Checklist Sécurité WINDOWS 11 — POSTE DE TRAVAIL

Ayi NEDJIMI Consultants
ayinedjimi-consultants.fr
v1.0 — 2026-04-04 | **Classification :** CONFIDENTIEL | **Auteur :** AYI NEDJIMI CONSULTANTS · 410 controles

Sommaire

Section 1 — POLITIQUE DE COMPTES ET MOTS DE PASSE

1.0 — POLITIQUE DE COMPTES ET MOTS DE PASSE

1.1.1 *Historique des mots de passe — Conserver au minimum 24 mots de passe*

DESCRIPTION :
L'historique des mots de passe empêche les utilisateurs de réutiliser leurs anciens mots de passe. La configuration recommandée est de conserver au minimum 24 mots de passe dans l'historique, réduisant considérablement le risque de rotation cyclique.

Sur un poste autonome Windows 11, cette politique s'applique au compte administrateur local et aux comptes utilisateurs locaux. Combinée avec un âge minimum (contrôle 1.1.2), elle empêche le contournement par changements rapides successifs.

```
net accounts | Select-String 'Length of password history'
```

AUDIT :

- **Registre :** `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de mot de passe > Conserver l'historique des mots de passe
- **Valeur attendue :** `24 mots de passe mémorisés` (ou plus)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history → `24 passwords remembered`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Mot de passe > Nombre de mots de passe précédents → `24`
    1. **PowerShell :**

```
net accounts /uniquepw:24
```

REMÉDIATION :

1. **Registre :**

```
Utiliser secedit pour configurer : PasswordHistorySize = 24
```

VALEUR PAR DÉFAUT :
0 (aucun historique conservé)

1.1.2 *Âge minimum du mot de passe — Au moins 1 jour*

DESCRIPTION :
L'âge minimum du mot de passe détermine le nombre de jours pendant lesquels un mot de passe doit être utilisé avant modification. La valeur recommandée est d'au moins 1 jour.

Cette politique empêche les utilisateurs de changer immédiatement leur mot de passe plusieurs fois pour revenir à un ancien, contournant la politique d'historique.

```
net accounts | Select-String 'Minimum password age'
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de mot de passe > Durée de vie minimale du mot de passe
- **Valeur attendue :** `1 jour` (ou plus)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age → `1 day`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Mot de passe > Âge minimum → `1`
    1. **PowerShell :**

```
net accounts /minpwage:1
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secedit ou GPO
```

VALEUR PAR DÉFAUT :
0 (aucune restriction)

1.1.3 *Âge maximum du mot de passe — Au plus 365 jours*

DESCRIPTION :
L'âge maximum détermine la durée maximale d'utilisation d'un mot de passe. La valeur recommandée est de 365 jours maximum. Note : Microsoft et le NIST SP 800-63B recommandent désormais de ne pas imposer de rotation obligatoire sauf compromission avérée.

Le benchmark CIS maintient cette recommandation pour les postes autonomes. L'organisation doit évaluer cette politique en fonction de son contexte de risque.

```
net accounts | Select-String 'Maximum password age'
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de mot de passe > Durée de vie maximale du mot de passe
- **Valeur attendue :** `365 jours` (ou moins)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age → `365 days`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Mot de passe > Âge maximum → `365`
    1. **PowerShell :**

```
net accounts /maxpwage:365
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secedit ou GPO
```

VALEUR PAR DÉFAUT :
42 jours

1.1.4 *Longueur minimale du mot de passe — Au moins 14 caractères*

DESCRIPTION :
La longueur minimale est l'un des paramètres les plus importants. La valeur recommandée est de 14 caractères minimum, conformément aux recommandations CIS et ANSSI.

Un mot de passe de 14 caractères offre une résistance significative contre les attaques par force brute et les tables arc-en-ciel. L'ANSSI recommande 12 caractères minimum (16 pour les comptes à privilèges). Sur Windows 11, cette mesure protège les comptes locaux contre les attaques hors ligne sur le fichier SAM.

```
net accounts | Select-String 'Minimum password length'
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de mot de passe > Longueur minimale du mot de passe
- **Valeur attendue :** `14 caractères` (ou plus)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length → `14`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Mot de passe > Longueur minimale → `14`
    1. **PowerShell :**

```
net accounts /minpwlen:14
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secedit : MinimumPasswordLength = 14
```

VALEUR PAR DÉFAUT :
0 (aucune exigence)

1.1.5 *Exigences de complexité du mot de passe — Activé*

DESCRIPTION :
Lorsque activée, les mots de passe doivent contenir des caractères d'au moins 3 des 5 catégories : majuscules (A-Z), minuscules (a-z), chiffres (0-9), caractères spéciaux et caractères Unicode. Le mot de passe ne doit pas contenir le nom du compte utilisateur.
Cette exigence augmente considérablement l'espace de recherche pour les attaques par force brute et rend les attaques par dictionnaire moins efficaces.

