utilisateurs bénéficient des protections nécessaires sans possibilité de désinstallation.

```
# Vérifier les extensions force-installées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallForcelist"
# Vérifier les extensions installées
Get-ChildItem "C:\Users\*\AppData\Local\Google\Chrome\User Data\Default\Extensions"
```

REMÉDIATION :

1. Identifier les extensions de sécurité critiques (antivirus, DLP, etc.)
2. Configurer `ExtensionInstallForcelist` avec les ID et URLs des extensions
3. Tester le déploiement sur un groupe pilote
4. Surveiller le statut d'installation sur tous les postes

VALEUR PAR DÉFAUT :

Aucune extension force-installée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

6.1.3 *Blocage des Extensions de Développement*

MITRE ATT&CK : T1176

DESCRIPTION :

Empêcher l'installation d'extensions en mode développeur (unpacked) qui contournent les contrôles de sécurité du Chrome Web Store et représentent un risque élevé.

```
# Vérifier le blocage du mode développeur
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DeveloperToolsDisabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallSources"
```

REMÉDIATION :

1. Restreindre `ExtensionInstallSources` au Chrome Web Store uniquement
2. Bloquer l'accès aux outils de développement si non nécessaires
3. Surveiller les tentatives d'installation d'extensions en mode dev
4. Former les développeurs sur les procédures sécurisées

VALEUR PAR DÉFAUT :

Installation depuis sources multiples autorisée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

6.1.4 *Audit et Inventaire des Extensions*

4.4.6 *Dark Web Monitoring Integration*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Monitoring dark web pour credentials compromis

AUDIT :

:

- chrome://policy/ → PasswordProtectionWarningTrigger configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

4.4.7 *Credential Stuffing Attack Protection*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Protection attaques credential stuffing avec rate limiting

AUDIT :

:

- chrome://policy/ → PasswordProtectionLoginURLs configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

MITRE ATT&CK : T1176

DESCRIPTION :

Maintenir un inventaire complet des extensions installées sur tous les postes et effectuer des audits réguliers pour identifier les extensions non-autorisées ou obsolètes.

```
# Générer un inventaire des extensions
$Users = Get-ChildItem "C:\Users" -Directory
foreach ($User in $Users) {
    Get-ChildItem "$($User.FullName)\AppData\Local\Google\Chrome\User Data\Default\Extensions" -Directory
}
```

REMÉDIATION :

1. Créer un script d'inventaire automatisé des extensions
2. Comparer avec la liste des extensions autorisées
3. Générer des alertes pour les extensions non-conformes
4. Programmer des audits mensuels automatisés

VALEUR PAR DÉFAUT :

Pas d'inventaire automatique

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

6.1.5 *Gestion des Mises à Jour d'Extensions*

MITRE ATT&CK : T1176

DESCRIPTION :

Contrôler les mises à jour automatiques des extensions pour s'assurer que les correctifs de sécurité sont appliqués rapidement tout en évitant les régressions non testées.

```
# Vérifier la configuration des mises à jour d'extensions
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionUpdateEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionInstallAllowlist"
```

REMÉDIATION :

1. Activer les mises à jour automatiques pour les extensions de sécurité
2. Configurer un délai de test pour les extensions critiques métier
3. Surveiller les notifications de mise à jour sécurité
4. Maintenir des versions de rollback pour les extensions critiques

VALEUR PAR DÉFAUT :

Mises à jour automatiques activées

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

6.1.6 *Configuration des Extensions Force-Installées*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Installation forcée extensions sécuritaires critiques (antimalware, DLP, monitoring)
AUDIT :
:

- chrome://policy/ → ExtensionInstallForcelist avec extensions sécurité validées
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Liste extensions approuvées + validation sécurité + mise à jour automatique
- Documentation procédures d'exception
- Formation équipes techniques

6.1.7 *Blocage des Extensions de Développement et Test*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Interdiction chargement extensions non-packagées et modes développeur
AUDIT :
:

- chrome://policy/ → DeveloperToolsAvailability = 2 (désactivé)
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Blocage mode développeur + monitoring tentatives + exceptions développeurs
- Documentation procédures d'exception
- Formation équipes techniques

6.1.8 *Contrôle des Sources d'Installation d'Extensions*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Restriction installation extensions aux sources approuvées (Chrome Web Store Enterprise)
AUDIT :
:

- chrome://policy/ → ExtensionAllowedTypes = ["extension", "theme"] uniquement
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Whitelist Chrome Web Store + blocage sideloading + audit sources
- Documentation procédures d'exception
- Formation équipes techniques

6.1.9 *Gestion du Cycle de Vie des Extensions*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Définition sources autorisées installation et mise à jour extensions
AUDIT :
:

- chrome://policy/ → ExtensionInstallSources configuré domaines approuvés
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- URLs sources validées + HTTPS obligatoire + monitoring installations
- Documentation procédures d'exception
- Formation équipes techniques

6.1.10 *Audit et Inventaire Automatisé des Extensions*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Configuration granulaire par extension avec logging et reporting centralisé
AUDIT :
:
- chrome://policy/ → ExtensionSettings avec règles détaillées par extension
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:
- Politique par extension + logs CBCM + alertes violations + inventaire temps réel
- Documentation procédures d'exception
- Formation équipes techniques

6.1.11 *Contrôle Externally Connectable Extensions*

Politique Chrome Enterprise :
Registre Windows :

5.1.6 *Cookie SameSite Policy Strict Enforcement*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Enforcement SameSite strict avec legacy compatibility
AUDIT :
:
- chrome://policy/ → LegacySameSiteCookieBehaviorEnabled configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:
- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

5.1.7 *Cross-Site Request Forgery (CSRF) Protection*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Protection CSRF avec tokens et validation origin
AUDIT :
:
- chrome://policy/ → DefaultCookiesSetting configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:
- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

DESCRIPTION :
: Restriction communications inter-extensions via externally_connectable
AUDIT :
:
- Audit manifests externally_connectable + test communications + monitoring
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:
- Validation communications + whitelist + monitoring + isolation renforcée
- Documentation procédures d'exception
- Formation équipes techniques

6.1.12 *Gestion Native Messaging Extensions*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Contrôle strict native messaging avec applications système

AUDIT :

:

- chrome://policy/ → NativeMessagingAllowlist + audit communications natives
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Whitelist applications natives + signature validation + monitoring
- Documentation procédures d'exception
- Formation équipes techniques

6.2 — Contrôle des Permissions d'Extensions

6.2.1 *Audit des Permissions Accordées*

MITRE ATT&CK : T1176

DESCRIPTION :

Auditer régulièrement les permissions accordées aux extensions installées pour identifier les privilèges excessifs et les risques potentiels d'abuse de permissions.

```
# Analyser les permissions des extensions (nécessite parsing JSON des manifests)
Get-ChildItem "C:\Users\*\AppData\Local\Google\Chrome\User Data\Default\Extensions\*\*\manifest.json"
```

REMÉDIATION :

1. Développer des outils d'analyse automatique des permissions
2. Créer une matrice risque basée sur les types de permissions
3. Réviser les permissions lors de chaque mise à jour d'extension
4. Documenter les permissions critiques acceptées

VALEUR PAR DÉFAUT :

Permissions accordées selon les demandes d'extension

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

6.2.2 *Restriction d'Accès aux Données Sensibles*

MITRE ATT&CK : T1176, T1555.003

DESCRIPTION :

Limiter l'accès des extensions aux données sensibles comme les mots de passe, historique de navigation, cookies et données de formulaires via des politiques strictes.

```
# Vérifier les restrictions d'accès aux données
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionPermissions"
```

REMÉDIATION :

1. Bloquer par défaut l'accès aux APIs sensibles pour toutes les extensions
2. Créer des exceptions explicites pour les extensions métier critiques
3. Surveiller les tentatives d'accès aux données sensibles
4. Implémenter des contrôles de consentement utilisateur

VALEUR PAR DÉFAUT :

Accès selon les permissions demandées par l'extension

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

6.2.3 *Contrôle d'Accès aux APIs Dangereuses*

MITRE ATT&CK : T1176

DESCRIPTION :

Restreindre l'accès des extensions aux APIs potentiellement dangereuses comme webRequest, debugger, management, et nativeMessaging qui permettent des actions privilégiées.

```
# Analyser l'utilisation d'APIs sensibles dans les extensions
# Nécessite analyse des manifests et code des extensions
```

REMÉDIATION :

1. Maintenir une liste noire des APIs dangereuses
2. Exiger une justification métier pour l'accès aux APIs sensibles
3. Limiter le nombre d'extensions avec accès privilégié
4. Surveiller l'utilisation des APIs critiques

VALEUR PAR DÉFAUT :

Accès aux APIs selon les permissions extension

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

6.2.4 *Monitoring des Communications Extension*

MITRE ATT&CK : T1176

DESCRIPTION :