```
secedit /export /cfg C:\AuditANC\secpol.cfg /quiet
Get-Content C:\AuditANC\secpol.cfg | Select-String 'PasswordComplexity'
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de mot de passe > Le mot de passe doit respecter des exigences de complexité
- **Valeur attendue :** `Activé`

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements → `Enabled`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Mot de passe > Exiger la complexité → `Oui`
    1. **PowerShell :**

```
# Vérification via secedit — PasswordComplexity doit être = 1
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secedit ou GPO uniquement
```

VALEUR PAR DÉFAUT :
Activé

1.1.6 *Relaxation de la longueur minimale des mots de passe — Audit activé*

DESCRIPTION :
Windows 11 introduit le paramètre de relaxation permettant de configurer un audit pour détecter les mots de passe plus courts que la limite recommandée. Ce contrôle est utile en phase de transition vers une politique plus stricte.
Ce paramètre permet d'identifier les comptes à risque avant d'imposer la nouvelle politique de longueur minimale.

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SAM' -Name 'RelaxMinimumPasswordLengthLimits' -ErrorAction SilentlyC
```

AUDIT :

- **Registre :** `HKLM\SYSTEM\CurrentControlSet\Control\SAM\RelaxMinimumPasswordLengthLimits`
- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de mot de passe > Relax minimum password length limits
- **Valeur attendue :** `Activé`

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Relax minimum password length limits → `Enabled`
2. **Intune / MEM :** Non disponible nativement — script de remédiation personnalisé
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SAM' -Name 'RelaxMinimumPasswordLengthLimits' -Value 1 -Type DWord
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SYSTEM\CurrentControlSet\Control\SAM\RelaxMinimumPasswordLengthLimits = 1 (DWORD)
```

VALEUR PAR DÉFAUT :
Non défini

1.1.7 *Stocker les mots de passe en chiffrement réversible — Désactivé*

DESCRIPTION :
Ce paramètre détermine si le système stocke les mots de passe en chiffrement réversible. Si activé, les mots de passe sont effectivement stockés en clair, ce qui constitue une vulnérabilité critique.
Sur un poste Windows 11, il n'existe aucune raison légitime d'activer ce paramètre. Un attaquant compromettant le fichier SAM pourrait récupérer tous les mots de passe en clair.

```
secedit /export /cfg C:\AuditANC\secpol.cfg /quiet
Get-Content C:\AuditANC\secpol.cfg | Select-String 'ClearTextPassword'
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de mot de passe > Stocker les mots de passe en chiffrement réversible
- **Valeur attendue :** `Désactivé`

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption → `Disabled`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Mot de passe > Chiffrement réversible → `Non`
    1. **PowerShell :**

```
# ClearTextPassword doit être = 0 dans secedit
```

REMÉDIATION :

1. **Registre :**

```
ClearTextPassword = 0
```

VALEUR PAR DÉFAUT :
Désactivé

1.2.1 *Durée de verrouillage du compte — Au moins 15 minutes*

DESCRIPTION :
La durée de verrouillage définit le temps pendant lequel un compte reste verrouillé après le seuil de tentatives infructueuses atteint. La valeur recommandée est d'au moins 15 minutes.
Cette mesure contrecarre les attaques par force brute et le password spraying. Une valeur de 0 signifie verrouillage permanent jusqu'à intervention d'un administrateur.

```
net accounts | Select-String 'Lockout duration'
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de verrouillage du compte > Durée de verrouillage
- **Valeur attendue :** `15 minutes` (ou plus, ou `0` pour permanent)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration → `15 minutes`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Verrouillage du compte > Durée → `15`
    1. **PowerShell :**

```
net accounts /lockoutduration:15
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secpol.msc
```

VALEUR PAR DÉFAUT :
Non défini

1.2.2 *Seuil de verrouillage du compte — Au plus 5 tentatives*

DESCRIPTION :
Le seuil détermine le nombre de tentatives échouées avant verrouillage. La valeur recommandée est de 5 tentatives maximum (entre 1 et 5).
Un seuil trop élevé permet les attaques par force brute. Un seuil trop bas (1-2) entraîne des verrouillages accidentels. La valeur de 5 offre un bon compromis.

```
net accounts | Select-String 'Lockout threshold'
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de verrouillage > Seuil de verrouillage
- **Valeur attendue :** `5 tentatives` (ou moins, > 0)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold → `5 invalid logon attempts`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Verrouillage > Tentatives → `5`
    1. **PowerShell :**

```
net accounts /lockoutthreshold:5
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secpol.msc
```

VALEUR PAR DÉFAUT :
0 (désactivé)

1.2.3 *Réinitialisation du compteur de verrouillage — Au moins 15 minutes*

DESCRIPTION :
Ce paramètre détermine le délai après lequel le compteur de tentatives échouées est remis à zéro. La valeur recommandée est d'au moins 15 minutes.
Si trop court, un attaquant pourrait espacer ses tentatives pour éviter le verrouillage. Ce paramètre doit être ≤ à la durée de verrouillage (contrôle 1.2.1).

```
net accounts | Select-String 'Lockout observation window'
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de verrouillage > Réinitialiser le compteur après
- **Valeur attendue :** `15 minutes` (ou plus)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after → `15 minutes`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Verrouillage > Réinitialisation → `15`
    1. **PowerShell :**

```
net accounts /lockoutwindow:15
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secpol.msc
```

VALEUR PAR DÉFAUT :
Non défini

1.2.4 *Verrouillage du compte administrateur intégré — Activé*

DESCRIPTION :
Ce paramètre Windows 11 permet d'appliquer la politique de verrouillage au compte administrateur intégré (RID 500). Par défaut, ce compte n'est pas soumis au verrouillage.
La recommandation CIS est d'activer ce paramètre pour que le compte administrateur soit verrouillé après le nombre de tentatives défini, empêchant les attaques par force brute ciblant spécifiquement ce compte.

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'AdministratorAccountLockout' -ErrorAction SilentlyContin
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de comptes > Stratégie de verrouillage > Verrouillage du compte Administrateur
- **Valeur attendue :** `Activé`

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Allow Administrator account lockout → `Enabled`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Verrouillage > Verrouiller administrateur → `Oui`
    1. **PowerShell :**

```
# Configuration via secpol.msc uniquement
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secpol.msc ou GPO
```

VALEUR PAR DÉFAUT :
Non défini

1.3.1 *Windows Hello — PIN complexe requis (6 caractères minimum)*

DESCRIPTION :
Windows Hello for Business remplace les mots de passe par une authentification forte à deux facteurs liée au TPM. Le PIN Windows Hello ne transite pas sur le réseau, contrairement aux mots de passe.
La recommandation est un PIN complexe d'au moins 6 chiffres (ou alphanumérique) avec biométrie comme facteur complémentaire.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -ErrorAction SilentlyContinue
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity`
- **GUI :** Paramètres > Comptes > Options de connexion > Code PIN (Windows Hello)
- **Valeur attendue :** PIN minimum `6` caractères, complexité activée

REMÉDIATION :

1. **GPO :** Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business\PIN Complexity\Minimum PIN length → `6`
2. **Intune / MEM :** Endpoint Security > Protection du compte > Windows Hello > Longueur minimale PIN → `6`
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'MinimumPINLength' -Value 6 -Type DW
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'RequireDigits' -Value 1 -Type DWord
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity\MinimumPINLength = 6
```

VALEUR PAR DÉFAUT :
PIN 4 chiffres sans complexité

1.3.2 *Windows Hello — Expiration du PIN — 365 jours maximum*

DESCRIPTION :
Ce paramètre contrôle la durée de validité du PIN Windows Hello. Bien que lié au TPM, une rotation périodique réduit la fenêtre d'exploitation en cas de compromission par shoulder surfing.
La recommandation est une expiration de 180 à 365 jours pour les postes autonomes.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'Expiration' -ErrorAction SilentlyCo
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity\Expiration`
- **GUI :** Paramètres > Comptes > Options de connexion > PIN
- **Valeur attendue :** `365` jours ou moins

REMÉDIATION :

1. **GPO :** Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business\PIN Complexity\Expiration → `365`
2. **Intune / MEM :** Endpoint Security > Protection du compte > Windows Hello > Expiration PIN → `365`
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'Expiration' -Value 365 -Type DWord
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity\Expiration = 365
```

VALEUR PAR DÉFAUT :
Non défini (pas d'expiration)

1.3.3 *Windows Hello — Historique du PIN — Au moins 5 PIN*

DESCRIPTION :
L'historique du PIN empêche la réutilisation des anciens PIN. La configuration recommandée est de conserver au moins 5 PIN dans l'historique.
Cette mesure complète la politique d'expiration en garantissant que les utilisateurs ne reviennent pas cycliquement aux mêmes PIN.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'History' -ErrorAction SilentlyConti
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity\History`
- **GUI :** Non accessible via l'interface graphique standard
- **Valeur attendue :** `5` ou plus

REMÉDIATION :