Surveiller les communications réseau et les interactions des extensions pour détecter les comportements malveillants ou les exfiltrations de données non autorisées.

```
# Vérifier la surveillance des extensions
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ExtensionNetworkMonitoring"
```

REMÉDIATION :

1. Activer le monitoring des requêtes réseau des extensions
2. Créer des alertes pour les communications vers des domaines suspects
3. Analyser les patterns de trafic anormaux
4. Intégrer avec les outils de monitoring réseau

VALEUR PAR DÉFAUT :

Monitoring basique des extensions

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

6.2.5 *Sandboxing et Isolation des Extensions*

MITRE ATT&CK : T1176

DESCRIPTION :

S'assurer que les extensions sont correctement isolées les unes des autres et du système hôte pour limiter l'impact en cas de compromission d'une extension.

```
# Vérifier l'isolation des extensions
Get-Process "chrome" | Where-Object {$_.ProcessName -eq "chrome" -and $_.CommandLine -like "*extension*"}
```

REMÉDIATION :

1. Vérifier l'activation du sandboxing des extensions
2. S'assurer de l'isolation des processus d'extensions
3. Limiter les capacités de communication inter-extensions
4. Auditer les mécanismes d'isolation régulièrement

VALEUR PAR DÉFAUT :

Sandboxing de base activé pour les extensions

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

7.0 — CERTIFICATS & TLS

6.2.6 *Restriction Permissions Extensions Runtime*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Contrôle granulaire permissions runtime (géolocalisation, caméra, microphone)

AUDIT :

:

- chrome://policy/ → ExtensionSettings avec permissions spécifiques par extension
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Matrice permissions par extension + principe moindre privilège + audit accès
- Documentation procédures d'exception
- Formation équipes techniques

6.2.7 *Contrôle Access Content Scripts et Injection*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Limitation injection scripts et accès DOM pour extensions autorisées

AUDIT :

:

- Vérification manifest.json extensions + content_scripts restrictions
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Validation manifests + CSP strict + isolation content scripts + monitoring
- Documentation procédures d'exception
- Formation équipes techniques

6.2.8 *Blocage Communications Extensions Externes*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Restriction communications avec serveurs externes et APIs tierces

AUDIT :

:

- Analyse permissions host et activeTab + monitoring traffic réseau extensions
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Whitelist domaines communication + proxy filtrant + analyse traffic + DLP
- Documentation procédures d'exception
- Formation équipes techniques

6.2.9 *Sandboxing Renforcé des Extensions*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Isolation processus extensions avec contrôles accès système strict
AUDIT :
:

- Vérification isolation processus + permissions système + accès fichiers
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Process isolation + restrictions filesystem + monitoring syscalls + alertes
- Documentation procédures d'exception
- Formation équipes techniques

6.2.10 *Monitoring Comportemental Extensions Temps Réel*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Surveillance comportement extensions avec détection anomalies et menaces
AUDIT :
:

- Logs comportement extensions + analyse patterns + alertes déviations
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Baseline comportement + ML détection + quarantaine auto + investigation
- Documentation procédures d'exception
- Formation équipes techniques

7.1 — Configuration TLS et Chiffrement

7.1.1 *Enforcement TLS 1.3 Minimum*

MITRE ATT&CK : T1557.001
DESCRIPTION :
Configurer Chrome pour exiger TLS 1.3 minimum sur toutes les connexions HTTPS et rejeter les protocoles plus anciens vulnérables aux attaques cryptographiques.

```
# Vérifier la version TLS minimum
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SSLVersionMin"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SSLVersionFallbackMin"
```

REMÉDIATION :

1. Configurer `SSLVersionMin = "tls1.2"` au minimum (tls1.3 si supporté partout)
2. Désactiver les protocoles obsolètes (SSL 3.0, TLS 1.0, TLS 1.1)
3. Tester la compatibilité avec les applications d'entreprise
4. Documenter les exceptions temporaires si nécessaires

5.3.6 *Incognito Mode Forensic Residue Analysis*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Analyse résidus forensiques mode privé avec recovery
AUDIT :
:

- chrome://policy/ → IncognitoModeAvailability configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

5.3.7 *Private Browsing DLP Controls*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Contrôles DLP mode navigation privée entreprise

AUDIT :

:

- chrome://policy/ → IncognitoModeAvailability configuré selon baseline sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Configuration selon recommandations CIS Google Chrome v3.0.0
- Documentation procédures d'exception
- Formation équipes techniques

VALEUR PAR DÉFAUT :

TLS 1.2 minimum sur Chrome récent

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

7.1.2 *Configuration des Suites de Chiffrement Sécurisées*

MITRE ATT&CK : T1557.001

DESCRIPTION :

Restreindre les suites de chiffrement autorisées aux algorithmes modernes et sécurisés, en excluant les chiffrements faibles ou compromis.

```
# Vérifier les suites de chiffrement configurées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CipherSuiteBlacklist"
```

REMÉDIATION :

1. Bloquer les suites de chiffrement faibles (RC4, DES, export ciphers)
2. Privilégier AEAD ciphers (AES-GCM, ChaCha20-Poly1305)
3. Désactiver les échanges de clés vulnérables
4. Tester avec les serveurs d'entreprise critiques

VALEUR PAR DÉFAUT :

Suites modernes privilégiées, anciennes encore acceptées

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

7.1.3 *Activation HSTS et Preload*

MITRE ATT&CK : T1557.001

DESCRIPTION :

Activer HTTP Strict Transport Security (HSTS) et utiliser la preload list pour forcer HTTPS sur tous les domaines d'entreprise et empêcher les attaques de downgrade.

```
# Vérifier la configuration HSTS
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "HSTSPolicyBypassList"
# Vérifier chrome://net-internals/#hsts
```

REMÉDIATION :

1. S'assurer qu'aucun domaine d'entreprise n'est dans la bypass list HSTS
2. Ajouter les domaines d'entreprise à la HSTS preload list
3. Configurer HSTS sur tous les serveurs web d'entreprise
4. Tester l'absence de contournement HSTS

VALEUR PAR DÉFAUT :

HSTS respecté, preload list activée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

7.1.4 *Certificate Transparency et CT Logs*

MITRE ATT&CK : T1557.001

DESCRIPTION :

Activer et surveiller Certificate Transparency pour détecter les certificats frauduleux émis pour les domaines d'entreprise et prévenir les attaques man-in-the-middle.

```
# Vérifier la configuration Certificate Transparency
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CertificateTransparencyEnforcementDisabledForUrls"
```

REMÉDIATION :

1. Éviter de désactiver CT sauf cas critique documenté
2. Surveiller les CT logs pour les certificats d'entreprise
3. Configurer des alertes pour nouveaux certificats détectés
4. Intégrer avec les outils de monitoring SSL/TLS

VALEUR PAR DÉFAUT :

Certificate Transparency activé par défaut

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

7.1.5 *Gestion des Erreurs de Certificat*

MITRE ATT&CK : T1557.001

DESCRIPTION :

Configurer Chrome pour traiter strictement les erreurs de certificat SSL/TLS et empêcher les contournements non autorisés par les utilisateurs.

```
# Vérifier la gestion des erreurs SSL
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SSLErrorOverrideAllowed"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SSLErrorOverrideAllowedForOrigins"
```

REMÉDIATION :

1. Désactiver les contournements d'erreur SSL : `SSLErrorOverrideAllowed = 0`
2. Limiter les exceptions aux domaines internes nécessaires uniquement
3. Sensibiliser les utilisateurs aux risques des erreurs SSL
4. Mettre en place des processus de résolution rapide des problèmes de certificats

VALEUR PAR DÉFAUT :

Contournement d'erreur SSL autorisé avec avertissement

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

8.0 — CONFIDENTIALITÉ & TÉLÉMÉTRIE

7.1.6 *Configuration Certificate Transparency Logging*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Enforcement CT logs pour détecter certificats malveillants ou compromis
AUDIT :
:

- chrome://policy/ → CertificateTransparencyEnforcementDisabledForUrls minimal
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Monitoring CT logs + alertes certificats suspects + révocation automatique
- Documentation procédures d'exception
- Formation équipes techniques

7.1.7 *Gestion des Certificate Revocation Lists (CRL)*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Vérification temps réel statut révocation certificats via OCSP/CRL
AUDIT :
:

- chrome://policy/ → EnableOnlineRevocationChecks = true
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Configuration OCSP stapling + CRL caching + fallback sécurisé
- Documentation procédures d'exception
- Formation équipes techniques

7.1.8 *Configuration des Certificats Clients d'Entreprise*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Sélection automatique certificats clients pour authentification mutuelle TLS
AUDIT :
:

- chrome://policy/ → AutoSelectCertificateForUrls configuré par domaine
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Cartographie certificats par service + rotation automatique + audit accès
- Documentation procédures d'exception
- Formation équipes techniques

7.1.9 *Épinglage de Certificats (Certificate Pinning)*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Épinglage clés publiques services critiques contre attaques MITM
AUDIT :
:

- chrome://policy/ → StaticKeyPinningForUrls pour domaines sensibles
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Pinning services critiques + backup pins + monitoring violations
- Documentation procédures d'exception
- Formation équipes techniques

7.1.10 *Configuration des Protocoles de Sécurité Avancés*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Interdiction fallback vers protocoles SSL/TLS obsolètes ou vulnérables
AUDIT :
:

- chrome://policy/ → SSLVersionFallbackMin = tls1.2 minimum
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Audit compatibilité serveurs + mise à jour infrastructure + exception documentée
- Documentation procédures d'exception
- Formation équipes techniques

7.1.11 *Configuration HTTP Strict Transport Security (HSTS)*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Enforcement HSTS avec preload et protection downgrade attacks
AUDIT :
:

- chrome://policy/ → HSTSPolicyBypassList minimal + test preload + monitoring
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- HSTS strict + preload submission + monitoring bypasses + cert validation
- Documentation procédures d'exception
- Formation équipes techniques

7.1.12 *Validation Certificate Authority (CA) Restreinte*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Restriction CAs autorisées avec pinning et validation étendue
AUDIT :
:

- Liste CAs validées + test validation + monitoring nouvelles CAs + pinning
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- CA whitelist + pinning critique + monitoring + incident response + forensique
- Documentation procédures d'exception
- Formation équipes techniques

8.1 — Contrôle de la Collecte de Données

8.1.1 *Désactivation de la Télémétrie Non-Critique*

MITRE ATT&CK : T1041

DESCRIPTION :

Désactiver la collecte de télémétrie non-essentielle pour limiter l'exposition des données d'usage tout en maintenant les fonctions de sécurité nécessaires.

```
# Vérifier la configuration de télémétrie
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "MetricsReportingEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "UserFeedbackAllowed"
```

REMÉDIATION :

1. Évaluer quelles métriques sont nécessaires pour la sécurité vs. privacy
2. Désactiver la télémétrie non-critique : `MetricsReportingEnabled = 0`
3. Maintenir les rapports de sécurité critiques
4. Documenter les données collectées et leur finalité

VALEUR PAR DÉFAUT :

Télémétrie basique activée

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

8.1.2 *Contrôle des Rapports de Crash*

MITRE ATT&CK : T1041

DESCRIPTION :

Configurer l'envoi des rapports de crash pour équilibrer les besoins de débogage sécurité et la protection des données potentiellement sensibles contenues dans les dumps.

```
# Vérifier la configuration des rapports de crash
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ChromeCleanupReportingEnabled"
```

REMÉDIATION :

1. Activer les rapports de crash pour la sécurité uniquement
2. S'assurer de l'anonymisation des données sensibles
3. Configurer un serveur interne de collecte si nécessaire
4. Limiter les informations incluses dans les rapports

VALEUR PAR DÉFAUT :

Rapports de crash activés

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

9.0 — ISOLATION DES SITES & SANDBOXING

8.1.3 *Désactivation Privacy Sandbox et Topics API*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Désactivation APIs publicitaires Privacy Sandbox (Topics, FLEDGE, Attribution)

AUDIT :

:

- chrome://policy/ → PrivacySandboxAdsAPIsEnabled = false
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Désactivation complète APIs + audit données collectées + purge historiques
- Documentation procédures d'exception
- Formation équipes techniques

8.1.4 *Contrôle Collecte Métriques Utilisateur (UMA)*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Désactivation télémétrie usage et métriques utilisateur non-essentielles

AUDIT :

:

- chrome://policy/ → MetricsReportingEnabled = false
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Blocage métriques + audit data flows + configuration logging local uniquement
- Documentation procédures d'exception
- Formation équipes techniques

8.1.5 *Gestion des Prédictions et Préchargement*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Contrôle prédictions réseau et préchargement pages pour limiter fuites données

AUDIT :

:

- chrome://policy/ → NetworkPredictionOptions = 2 (désactivé)
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Désactivation prédictions + audit traffic + monitoring requests prédictives
- Documentation procédures d'exception
- Formation équipes techniques

8.1.6 *Contrôle Synchronisation Chrome Enterprise*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Restriction synchronisation compte Google avec contrôle comptes entreprise
AUDIT :
:

- chrome://policy/ → BrowserSignin = 1 (force signin) ou 0 (disable)
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Authentification entreprise uniquement + audit sync data + DLP cloud
- Documentation procédures d'exception
- Formation équipes techniques

8.1.7 *Blocage Partage Données Diagnostiques Google*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Désactivation remontée automatique diagnostics et rapports crash vers Google
AUDIT :
:

- chrome://policy/ → CloudReportingEnabled = false
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Reporting local uniquement + serveur crash interne + audit données envoyées
- Documentation procédures d'exception
- Formation équipes techniques

8.1.8 *Contrôle FLoC et Topics API Enterprise*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Désactivation APIs ciblage publicitaire et tracking comportemental
AUDIT :
:

- chrome://policy/ → TopicsAPIEnabled = false + audit data collection
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Désactivation complète APIs + audit privacy + RGPD compliance + documentation
- Documentation procédures d'exception
- Formation équipes techniques

8.1.9 *Gestion Transition Third-Party Cookies*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Préparation phase-out cookies tiers avec Privacy Sandbox alternatives
AUDIT :
:

- Status cookies tiers + alternatives Privacy Sandbox + impact applications
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Migration plan + testing alternatives + timeline + compatibility + monitoring
- Documentation procédures d'exception
- Formation équipes techniques

9.1 — Configuration de l'Isolation Avancée

9.1.1 *Activation de Site Isolation Stricte*

MITRE ATT&CK : T1055

DESCRIPTION :

Activer l'isolation stricte des sites pour s'assurer que chaque origine web s'exécute dans son propre processus, limitant l'impact des vulnérabilités de type Spectre/Meltdown.

```
# Vérifier l'isolation des sites
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SitePerProcess"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "IsolateOrigins"
```

REMÉDIATION :

1. Activer `SitePerProcess = 1` pour isolation complète
2. Configurer `IsolateOrigins` avec les domaines sensibles d'entreprise
3. Monitorer l'impact sur les performances
4. Tester avec les applications web critiques

VALEUR PAR DÉFAUT :

Isolation partielle activée par défaut

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

10.0 — TÉLÉCHARGEMENTS & FICHIERS

9.1.2 *Configuration Site Isolation Stricte par Domaine*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Isolation processus stricte par site avec OOPIF (Out-of-Process iFrames)
AUDIT :
:

- chrome://policy/ → SitePerProcess = true + chrome://process-internals/
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Activation isolation + monitoring processus + test compatibilité applications
- Documentation procédures d'exception
- Formation équipes techniques

9.1.3 *Protection Cross-Origin Read Blocking (CORB)*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Blocage automatique lectures cross-origin suspectes (CORB/CORP)
AUDIT :
:

- Vérification en-têtes CORP + monitoring violations CORB + logs sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Configuration CORP headers + whitelist exceptions + monitoring violations
- Documentation procédures d'exception
- Formation équipes techniques

9.1.4 *Isolation Renderer Processes Avancée*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Protection intégrité code renderer avec Control Flow Guard (CFG)
AUDIT :
:

- chrome://policy/ → RendererCodeIntegrityEnabled = true
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Activation CFG + monitoring violations + mise à jour Windows défense
- Documentation procédures d'exception
- Formation équipes techniques

9.1.5 *Protection Speculative Execution (Spectre/Meltdown)*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Mitigations hardware contre attaques speculative execution

AUDIT :

:

- chrome://policy/ → SpectreVariant2MitigationEnabled = true
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Activation mitigations + mise à jour microcode + performance monitoring
- Documentation procédures d'exception
- Formation équipes techniques

10.1 — Contrôle des Téléchargements

10.1.1 *Restriction des Types de Fichiers Dangereux*

MITRE ATT&CK : T1204.002

DESCRIPTION :

Bloquer automatiquement le téléchargement de types de fichiers potentiellement dangereux (.exe, .bat, .scr, .vbs) sauf exceptions métier documentées.

```
# Vérifier les restrictions de téléchargement
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DownloadRestrictions"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "FileTypeDownloadRestrictions"
```

REMÉDIATION :

1. Configurer `DownloadRestrictions = 1` pour bloquer les fichiers dangereux
2. Créer une liste noire des extensions de fichiers à risque
3. Documenter les exceptions nécessaires au métier
4. Surveiller les tentatives de téléchargement bloquées

VALEUR PAR DÉFAUT :