1. **GPO :** Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business\PIN Complexity\History → `5`
2. **Intune / MEM :** Endpoint Security > Protection du compte > Windows Hello > Historique PIN → `5`
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'History' -Value 5 -Type DWord
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity\History = 5
```

VALEUR PAR DÉFAUT :
Non défini

1.3.4 *Windows Hello — Caractères spéciaux requis dans le PIN*

DESCRIPTION :
Ce paramètre détermine si les caractères spéciaux sont requis dans le PIN Windows Hello. Un PIN alphanumérique avec caractères spéciaux offre une meilleure résistance.
Valeur 1 = autorisés, Valeur 2 = requis. Recommandation : au moins autorisés pour les environnements standard, requis pour haute sécurité.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'SpecialCharacters' -ErrorAction Sil
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity\SpecialCharacters`
- **GUI :** Non accessible via GUI standard
- **Valeur attendue :** `1` (autorisés) ou `2` (requis)

REMÉDIATION :

1. **GPO :** Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business\PIN Complexity\Require special characters → `Allowed` ou `Required`
2. **Intune / MEM :** Endpoint Security > Protection du compte > Windows Hello > Caractères spéciaux → `Autorisé`
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'SpecialCharacters' -Value 2 -Type D
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity\SpecialCharacters = 2
```

VALEUR PAR DÉFAUT :
Non défini

1.4.1 *Windows LAPS — Gestion du mot de passe administrateur local activée*

DESCRIPTION :
Windows LAPS est intégré nativement à Windows 11 (21H2+). Il gère automatiquement le mot de passe du compte administrateur local en le changeant régulièrement et en le stockant de manière sécurisée dans Entra ID ou AD.

L'absence de LAPS expose le poste au risque de mot de passe administrateur identique sur tous les postes, facilitant le mouvement latéral après compromission d'un seul poste.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config' -ErrorAction SilentlyContinue
Get-LapsAADPassword -DeviceIds $env:COMPUTERNAME -ErrorAction SilentlyContinue
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config`
- **GUI :** Paramètres > Comptes > Options de connexion > Gestion LAPS
- **Valeur attendue :** LAPS activé et configuré

REMÉDIATION :

1. **GPO :** Computer Configuration\Administrative Templates\System\LAPS\Configure password backup directory → `Azure Active Directory`
2. **Intune / MEM :** Endpoint Security > Protection du compte > Windows LAPS > Activer → `Oui`
    1. **PowerShell :**

```
Get-LapsAADPassword -DeviceIds $env:COMPUTERNAME
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config\BackupDirectory = 1
```

VALEUR PAR DÉFAUT :
Non configuré

1.4.2 *Windows LAPS — Complexité du mot de passe — Niveau 4*

DESCRIPTION :
La complexité du mot de passe LAPS doit être au niveau 4 : majuscules + minuscules + chiffres + caractères spéciaux, avec une longueur d'au moins 15 caractères.

Un mot de passe LAPS faible pourrait être craqué si un attaquant accède au hash stocké dans l'annuaire.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config' -Name 'PasswordComplexity' -ErrorAction Silent
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config\PasswordComplexity`
- **GUI :** Non accessible via GUI
- **Valeur attendue :** `4` avec longueur ≥ 15

REMÉDIATION :

1. **GPO :** Computer Configuration\Administrative Templates\System\LAPS\Password Settings\Password Complexity → `Large letters + small letters + numbers + specials`
2. **Intune / MEM :** Endpoint Security > Protection du compte > Windows LAPS > Complexité → `4`
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config' -Name 'PasswordComplexity' -Value 4 -Type DWor
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config\PasswordComplexity = 4
```

VALEUR PAR DÉFAUT :
Non configuré

1.4.3 *Windows LAPS — Rotation du mot de passe — 30 jours maximum*

DESCRIPTION :
La durée maximale d'utilisation du mot de passe LAPS est recommandée à 30 jours. Une rotation fréquente réduit la fenêtre d'exploitation en cas de compromission.

Sur un poste autonome, le compte administrateur local est souvent le seul compte à privilèges, rendant cette rotation critique.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config' -Name 'PasswordAgeDays' -ErrorAction SilentlyC
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config\PasswordAgeDays`
- **GUI :** Non accessible via GUI
- **Valeur attendue :** `30` jours ou moins

REMÉDIATION :

1. **GPO :** Computer Configuration\Administrative Templates\System\LAPS\Password Settings\Password Age Days → `30`
2. **Intune / MEM :** Endpoint Security > Protection du compte > Windows LAPS > Âge → `30`
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config' -Name 'PasswordAgeDays' -Value 30 -Type DWord
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config\PasswordAgeDays = 30
```

VALEUR PAR DÉFAUT :
Non configuré

1.4.4 *Renommer le compte administrateur intégré*

DESCRIPTION :
Le compte administrateur intégré (RID 500) doit être renommé pour réduire la surface d'attaque. Le nom « Administrateur » est une cible privilégiée pour les attaques automatisées.