Avertissement mais téléchargement autorisé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

11.0 — JAVASCRIPT & CONTENU WEB

10.1.2 *Configuration Safe Browsing pour Téléchargements*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Restriction téléchargements par type fichier avec analyse malware temps réel
AUDIT :
:

- chrome://policy/ → DownloadRestrictions configuré + Safe Browsing actif
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Blocage types dangereux + scanning cloud + quarantaine + logs détaillés
- Documentation procédures d'exception
- Formation équipes techniques

10.1.3 *Contrôle Répertoires de Téléchargement*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Restriction téléchargements vers répertoires sécurisés avec monitoring
AUDIT :
:

- chrome://policy/ → DownloadDirectory vers dossier surveillé + permissions
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Dossier sécurisé + antivirus temps réel + audit accès + DLP
- Documentation procédures d'exception
- Formation équipes techniques

10.1.4 *Blocage Téléchargements Sites Non-HTTPS*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Interdiction téléchargements depuis sites HTTP non-sécurisés
AUDIT :
:

- chrome://policy/ → InsecureContentBlockedForUrls = tous domaines HTTP
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Whitelist HTTPS uniquement + exceptions documentées + audit violations
- Documentation procédures d'exception
- Formation équipes techniques

10.1.5 *Analyse Comportementale Téléchargements*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Détection patterns téléchargements suspects avec ML et threat intelligence

AUDIT :

:

- Analyse patterns + corrélation IoCs + detection anomalies volume/type
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Baseline comportement + alertes déviations + investigation automatique
- Documentation procédures d'exception
- Formation équipes techniques

11.1 — Contrôle de l'Exécution JavaScript

11.1.1 *Restriction JavaScript par Site*

MITRE ATT&CK : T1059.007

DESCRIPTION :

Configurer des restrictions JavaScript granulaires par site pour limiter l'exécution de scripts malveillants tout en préservant la fonctionnalité des applications métier.

```
# Vérifier les politiques JavaScript
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DefaultJavaScriptSetting"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "JavaScriptBlockedForUrls"
```

REMÉDIATION :

1. Configurer JavaScript sur "Ask" par défaut pour sites non-fiables
2. Créer une whitelist des domaines d'entreprise autorisés
3. Bloquer JavaScript sur les domaines à risque identifiés
4. Surveiller les demandes d'exécution JavaScript

VALEUR PAR DÉFAUT :

JavaScript autorisé sur tous les sites

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

11.1.2 *Blocage WebAssembly Non-Autorisé*

MITRE ATT&CK : T1059.007

DESCRIPTION :

Contrôler l'exécution de WebAssembly pour prévenir l'utilisation de ce vecteur pour contourner les protections JavaScript et exécuter du code natif.

```
# Vérifier les restrictions WebAssembly
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "WebAssemblyEnabled"
```

REMÉDIATION :

1. Désactiver WebAssembly si non nécessaire : `WebAssemblyEnabled = 0`
2. Si nécessaire, limiter aux domaines d'entreprise de confiance
3. Surveiller l'utilisation de WebAssembly dans les logs
4. Maintenir une liste des applications légitimes utilisant WASM

VALEUR PAR DÉFAUT :

WebAssembly activé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

12.0 — DNS & RÉSEAU

11.1.3 *Configuration Content Security Policy (CSP) Stricte*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Enforcement CSP stricte avec blocage inline scripts et eval()

AUDIT :

:

- Vérification headers CSP + test bypass tentatives + logs violations
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- CSP strict + nonces/hashes + monitoring violations + whitelist minimale
- Documentation procédures d'exception
- Formation équipes techniques

11.1.4 *Restriction Execution WebAssembly (WASM)*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Contrôle strict exécution WebAssembly avec whitelist applications

AUDIT :

:

- chrome://policy/ → DefaultWebAssemblySetting + monitoring WASM loads
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Whitelist applications WASM + signature validation + sandboxing renforcé
- Documentation procédures d'exception
- Formation équipes techniques

11.1.5 *Protection contre JavaScript Malveillant*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Désactivation JIT compilation pour réduire surface attaque

AUDIT :

:

- chrome://policy/ → JavaScriptJitSetting selon policy sécurité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Évaluation performance vs sécurité + monitoring exploits + baseline
- Documentation procédures d'exception
- Formation équipes techniques

12.1 — Configuration DNS Sécurisée

12.1.1 *Activation DNS-over-HTTPS (DoH)*

MITRE ATT&CK : T1557.001

DESCRIPTION :

Configurer DNS-over-HTTPS pour chiffrer les requêtes DNS et prévenir l'interception ou la manipulation des résolutions de noms.

```
# Vérifier la configuration DoH
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DnsOverHttpsMode"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DnsOverHttpsTemplates"
```

REMÉDIATION :

1. Évaluer la compatibilité avec l'infrastructure DNS d'entreprise
2. Configurer DoH avec les serveurs DNS d'entreprise si supporté
3. Tester l'impact sur la résolution des domaines internes
4. Documenter la configuration et les exceptions

VALEUR PAR DÉFAUT :

DoH automatique selon la configuration réseau

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

12.1.2 *Protection contre les Fuites WebRTC IP*

MITRE ATT&CK : T1016

DESCRIPTION :

Configurer Chrome pour empêcher les fuites d'adresses IP locales via WebRTC qui pourraient exposer la topologie réseau interne.

```
# Vérifier la protection WebRTC IP
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "WebRtcIPHandlingPolicy"
```

REMÉDIATION :

1. Configurer `WebRtcIPHandlingPolicy = "default_public_interface_only"`
2. Tester l'impact sur les applications de visioconférence
3. Créer des exceptions pour les outils WebRTC d'entreprise
4. Sensibiliser sur les risques de fuite d'informations réseau

VALEUR PAR DÉFAUT :

Toutes les interfaces réseau exposées via WebRTC

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

13.0 — AUTHENTIFICATION & IDENTITÉ

12.1.3 *Configuration Providers DNS-over-HTTPS Sécurisés*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Configuration fournisseurs DoH validés avec filtering et logging

AUDIT :

:

- chrome://policy/ → DnsOverHttpsTemplates avec providers approuvés uniquement
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Providers validés (Cloudflare for Teams, Quad9) + logs DNS + filtering
- Documentation procédures d'exception
- Formation équipes techniques

12.1.4 *Blocage Fallback DNS Non-Sécurisé*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Enforcement DoH strict sans fallback vers DNS traditionnel non-chiffré

AUDIT :

:

- chrome://policy/ → DnsOverHttpsMode = secure (pas de fallback)
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Mode sécurisé strict + monitoring échecs DNS + backup providers DoH
- Documentation procédures d'exception
- Formation équipes techniques

12.1.5 *Protection WebRTC contre Fuites IP*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Prévention exposition adresses IP locales via WebRTC

AUDIT :

:

- chrome://policy/ → WebRtcIPHandlingPolicy = default_public_interface_only
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Masquage IP locales + test fuites + monitoring connexions WebRTC
- Documentation procédures d'exception
- Formation équipes techniques

12.1.6 *Configuration QUIC Protocol Security*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Contrôle protocole QUIC avec validation sécurité et monitoring

AUDIT :

:

- chrome://policy/ → QuicAllowed selon policy réseau + analyse traffic
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Évaluation QUIC vs TCP/TLS + monitoring protocoles + baseline sécurité
- Documentation procédures d'exception
- Formation équipes techniques

13.1 — Intégration SSO et Authentification

13.1.1 *Configuration SAML/OAuth Enterprise*

MITRE ATT&CK : T1556

DESCRIPTION :

Configurer l'intégration avec les systèmes d'authentification d'entreprise (SAML, OAuth, ADFS) pour l'authentification unique sécurisée.

```
# Vérifier la configuration SSO
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AuthServerWhitelist"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "AuthNegotiateDelegateWhitelist"
```

REMÉDIATION :

1. Configurer les serveurs d'authentification autorisés
2. Activer l'authentification intégrée pour les domaines d'entreprise
3. Configurer la délégation Kerberos appropriée
4. Tester l'authentification automatique sur les applications critiques

VALEUR PAR DÉFAUT :

Authentification manuelle requise

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

14.0 — MODE KIOSK & RESTRICTIONS

13.1.2 *Configuration Kerberos et Authentification Windows*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Intégration Kerberos sécurisée avec delegation contrôlée

AUDIT :

:

- chrome://policy/ → AuthServerAllowlist + AuthNegotiateDelegateAllowlist
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Serveurs Kerberos validés + delegation restreinte + audit authentifications
- Documentation procédures d'exception
- Formation équipes techniques

13.1.3 *Support WebAuthn et FIDO2 Enterprise*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Authentification forte WebAuthn avec clés sécurité matérielles

AUDIT :

:

- Test WebAuthn + vérification policies attestation + registre clés
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Déploiement clés FIDO2 + policies attestation + backup recovery
- Documentation procédures d'exception
- Formation équipes techniques

13.1.4 *Restriction NTLM et Authentifications Legacy*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Désactivation NTLM v1 et protocoles authentification obsolètes

AUDIT :

:

- chrome://policy/ → NtlmV2Enabled = true + audit protocoles legacy
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Migration Kerberos + désactivation NTLM v1 + monitoring authentifications
- Documentation procédures d'exception
- Formation équipes techniques

13.1.5 *Intégration Certificate-Based Authentication*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Authentification par certificats clients avec sélection automatique

AUDIT :

:

- Test authentification certificats + vérification sélection auto + logs
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- PKI entreprise + sélection auto certificats + révocation + audit
- Documentation procédures d'exception
- Formation équipes techniques

14.1 — Restrictions d'Utilisation

14.1.1 *Configuration Mode Kiosk Sécurisé*

MITRE ATT&CK : T1562

DESCRIPTION :

Configurer le mode kiosk pour les postes publics ou à usage restreint avec limitations d'accès appropriées et reset automatique des sessions.

```
# Vérifier la configuration kiosk
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "KioskModeEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "RestrictSigninToPattern"
```

REMÉDIATION :

1. Activer le mode kiosk pour les postes publics appropriés
2. Configurer l'URL de démarrage et les restrictions de navigation
3. Désactiver les fonctionnalités non nécessaires (téléchargements, extensions)
4. Programmer le reset automatique des sessions

VALEUR PAR DÉFAUT :

Mode kiosk désactivé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

15.0 — CHROME ENTERPRISE FEATURES

14.1.2 *Configuration Sécurisée Mode Kiosk Multi-App*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Restriction applications autorisées en mode kiosk avec sandboxing renforcé
AUDIT :
:

- chrome://policy/ → KioskAppId + validation applications + test breakout
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Liste applications validées + sandboxing + monitoring tentatives évasion
- Documentation procédures d'exception
- Formation équipes techniques

14.1.3 *Verrouillage Interface Utilisateur Kiosk*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Désactivation accès menus système et raccourcis clavier dangereux
AUDIT :
:

- Test raccourcis (Alt+F4, Ctrl+Alt+Del, Win+R) + menus contextuels
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Blocage raccourcis + interface locked + monitoring inputs + tamper detection
- Documentation procédures d'exception
- Formation équipes techniques

14.1.4 *Monitoring et Alertes Mode Kiosk*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Surveillance violations tentatives sortie mode kiosk avec alertes temps réel
AUDIT :
:

- Logs violations + monitoring système + alertes tentatives breakout
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- SIEM integration + alertes + intervention automatique + forensique
- Documentation procédures d'exception
- Formation équipes techniques

15.1 — Fonctionnalités Avancées Enterprise

15.1.1 *Chrome Browser Cloud Management (CBCM)*

MITRE ATT&CK : T1484

DESCRIPTION :

Déployer et configurer Chrome Browser Cloud Management pour la gestion centralisée et le reporting avancé des installations Chrome d'entreprise.

```
# Vérifier l'inscription CBCM
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "CloudManagementEnrollmentToken"
```

REMÉDIATION :

1. Obtenir et déployer le token d'enrollment CBCM
2. Configurer les politiques centralisées via Google Admin Console
3. Activer le reporting et monitoring avancé
4. Former les administrateurs à l'interface CBCM

VALEUR PAR DÉFAUT :

CBCM non configuré

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

16.0 — DEVTOOLS & DEBUG

15.1.2 *Configuration Chrome Enterprise Premium*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Activation fonctionnalités Premium avec DLP et threat protection avancée
AUDIT :
:

- Vérification licence Premium + DLP rules actives + threat detection
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Licence Premium + configuration DLP + rules métier + monitoring violations
- Documentation procédures d'exception
- Formation équipes techniques

15.1.3 *Device Trust Connector Configuration*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Intégration Device Trust pour validation conformité endpoints
AUDIT :
:

- Status Device Trust + compliance checks + device attestation
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Déploiement connector + policies compliance + monitoring devices
- Documentation procédures d'exception
- Formation équipes techniques

15.1.4 *Chrome Browser Cloud Management Analytics*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Enforcement enrollment CBCM avec analytics et reporting avancé
AUDIT :
:

- Status enrollment + analytics data + compliance dashboard + policies sync
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Enrollment forcé + dashboard monitoring + KPIs sécurité + alertes
- Documentation procédures d'exception
- Formation équipes techniques

16.1 — Restriction des Outils de Développement

16.1.1 *Désactivation DevTools pour Utilisateurs Standard*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Désactiver l'accès aux outils de développement Chrome pour les utilisateurs non-développeurs afin de prévenir la manipulation de contenu et l'inspection de données sensibles.

```
# Vérifier la désactivation DevTools
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DeveloperToolsDisabled"
```

REMÉDIATION :

1. Désactiver DevTools : `DeveloperToolsDisabled = 1`
2. Créer des exceptions pour les groupes de développeurs
3. Surveiller les tentatives d'accès aux DevTools
4. Former sur les risques d'exposition de données via DevTools

VALEUR PAR DÉFAUT :

DevTools accessibles via F12

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

17.0 — JOURNALISATION & AUDIT

16.1.2 *Restriction Accès Remote Debugging*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Blocage debugging à distance pour prévenir accès non-autorisé
AUDIT :
:

- chrome://policy/ → RemoteDebuggingAllowed = false + scan ports
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Désactivation remote debugging + monitoring ports + exceptions développeurs
- Documentation procédures d'exception
- Formation équipes techniques

16.1.3 *Contrôle Accès Sources et Console*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Restriction accès sources applications et console JavaScript
AUDIT :
:

- Test F12 + accès sources + console + network tab + audit utilisateurs
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Profils utilisateurs différenciés + audit accès + formation sécurité
- Documentation procédures d'exception
- Formation équipes techniques

16.1.4 *Monitoring Utilisation DevTools*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Surveillance ouverture DevTools avec logging et alertes sécurité
AUDIT :
:

- Logs ouverture DevTools + corrélation utilisateurs + patterns suspects
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Logging local + SIEM integration + alertes + investigation procédures
- Documentation procédures d'exception
- Formation équipes techniques

17.1 — Configuration des Logs de Sécurité

17.1.1 *Activation du Logging Sécurité Avancé*

MITRE ATT&CK : T1562.002

DESCRIPTION :

Activer la journalisation détaillée des événements de sécurité Chrome pour la détection d'incidents et l'analyse forensique.

```
# Vérifier la configuration de logging
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "ChromeCleanupReportingEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SafeBrowsingExtendedReportingEnabled"
```

REMÉDIATION :

1. Activer le reporting détaillé des événements sécurité
2. Configurer la rétention appropriée des logs
3. Intégrer avec les systèmes SIEM d'entreprise
4. Créer des alertes pour les événements critiques

VALEUR PAR DÉFAUT :

Logging basique activé

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

18.0 — CONFORMITÉ & GOUVERNANCE

17.1.2 *Configuration Security Event Reporting*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Reporting événements sécurité vers SIEM avec enrichissement contexte
AUDIT :
:

- Flux logs sécurité + intégration SIEM + format events + corrélations
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- SIEM connector + format CEF/LEEF + enrichissement + use cases détection
- Documentation procédures d'exception
- Formation équipes techniques

17.1.3 *Audit Trail Extensions et Permissions*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Traçabilité complète installations/suppressions extensions avec forensique
AUDIT :
:

- Logs extensions + timeline installations + permissions changes + audit trail
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Logging détaillé + rétention longue + forensique + investigation playbooks
- Documentation procédures d'exception
- Formation équipes techniques

17.1.4 *Network Security Monitoring Integration*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Intégration monitoring réseau avec corrélation traffic et menaces
AUDIT :
:

- Logs network + corrélation DNS/HTTP + IoCs + threat intelligence
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Integration NDR + corrélation + IoCs feeding + automated response
- Documentation procédures d'exception
- Formation équipes techniques

18.1 — Mise en Conformité Réglementaire

18.1.1 *Alignement RGPD et Protection Données*

MITRE ATT&CK : T1041

DESCRIPTION :

S'assurer que la configuration Chrome respecte les exigences RGPD en matière de protection des données personnelles et de contrôle des transferts de données.

```
# Vérifier les contrôles RGPD
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DataLeakPreventionEnabled"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "SyncDisabled"
```

REMÉDIATION :

1. Désactiver les transferts de données non-contrôlés
2. Configurer les politiques de rétention conformes RGPD
3. Documenter les bases légales de traitement des données
4. Implémenter les droits des personnes concernées

VALEUR PAR DÉFAUT :