Le renommage ne masque pas le RID 500 mais complique les scripts malveillants ciblant le nom par défaut.

```
Get-LocalUser | Where-Object {$_.SID -like '*-500'} | Select-Object Name, Enabled, SID
```

AUDIT :

- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Comptes : Renommer le compte Administrateur
- **Valeur attendue :** Nom différent de `Administrateur` et `Administrator`

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account → `[Nom personnalisé]`
2. **Intune / MEM :** Non disponible — script de remédiation personnalisé
    1. **PowerShell :**

```
Rename-LocalUser -Name 'Administrateur' -NewName 'AdminANC'
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secpol.msc ou GPO
```

VALEUR PAR DÉFAUT :
Administrateur

1.4.5 *Désactiver le compte invité intégré*

DESCRIPTION :
Le compte invité fournit un accès anonyme sans authentification. Il doit être désactivé. Bien que désactivé par défaut sur Windows 11, vérifier qu'il n'a pas été activé manuellement.

Un attaquant avec accès physique pourrait utiliser ce compte pour accéder à des données sensibles.

```
Get-LocalUser -Name 'Invité' -ErrorAction SilentlyContinue | Select-Object Name, Enabled
Get-LocalUser -Name 'Guest' -ErrorAction SilentlyContinue | Select-Object Name, Enabled
```

AUDIT :

- **GUI :** lusrmgr.msc > Utilisateurs > Invité > Propriétés > Le compte est désactivé
- **Valeur attendue :** Compte invité `Désactivé`

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status → `Disabled`
2. **Intune / MEM :** Non disponible — script de remédiation personnalisé
    1. **PowerShell :**

```
Disable-LocalUser -Name 'Invité'
Disable-LocalUser -Name 'Guest'
```

REMÉDIATION :

1. **Registre :**

```
Configuration via lusrmgr.msc ou GPO
```

VALEUR PAR DÉFAUT :
Désactivé

1.4.6 *Renommer le compte invité intégré*

DESCRIPTION :
Le compte invité doit être renommé en plus d'être désactivé. Le renommage ajoute une couche de défense en profondeur contre les tentatives d'activation malveillante.
Bien que le compte doive rester désactivé, le renommage complique les attaques automatisées.

```
Get-LocalUser | Where-Object {$_.SID -like '*-501'} | Select-Object Name, Enabled, SID
```

AUDIT :

- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Comptes : Renommer le compte Invité
- **Valeur attendue :** Nom différent de `Invité` et `Guest`

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account → `[Nom personnalisé]`
2. **Intune / MEM :** Non disponible — script de remédiation personnalisé
    1. **PowerShell :**

```
Rename-LocalUser -Name 'Invité' -NewName 'InviteANC_Off'
```

REMÉDIATION :

1. **Registre :**

```
Configuration via secpol.msc
```

VALEUR PAR DÉFAUT :
Invité

1.5.1 *Verrouillage automatique de l'écran — 15 minutes maximum*

DESCRIPTION :
Le verrouillage automatique après inactivité protège contre les accès physiques non autorisés. La valeur recommandée est 900 secondes (15 minutes) maximum.
Sur un poste portable, cette mesure est critique car les utilisateurs oublient souvent de verrouiller manuellement leur poste.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'InactivityTimeoutSecs' -ErrorAction
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\InactivityTimeoutSecs`
- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Ouverture de session interactive : Limite d'inactivité
- **Valeur attendue :** `900` secondes (15 minutes) ou moins

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit → `900`
2. **Intune / MEM :** Endpoint Security > Stratégie de conformité > Configuration système > Délai d'inactivité → `15 min`
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'InactivityTimeoutSecs' -Value 900 -
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\InactivityTimeoutSecs = 900
```

VALEUR PAR DÉFAUT :
0 (pas de verrouillage auto)

1.5.2 *Exiger Ctrl+Alt+Suppr pour l'ouverture de session — Activé*

DESCRIPTION :
La séquence Ctrl+Alt+Suppr est interceptée par le noyau Windows et ne peut être simulée par un logiciel, protégeant contre les faux écrans de connexion (credential harvesting).
L'activation empêche les attaques de type « faux écran de connexion » où un malware imite l'écran de connexion pour capturer les identifiants.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'DisableCAD' -ErrorAction SilentlyCo
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD`
- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Ouverture de session interactive : Ne pas demander Ctrl+Alt+Suppr
- **Valeur attendue :** `0` (Ctrl+Alt+Suppr requis)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL → `Disabled`
2. **Intune / MEM :** Endpoint Security > Protection du point de terminaison > Ouverture de session > Ctrl+Alt+Suppr → `Oui`
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'DisableCAD' -Value 0 -Type DWord
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD = 0
```

VALEUR PAR DÉFAUT :
1 (non requis)

1.5.3 *Nombre de connexions interactives précédentes à mettre en cache — 4 maximum*

DESCRIPTION :
Ce paramètre contrôle le nombre d'informations de connexion mises en cache localement. La valeur recommandée est de 4 maximum pour les postes autonomes, ou 2 pour les postes à haute sécurité.
Les identifiants mis en cache peuvent être extraits par des outils comme Mimikatz. Réduire ce nombre limite la surface d'attaque, tout en maintenant la capacité de connexion hors ligne pour les postes portables.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' -Name 'CachedLogonsCount' -ErrorAction Silentl
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount`
- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Ouverture de session interactive : Nombre de connexions précédentes à mettre en cache
- **Valeur attendue :** `4` (ou moins)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache → `4`
2. **Intune / MEM :** Non disponible nativement — script de remédiation
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' -Name 'CachedLogonsCount' -Value '4' -Type Str
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount = 4 (REG_SZ)
```

VALEUR PAR DÉFAUT :
10

1.5.4 *Message d'avertissement juridique avant connexion — Configuré*

DESCRIPTION :
Un message d'avertissement juridique doit être affiché avant l'ouverture de session pour informer les utilisateurs des conditions d'utilisation et des conséquences d'un accès non autorisé.

Ce message a une valeur juridique en cas de poursuite pour accès non autorisé. Il doit mentionner que le poste est surveillé et que l'accès non autorisé est interdit.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'LegalNoticeCaption' -ErrorAction Si
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'LegalNoticeText' -ErrorAction Silen
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption`
- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Ouverture de session interactive : Titre/Texte du message
- **Valeur attendue :** Titre et texte configurés avec avertissement juridique

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message title/text for users attempting to log on → `[Texte personnalisé]`
2. **Intune / MEM :** Endpoint Security > Protection du point de terminaison > Messages de connexion
    1. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'LegalNoticeCaption' -Value 'AVERTIS
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'LegalNoticeText' -Value 'Ce système
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption = [Texte]
```

VALEUR PAR DÉFAUT :
Non défini

🔐 SECTION 2 : COMPTES & AUTHENTIFICATION

2.1 — Configuration des comptes utilisateurs

2.1.1 *Désactivation du compte Administrateur intégré*

DESCRIPTION :
Le compte Administrateur intégré (SID S-1-5-21-...-500) doit être désactivé pour réduire la surface d'attaque. Ce compte ne peut pas être supprimé mais peut être désactivé et renommé.

Les attaquants ciblent souvent ce compte car il possède des privilèges élevés par défaut et n'est pas soumis aux politiques de verrouillage de compte.

```
Get-LocalUser -Name 'Administrator' | Select-Object Name, Enabled, Description
Get-WmiObject -Class Win32_UserAccount -Filter "Name='Administrator' AND Domain='$env:COMPUTERNAME'" | Select-Object Name, Disabled
```

AUDIT :

- **CMD :** `net user Administrator`
- **GUI :** lusrmgr.msc > Utilisateurs > Administrateur > Propriétés > Compte est désactivé
- **Valeur attendue :** Enabled = False

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status → Disabled
2. **Intune / MEM :** Device Configuration > Profiles > Windows 10/11 > Device restrictions > General > Built-in Administrator account
3. **PowerShell :**

```
Disable-LocalUser -Name 'Administrator'
# Vérification
Get-LocalUser -Name 'Administrator' | Select-Object Enabled
```

REMÉDIATION :

1. **CMD :**

```
net user Administrator /active:no
```

VALEUR PAR DÉFAUT :
Activé (Enabled)

2.1.2 *Renommage du compte Administrateur intégré*

DESCRIPTION :
Le compte Administrateur intégré doit être renommé pour éviter son identification par des outils d'énumération automatisés. Cette mesure fait partie de la stratégie de sécurité par obscurité.
Même désactivé, le compte reste énumérable par son nom bien connu, d'où l'intérêt de le renommer.

```
Get-LocalUser | Where-Object {$_.SID -like '*-500'} | Select-Object Name, SID, Enabled
Get-WmiObject -Class Win32_UserAccount -Filter "SID LIKE '%-500'" | Select-Object Name, SID
```

AUDIT :

- **Registre :** `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultUserName`
- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Comptes : Renommer le compte administrateur
- **Valeur attendue :** Nom différent de "Administrator"

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account → "[NouveauNom]"
2. **PowerShell :**

```
# Renommer le compte Administrator
Rename-LocalUser -Name 'Administrator' -NewName 'SysAdmin01'
# Vérification
Get-LocalUser | Where-Object {$_.SID -like '*-500'}
```

REMÉDIATION :

1. **Registre :**

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\NewAdministratorName = "SysAdmin01"
```

VALEUR PAR DÉFAUT :
Administrator

2.1.3 *Désactivation du compte Invité intégré*

DESCRIPTION :
Le compte Invité (Guest) doit être désactivé car il permet un accès non authentifié au système. Ce compte présente un risque de sécurité majeur même avec des privilèges limités.
Les attaquants peuvent utiliser ce compte comme point d'entrée initial pour l'escalade de privilèges ou la reconnaissance du système.