Configuration non spécifiquement RGPD

Status : ☐ Conforme ☐ Non-conforme ☐ N/A

📊 RÉCAPITULATIF DES CONTRÔLES PAR SECTION

18.1.2 *Conformité ISO 27001 Gestion des Accès*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Alignement contrôles accès Chrome avec exigences ISO 27001:2022

AUDIT :

:

- Audit contrôles A.9 (Access Control) + documentation + évidence conformité
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Mapping contrôles + documentation + audit trail + certification
- Documentation procédures d'exception
- Formation équipes techniques

18.1.3 *Conformité RGPD Protection Données Navigation*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Respect RGPD pour collecte, traitement et rétention données navigation

AUDIT :

:

- Audit flux données + consentement + rétention + droits RGPD + DPO validation
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Privacy by design + consentement + rétention + exercice droits + DPIA
- Documentation procédures d'exception
- Formation équipes techniques

18.1.4 *Conformité NIST Cybersecurity Framework*

Politique Chrome Enterprise :

Registre Windows :

DESCRIPTION :

: Alignement fonctions NIST CSF (Identify, Protect, Detect, Respond, Recover)

AUDIT :

:

- Mapping contrôles NIST + maturity assessment + gaps analysis + roadmap
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :

:

- Implementation NIST functions + continuous monitoring + improvement cycle
- Documentation procédures d'exception
- Formation équipes techniques

18.1.5 *Reporting Conformité Réglementaire Automatisé*

Politique Chrome Enterprise :
Registre Windows :
DESCRIPTION :
: Génération automatique rapports conformité avec métriques et KPIs sécurité
AUDIT :
:

- Dashboards conformité + métriques automatisées + rapport management + audit trail
- Vérification logs événements sécurité
- Test fonctionnel configuration

REMÉDIATION :
:

- Automation reporting + KPIs + dashboards + management reporting + alertes
- Documentation procédures d'exception
- Formation équipes techniques

Tableau de Synthèse des Contrôles
📈 RÉSUMÉ EXÉCUTIF
Synthèse de la Posture Sécurité Chrome Enterprise
Score Global de Maturité
Contrôles Évalués : ___/222
Score de Conformité : ___%
Répartition par Criticité :

- 🔴 **Critiques (83 contrôles) :** ___% conformes
- 🟠 **Élevés (102 contrôles) :** ___% conformes
- 🟡 **Moyens (65 contrôles) :** ___% conformes
- 🟢 **Faibles (60 contrôles) :** ___% conformes

Niveau de Maturité Organisationnel
Votre Niveau Actuel : _____
Top 3 des Risques Critiques Identifiés

1. **[Risque #1]**
2. **Impact :** Très élevé
3. **Probabilité :** [Élevée/Moyenne/Faible]
4. **Contrôles défaillants :** [Liste des contrôles]
5. **Action prioritaire :** [Action recommandée]
    1. **[Risque #2]**
    2. **Impact :** Élevé
    3. **Probabilité :** [Élevée/Moyenne/Faible]
    4. **Contrôles défaillants :** [Liste des contrôles]
    5. **Action prioritaire :** [Action recommandée]
        1. **[Risque #3]**
        2. **Impact :** Élevé
        3. **Probabilité :** [Élevée/Moyenne/Faible]
        4. **Contrôles défaillants :** [Liste des contrôles]
        5. **Action prioritaire :** [Action recommandée]

        ### Roadmap de Remédiation Recommandée
        Phase 1 (0-30 jours) - Urgence Critique
        - Mise à jour Chrome vers version récente
        - Activation Safe Browsing Enhanced Protection
        - Blocage extensions non-autorisées
        - Configuration TLS minimum 1.2/1.3

        Phase 2 (30-90 jours) - Risques Élevés
        - Déploiement GPO/ADMX templates
        - Configuration gestionnaire mots de passe d'entreprise
        - Mise en place monitoring sécurité
        - Formation utilisateurs

        Phase 3 (90-180 jours) - Optimisation
        - Intégration SIEM/SOAR
        - Automatisation réponse incidents
        - Certification conformité réglementaire
        - Audit et amélioration continue

        # 🗺️ MAPPING RÉFÉRENTIELS SÉCURITÉ
        ## Alignement NIST Cybersecurity Framework
        ## Mapping ISO 27001:2022
        ## Correspondance MITRE ATT&CK
        # 📋 TEMPLATE PLAN DE REMÉDIATION
        ## Modèle de Plan d'Action Sécuritaire
        ### Informations Générales
        ### Priorisation des Actions
        ### Phases de Déploiement
        Phase 1 : Sécurisation d'Urgence (J+0 à J+30)

- [ ] Action 1
- [ ] Action 2
- [ ] Action 3

Phase 2 : Renforcement (J+30 à J+90)

- [ ] Action 1
- [ ] Action 2
- [ ] Action 3

Phase 3 : Optimisation (J+90 à J+180)

- [ ] Action 1
- [ ] Action 2
- [ ] Action 3

Métriques de Suivi

📞 SUPPORT ET CONTACT

AYI NEDJIMI CONSULTANTS

Siège Social : [Adresse complète]

Téléphone : +33 (0)X XX XX XX XX

Email : contact@ayi-nedjimi-consultants.com

Site Web : www.ayi-nedjimi-consultants.com

Services Associés

- **Audit de Sécurité Chrome Enterprise**
- **Implémentation Politiques GPO/Intune**
- **Formation Sécurité Navigateurs**
- **Support Incident Response**
- **Consulting Conformité RGPD/NIS2**

Équipe Spécialisée

- **Lead Consultant Sécurité :** [Nom]
- **Expert Chrome Enterprise :** [Nom]
- **Spécialiste Conformité :** [Nom]
- **Architecte Sécurité :** [Nom]

Document Version : 1.0

Dernière Mise à Jour : 2026-04-04

Prochaine Révision : 2026-07-04

FIN DU CHECKLIST SÉCURITÉ GOOGLE CHROME ENTERPRISE

Annexe : Checklist (222 controles)

#	Recommandation	Niveau	Oui	Non	N/A
Section 1 — MISES À JOUR & VERSIONING					
1.1.1	Configuration du Canal de Mise à Jour Stable	●	☐	☐	☐
1.1.2	Activation des Mises à Jour Automatiques	●	☐	☐	☐
1.1.3	Contrôle de Version Minimum Autorisée	●	☐	☐	☐
1.1.4	Blocage des Versions de Développement	●	☐	☐	☐
1.1.5	Gestion des Rollbacks de Version	●	☐	☐	☐
1.1.6	Configuration Canary Channel Monitoring pour Early Warning	●	☐	☐	☐
1.1.7	Beta Channel Security Testing Integration	●	☐	☐	☐
1.2.1	Monitoring des Versions Déployées	●	☐	☐	☐
1.2.2	Alertes de Sécurité pour Versions Vulnérables	●	☐	☐	☐
1.2.3	Reporting de Conformité Version	●	☐	☐	☐
1.2.4	Gestion des Exceptions de Version	●	☐	☐	☐
1.2.5	Tests de Régression Post-Mise à Jour	●	☐	☐	☐
1.2.6	Automated CVE Scanning pour Chrome Versions	●	☐	☐	☐
1.2.7	Zero-Day Vulnerability Early Warning System	●	☐	☐	☐
1.3.1	Planification des Déploiements de Version	●	☐	☐	☐
1.3.2	Validation Préalable des Versions	●	☐	☐	☐
1.3.3	Gestion des Versions Critiques d'Urgence	●	☐	☐	☐
1.3.4	Documentation des Changements de Version	●	☐	☐	☐
1.3.5	Archivage et Rétention des Versions	●	☐	☐	☐
Section 2 — GESTION DES POLITIQUES GPO/INTUNE					
2.1.1	Installation des Modèles ADMX Chrome Enterprise	●	☐	☐	☐
2.1.2	Validation de la Version des Templates ADMX	●	☐	☐	☐
2.1.3	Configuration du Magasin Central ADMX	●	☐	☐	☐
2.1.4	Gestion des Versions de Templates ADMX	●	☐	☐	☐
2.1.5	Validation de l'Intégrité des Templates	●	☐	☐	☐
2.1.6	ADMX Template Digital Signature Validation	●	☐	☐	☐
2.1.7	Central Store Replication Monitoring	●	☐	☐	☐
2.2.1	Création d'une GPO Dédiée Chrome Sécurité	●	☐	☐	☐
2.2.2	Configuration de la Priorité des GPO	●	☐	☐	☐
2.2.3	Filtrage de Sécurité des GPO Chrome	●	☐	☐	☐
2.2.4	Sauvegarde et Restauration des GPO Chrome	●	☐	☐	☐
2.2.5	Monitoring des Changements de GPO Chrome	●	☐	☐	☐
2.3.1	Configuration des Profils Chrome dans Intune	●	☐	☐	☐
2.3.2	Synchronisation GPO-Intune pour Chrome	●	☐	☐	☐
2.3.3	Gestion des Applications Chrome via Intune	●	☐	☐	☐
2.3.4	Conformité des Appareils Chrome-Intune	●	☐	☐	☐
2.3.5	Reporting Intune pour Chrome Enterprise	●	☐	☐	☐
2.4.1	Activation et Configuration CBCM	●	☐	☐	☐
2.4.2	Politiques de Sécurité CBCM Enterprise	●	☐	☐	☐
2.4.3	Intégration CBCM avec Identity Provider	●	☐	☐	☐
2.4.4	Monitoring et Analytics CBCM	●	☐	☐	☐
2.4.5	Sauvegarde et Réplication des Politiques CBCM	●	☐	☐	☐
Section 3 — NAVIGATION SÉCURISÉE					
3.1.1	Activation de Safe Browsing Standard	●	☐	☐	☐
3.1.2	Configuration de Safe Browsing Protection Renforcée	●	☐	☐	☐
3.1.3	Blocage des Téléchargements Dangereux	●	☐	☐	☐
3.1.4	Configuration des Alertes Phishing	●	☐	☐	☐
3.1.5	Monitoring des Événements Safe Browsing	●	☐	☐	☐
3.1.6	Configuration de la Protection contre les URLs Suspectes	●	☐	☐	☐
3.1.7	Activation de la Protection Renforcée des Mots de Passe	●	☐	☐	☐
3.1.8	Configuration du Scanning Avancé des Téléchargements	●	☐	☐	☐
2.4.6	Configuration Chrome Enterprise Connectors	●	☐	☐	☐
2.4.7	Real-time URL Check Enterprise	●	☐	☐	☐
3.1.9	Blocage des Connexions Non-Sécurisées	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
3.1.10	Protection contre les Attaques de Redirection Malveillante	●	☐	☐	☐
3.2.1	Scanning Antimalware Intégré	●	☐	☐	☐
3.2.2	Quarantaine des Fichiers Suspects	●	☐	☐	☐
3.1.11	Protection Avancée contre Social Engineering	●	☐	☐	☐
3.1.12	Intégration Threat Intelligence Feeds	●	☐	☐	☐
3.2.3	Blocage des Extensions Malveillantes	●	☐	☐	☐
3.2.4	Protection contre les Scripts Malveillants	●	☐	☐	☐
3.2.5	Surveillance des Indicateurs de Compromission	●	☐	☐	☐
3.3.1	Configuration du Filtrage URL Enterprise	●	☐	☐	☐
3.3.2	Blocage des Contenus Mixtes HTTPS/HTTP	●	☐	☐	☐
3.3.3	Restriction des Téléchargements par Type de Fichier	●	☐	☐	☐
3.3.4	Blocage des Pop-ups et Redirections Malveillantes	●	☐	☐	☐
3.3.5	Filtrage des Annonces et Trackers Malveillants	●	☐	☐	☐
3.4.1	Configuration de l'Isolation de Sites Avancée	●	☐	☐	☐
3.4.2	Protection contre les Attaques Spectre/Meltdown	●	☐	☐	☐
3.4.3	Détection des Tentatives d'Exploitation	●	☐	☐	☐
3.4.4	Protection contre les Attaques de Déni de Service	●	☐	☐	☐
3.4.5	Réponse Automatisée aux Incidents de Sécurité	●	☐	☐	☐
3.2.6	Advanced Persistent Threat (APT) Detection	●	☐	☐	☐
3.2.7	Zero-Day Exploit Protection	●	☐	☐	☐
3.5.1	Conservation des Logs de Navigation Sécurisée	●	☐	☐	☐
3.5.2	Intégration avec les Outils SIEM/SOAR	●	☐	☐	☐
3.5.3	Analyse Comportementale des Patterns de Navigation	●	☐	☐	☐
3.5.4	Threat Intelligence et IOC Feeding	●	☐	☐	☐
3.5.5	Reporting et Métriques de Sécurité Navigation	●	☐	☐	☐
3.3.6	Content Security Policy (CSP) Enforcement	●	☐	☐	☐
3.3.7	Subresource Integrity (SRI) Validation	●	☐	☐	☐
Section 4 — GESTION DES MOTS DE PASSE					
4.1.1	Activation Contrôlée du Gestionnaire Intégré	●	☐	☐	☐
4.1.2	Désactivation du Gestionnaire pour Solutions d'Entreprise	●	☐	☐	☐
4.1.3	Configuration du Chiffrement Local des Mots de Passe	●	☐	☐	☐
4.1.4	Audit des Mots de Passe Faibles et Compromis	●	☐	☐	☐
4.1.5	Gestion de la Synchronisation des Mots de Passe	●	☐	☐	☐
4.2.1	Configuration de l'Auto-Complétion Sécurisée	●	☐	☐	☐
3.4.6	Machine Learning Threat Detection	●	☐	☐	☐
3.4.7	Behavioral Analysis Engine	●	☐	☐	☐
4.2.2	Restriction sur Sites Non-HTTPS	●	☐	☐	☐
4.2.3	Gestion des Exceptions d'Auto-Complétion	●	☐	☐	☐
4.2.4	Protection contre les Attaques de Formulaires	●	☐	☐	☐
4.2.5	Audit des Données d'Auto-Complétion	●	☐	☐	☐
4.3.1	Déploiement d'Extensions de Gestionnaires Certifiés	●	☐	☐	☐
4.3.2	Configuration de l'Authentification Unique (SSO)	●	☐	☐	☐
4.3.3	Blocage des Gestionnaires Non-Autorisés	●	☐	☐	☐
3.5.6	Digital Forensics Evidence Collection	●	☐	☐	☐
3.5.7	Incident Response Automation	●	☐	☐	☐
4.3.4	Monitoring des Accès aux Gestionnaires	●	☐	☐	☐
4.3.5	Sauvegarde et Récupération des Politiques de Mots de Passe	●	☐	☐	☐
4.4.1	Activation de la Détection de Fuites Google	●	☐	☐	☐
4.4.2	Intégration avec Have I Been Pwned	●	☐	☐	☐
4.4.3	Monitoring des Tentatives de Réutilisation	●	☐	☐	☐
4.1.6	Password Breach Detection API	●	☐	☐	☐
4.1.7	Enterprise Password Policy Enforcement	●	☐	☐	☐
4.4.4	Blocage des Domaines de Phishing Connus	●	☐	☐	☐
4.4.5	Réponse Automatisée aux Détections de Fuites	●	☐	☐	☐
Section 5 — COOKIES & DONNÉES DE NAVIGATION					
5.1.1	Blocage des Cookies Tiers par Défaut	●	☐	☐	☐
5.1.2	Configuration SameSite Cookie Policy	●	☐	☐	☐
5.1.3	Gestion des Cookies de Session Sécurisés	●	☐	☐	☐
5.1.4	Limitation de la Durée de Vie des Cookies	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
5.1.5	Monitoring des Anomalies de Cookies	●	☐	☐	☐
4.2.6	Form Data Leak Prevention (DLP)	●	☐	☐	☐
4.2.7	Credit Card Data Protection Enhanced	●	☐	☐	☐
5.2.1	Chiffrement du Stockage Local	●	☐	☐	☐
5.2.2	Gestion de la Rétention d'Historique	●	☐	☐	☐