```
Get-LocalUser -Name 'Guest' | Select-Object Name, Enabled, Description
Get-WmiObject -Class Win32_UserAccount -Filter "Name='Guest' AND Domain='$env:COMPUTERNAME'" | Select-Object Name, Disabled, SID
```

AUDIT :

- **CMD :** `net user Guest`
- **GUI :** lusrmgr.msc > Utilisateurs > Invité > Propriétés > Compte est désactivé
- **Valeur attendue :** Enabled = False

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status → Disabled
2. **Intune / MEM :** Device Configuration > Profiles > Windows 10/11 > Device restrictions > General > Guest account
3. **PowerShell :**

```
Disable-LocalUser -Name 'Guest'
# Vérification
Get-LocalUser -Name 'Guest' | Select-Object Enabled
```

REMÉDIATION :

1. **CMD :**

```
net user Guest /active:no
```

VALEUR PAR DÉFAUT :
Désactivé par défaut sur Windows 11 Enterprise

2.1.4 *Renommage du compte Invité intégré*

DESCRIPTION :
Le compte Invité doit être renommé même s'il est désactivé, pour éviter son identification lors d'énumérations de comptes. Cette mesure complète la désactivation du compte.

```
Get-LocalUser | Where-Object {$_.SID -like '*-501'} | Select-Object Name, SID, Enabled
Get-WmiObject -Class Win32_UserAccount -Filter "SID LIKE '%-501'" | Select-Object Name, SID
```

AUDIT :

- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Comptes : Renommer le compte invité
- **Valeur attendue :** Nom différent de "Guest"

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account → "[NouveauNom]"
2. **PowerShell :**

```
# Renommer le compte Guest
Rename-LocalUser -Name 'Guest' -NewName 'Visitor01'
# Vérification
Get-LocalUser | Where-Object {$_.SID -like '*-501'}
```

VALEUR PAR DÉFAUT :
Guest

2.2 — Gestion des groupes d'administration

2.2.1 *Limitation des membres du groupe Administrateurs*

DESCRIPTION :
Le groupe Administrateurs local doit contenir le minimum d'utilisateurs nécessaire. Chaque membre de ce groupe a un contrôle total sur le système local.

Une prolifération des comptes administrateurs augmente considérablement les risques de compromission et rend difficile l'audit des actions administratives.

```
Get-LocalGroupMember -Group 'Administrators' | Select-Object Name, PrincipalSource, ObjectClass
Get-WmiObject -Class Win32_GroupUser | Where-Object {$_.GroupComponent -match 'Administrators'} | ForEach-Object {[WMI]$_.PartCompo
```

AUDIT :

- **CMD :** `net localgroup Administrators`
- **GUI :** lusrmgr.msc > Groupes > Administrateurs > Propriétés > Membres
- **Valeur attendue :** Seulement les comptes strictement nécessaires

REMÉDIATION :

1. **Audit des membres actuels :**

```
$AdminMembers = Get-LocalGroupMember -Group 'Administrators'
$AdminMembers | Export-Csv -Path 'C:\Audit\AdminMembers.csv' -NoTypeInformation
```

REMÉDIATION :

1. **Suppression des membres non nécessaires :**

```
# Exemple de suppression (adapter selon vos besoins)
Remove-LocalGroupMember -Group 'Administrators' -Member 'DOMAIN\UserNotNeeded'
```

REMÉDIATION :

1. **Documentation des membres légitimes :**
2. Compte de service local nécessaire
3. Compte d'administration d'urgence
4. Comptes de domaine strictement nécessaires

VALEUR PAR DÉFAUT :
Administrateur local, compte de l'utilisateur initial

2.2.2 *Configuration du groupe Utilisateurs avec privilèges de sauvegarde*

DESCRIPTION :
Le groupe "Opérateurs de sauvegarde" (Backup Operators) doit être vidé ou strictement contrôlé. Ce groupe peut accéder à tous les fichiers pour les sauvegarder, contournant les ACL.

Ce privilège peut être exploité par des attaquants pour accéder à des données sensibles ou pour l'exfiltration de données.