5.2.3	Protection contre l'Exfiltration de Données	●	☐	☐	☐
5.2.4	Audit des Accès aux Données Sensibles	●	☐	☐	☐
5.2.5	Nettoyage Automatique des Données Temporaires	●	☐	☐	☐
5.2.6	Encryption at Rest pour Données Navigation Enterprise	●	☐	☐	☐
5.2.7	Memory Protection contre Cold Boot Attacks	●	☐	☐	☐
5.3.1	Contrôle d'Accès au Mode Incognito	●	☐	☐	☐
5.3.2	Limitation des Extensions en Mode Privé	●	☐	☐	☐
4.3.6	Enterprise Vault Integration (CyberArk, HashiCorp)	●	☐	☐	☐
4.3.7	Privileged Access Management (PAM) Integration	●	☐	☐	☐
5.3.3	Monitoring des Sessions Privées	●	☐	☐	☐
5.3.4	Protection contre les Fuites de Données Privées	●	☐	☐	☐
5.3.5	Éducation et Sensibilisation Mode Privé	●	☐	☐	☐
Section 6 — EXTENSIONS & ADD-ONS					
6.1.1	Configuration de la Liste Blanche d'Extensions	●	☐	☐	☐
6.1.2	Force-Installation des Extensions Critiques	●	☐	☐	☐
6.1.3	Blocage des Extensions de Développement	●	☐	☐	☐
6.1.4	Audit et Inventaire des Extensions	●	☐	☐	☐
4.4.6	Dark Web Monitoring Integration	●	☐	☐	☐
4.4.7	Credential Stuffing Attack Protection	●	☐	☐	☐
6.1.5	Gestion des Mises à Jour d'Extensions	●	☐	☐	☐
6.1.6	Configuration des Extensions Force-Installées	●	☐	☐	☐
6.1.7	Blocage des Extensions de Développement et Test	●	☐	☐	☐
6.1.8	Contrôle des Sources d'Installation d'Extensions	●	☐	☐	☐
6.1.9	Gestion du Cycle de Vie des Extensions	●	☐	☐	☐
6.1.10	Audit et Inventaire Automatisé des Extensions	●	☐	☐	☐
6.1.11	Contrôle Externally Connectable Extensions	●	☐	☐	☐
5.1.6	Cookie SameSite Policy Strict Enforcement	●	☐	☐	☐
5.1.7	Cross-Site Request Forgery (CSRF) Protection	●	☐	☐	☐
6.1.12	Gestion Native Messaging Extensions	●	☐	☐	☐
6.2.1	Audit des Permissions Accordées	●	☐	☐	☐
6.2.2	Restriction d'Accès aux Données Sensibles	●	☐	☐	☐
6.2.3	Contrôle d'Accès aux APIs Dangereuses	●	☐	☐	☐
6.2.4	Monitoring des Communications Extension	●	☐	☐	☐
6.2.5	Sandboxing et Isolation des Extensions	●	☐	☐	☐
Section 7 — CERTIFICATS & TLS					
6.2.6	Restriction Permissions Extensions Runtime	●	☐	☐	☐
6.2.7	Contrôle Access Content Scripts et Injection	●	☐	☐	☐
6.2.8	Blocage Communications Extensions Externes	●	☐	☐	☐
6.2.9	Sandboxing Renforcé des Extensions	●	☐	☐	☐
6.2.10	Monitoring Comportemental Extensions Temps Réel	●	☐	☐	☐
7.1.1	Enforcement TLS 1.3 Minimum	●	☐	☐	☐
5.3.6	Incognito Mode Forensic Residue Analysis	●	☐	☐	☐
5.3.7	Private Browsing DLP Controls	●	☐	☐	☐
7.1.2	Configuration des Suites de Chiffrement Sécurisées	●	☐	☐	☐
7.1.3	Activation HSTS et Preload	●	☐	☐	☐
7.1.4	Certificate Transparency et CT Logs	●	☐	☐	☐
7.1.5	Gestion des Erreurs de Certificat	●	☐	☐	☐
Section 8 — CONFIDENTIALITÉ & TÉLÉMÉTRIE					
7.1.6	Configuration Certificate Transparency Logging	●	☐	☐	☐
7.1.7	Gestion des Certificate Revocation Lists (CRL)	●	☐	☐	☐
7.1.8	Configuration des Certificats Clients d'Entreprise	●	☐	☐	☐
7.1.9	Épinglage de Certificats (Certificate Pinning)	●	☐	☐	☐
7.1.10	Configuration des Protocoles de Sécurité Avancés	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
7.1.11	Configuration HTTP Strict Transport Security (HSTS)	●	☐	☐	☐
7.1.12	Validation Certificate Authority (CA) Restreinte	●	☐	☐	☐
8.1.1	Désactivation de la Télémétrie Non-Critique	●	☐	☐	☐
8.1.2	Contrôle des Rapports de Crash	●	☐	☐	☐
Section 9 — ISOLATION DES SITES & SANDBOXING					
8.1.3	Désactivation Privacy Sandbox et Topics API	●	☐	☐	☐
8.1.4	Contrôle Collecte Métriques Utilisateur (UMA)	●	☐	☐	☐
8.1.5	Gestion des Prédictions et Préchargement	●	☐	☐	☐
8.1.6	Contrôle Synchronisation Chrome Enterprise	●	☐	☐	☐
8.1.7	Blocage Partage Données Diagnostiques Google	●	☐	☐	☐
8.1.8	Contrôle FLoC et Topics API Enterprise	●	☐	☐	☐
8.1.9	Gestion Transition Third-Party Cookies	●	☐	☐	☐
9.1.1	Activation de Site Isolation Stricte	●	☐	☐	☐
Section 10 — TÉLÉCHARGEMENTS & FICHIERS					
9.1.2	Configuration Site Isolation Stricte par Domaine	●	☐	☐	☐
9.1.3	Protection Cross-Origin Read Blocking (CORB)	●	☐	☐	☐
9.1.4	Isolation Renderer Processes Avancée	●	☐	☐	☐
9.1.5	Protection Speculative Execution (Spectre/Meltdown)	●	☐	☐	☐
10.1.1	Restriction des Types de Fichiers Dangereux	●	☐	☐	☐
Section 11 — JAVASCRIPT & CONTENU WEB					
10.1.2	Configuration Safe Browsing pour Téléchargements	●	☐	☐	☐
10.1.3	Contrôle Répertoires de Téléchargement	●	☐	☐	☐
10.1.4	Blocage Téléchargements Sites Non-HTTPS	●	☐	☐	☐
10.1.5	Analyse Comportementale Téléchargements	●	☐	☐	☐
11.1.1	Restriction JavaScript par Site	●	☐	☐	☐
11.1.2	Blocage WebAssembly Non-Autorisé	●	☐	☐	☐
Section 12 — DNS & RÉSEAU					
11.1.3	Configuration Content Security Policy (CSP) Stricte	●	☐	☐	☐
11.1.4	Restriction Execution WebAssembly (WASM)	●	☐	☐	☐
11.1.5	Protection contre JavaScript Malveillant	●	☐	☐	☐
12.1.1	Activation DNS-over-HTTPS (DoH)	●	☐	☐	☐
12.1.2	Protection contre les Fuites WebRTC IP	●	☐	☐	☐
Section 13 — AUTHENTIFICATION & IDENTITÉ					
12.1.3	Configuration Providers DNS-over-HTTPS Sécurisés	●	☐	☐	☐
12.1.4	Blocage Fallback DNS Non-Sécurisé	●	☐	☐	☐
12.1.5	Protection WebRTC contre Fuites IP	●	☐	☐	☐
12.1.6	Configuration QUIC Protocol Security	●	☐	☐	☐
13.1.1	Configuration SAML/OAuth Enterprise	●	☐	☐	☐
Section 14 — MODE KIOSK & RESTRICTIONS					
13.1.2	Configuration Kerberos et Authentification Windows	●	☐	☐	☐
13.1.3	Support WebAuthn et FIDO2 Enterprise	●	☐	☐	☐
13.1.4	Restriction NTLM et Authentifications Legacy	●	☐	☐	☐
13.1.5	Intégration Certificate-Based Authentication	●	☐	☐	☐
14.1.1	Configuration Mode Kiosk Sécurisé	●	☐	☐	☐
Section 15 — CHROME ENTERPRISE FEATURES					
14.1.2	Configuration Sécurisée Mode Kiosk Multi-App	●	☐	☐	☐
14.1.3	Verrouillage Interface Utilisateur Kiosk	●	☐	☐	☐
14.1.4	Monitoring et Alertes Mode Kiosk	●	☐	☐	☐
15.1.1	Chrome Browser Cloud Management (CBCM)	●	☐	☐	☐
Section 16 — DEVTOOLS & DEBUG					
15.1.2	Configuration Chrome Enterprise Premium	●	☐	☐	☐
15.1.3	Device Trust Connector Configuration	●	☐	☐	☐
15.1.4	Chrome Browser Cloud Management Analytics	●	☐	☐	☐
16.1.1	Désactivation DevTools pour Utilisateurs Standard	●	☐	☐	☐
Section 17 — JOURNALISATION & AUDIT					
16.1.2	Restriction Accès Remote Debugging	●	☐	☐	☐
16.1.3	Contrôle Accès Sources et Console	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
16.1.4	Monitoring Utilisation DevTools	●	☐	☐	☐
17.1.1	Activation du Logging Sécurité Avancé	●	☐	☐	☐
Section 18 — CONFORMITÉ & GOUVERNANCE					
17.1.2	Configuration Security Event Reporting	●	☐	☐	☐
17.1.3	Audit Trail Extensions et Permissions	●	☐	☐	☐
17.1.4	Network Security Monitoring Integration	●	☐	☐	☐
18.1.1	Alignement RGPD et Protection Données	●	☐	☐	☐
18.1.2	Conformité ISO 27001 Gestion des Accès	●	☐	☐	☐
18.1.3	Conformité RGPD Protection Données Navigation	●	☐	☐	☐
18.1.4	Conformité NIST Cybersecurity Framework	●	☐	☐	☐
18.1.5	Reporting Conformité Réglementaire Automatisé	●	☐	☐	☐