```
Get-LocalGroupMember -Group 'Backup Operators' -ErrorAction SilentlyContinue | Select-Object Name, PrincipalSource
Get-LocalGroup 'Backup Operators' -ErrorAction SilentlyContinue | Select-Object Name, Description
```

AUDIT :

- **CMD :** `net localgroup "Backup Operators"`
- **GUI :** lusrmgr.msc > Groupes > Opérateurs de sauvegarde
- **Valeur attendue :** Aucun membre ou membres strictement contrôlés

REMÉDIATION :

1. **Vider le groupe si non utilisé :**

```
$BackupMembers = Get-LocalGroupMember -Group 'Backup Operators' -ErrorAction SilentlyContinue
foreach ($Member in $BackupMembers) {
    Remove-LocalGroupMember -Group 'Backup Operators' -Member $Member.Name
}
```

REMÉDIATION :

1. **Si des membres sont nécessaires, documenter et justifier chaque attribution**

VALEUR PAR DÉFAUT :
Vide par défaut

2.2.3 *Restriction du groupe Opérateurs de serveur*

DESCRIPTION :
Le groupe "Opérateurs de serveur" (Server Operators) possède des privilèges étendus sur les services système. Ce groupe doit être vidé car il peut démarrer/arrêter des services et accéder aux fichiers système.

Ces privilèges peuvent être exploités pour l'escalade de privilèges ou l'installation de logiciels malveillants via les services.

```
Get-LocalGroupMember -Group 'Server Operators' -ErrorAction SilentlyContinue | Select-Object Name, PrincipalSource
Get-LocalGroup 'Server Operators' -ErrorAction SilentlyContinue | Select-Object Name, Description
```

AUDIT :

- **CMD :** `net localgroup "Server Operators"`
- **Valeur attendue :** Aucun membre

```
$ServerOpMembers = Get-LocalGroupMember -Group 'Server Operators' -ErrorAction SilentlyContinue
foreach ($Member in $ServerOpMembers) {
    Remove-LocalGroupMember -Group 'Server Operators' -Member $Member.Name
}
```

VALEUR PAR DÉFAUT :
Vide par défaut sur Windows 11

2.2.4 *Restriction du groupe Opérateurs d'impression*

DESCRIPTION :
Le groupe "Opérateurs d'impression" (Print Operators) peut gérer les imprimantes et les travaux d'impression. Ce groupe doit être contrôlé car il peut accéder à des documents sensibles.

```
Get-LocalGroupMember -Group 'Print Operators' -ErrorAction SilentlyContinue | Select-Object Name, PrincipalSource
```

REMÉDIATION :
Supprimer les membres non nécessaires du groupe Print Operators.

VALEUR PAR DÉFAUT :
Vide par défaut

2.3 — Configuration de l'ouverture de session

2.3.1 *Configuration de l'écran de verrouillage automatique*

DESCRIPTION :
L'écran de verrouillage automatique doit être configuré pour se déclencher après une période d'inactivité définie. Cette mesure protège contre l'accès non autorisé aux sessions laissées ouvertes.

```
Get-ItemProperty -Path 'HKCU:\Software\Policies\Microsoft\Windows\Control Panel\Desktop' -Name 'ScreenSaveTimeOut' -ErrorAction Sil
Get-ItemProperty -Path 'HKCU:\Software\Policies\Microsoft\Windows\Control Panel\Desktop' -Name 'ScreenSaverIsSecure' -ErrorAction S
```

AUDIT :

- **Registre machine :** `HKLM\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop`
- **Valeur attendue :** ScreenSaveTimeOut ≤ 900 secondes (15 minutes), ScreenSaverIsSecure = 1

REMÉDIATION :

1. **GPO :** User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Screen saver timeout/Password protect screen saver
2. **PowerShell :**

```
# Configuration pour tous les utilisateurs (HKLM)
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop' -Name 'ScreenSaveTimeOut' -Value '900' -Ty
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop' -Name 'ScreenSaverIsSecure' -Value '1' -Ty
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop' -Name 'ScreenSaveActive' -Value '1' -Type
```

VALEUR PAR DÉFAUT :
Non configuré

2.3.2 *Suppression des informations de dernière connexion*

DESCRIPTION :
Les informations de dernière connexion ne doivent pas être affichées à l'écran d'ouverture de session pour éviter la divulgation d'informations sur l'utilisation du système.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'DontDisplayLastUserName' -ErrorActi
```

AUDIT :

- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Ouverture de session interactive : Ne pas afficher le nom de la dernière personne connectée
- **Valeur attendue :** DontDisplayLastUserName = 1

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name → Enabled
2. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'DontDisplayLastUserName' -Value 1 -
```

VALEUR PAR DÉFAUT :
0 (affichage activé)

2.3.3 *Configuration de l'authentification forte (CTRL+ALT+DEL)*

DESCRIPTION :
La séquence sécurisée CTRL+ALT+DEL doit être requise pour l'ouverture de session. Cette séquence ne peut pas être interceptée par des logiciels malveillants au niveau utilisateur.

Cette mesure protège contre les faux écrans de connexion (keyloggers) et garantit l'authentification via le Secure Attention Sequence (SAS).

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'DisableCAD' -ErrorAction SilentlyCo
```

AUDIT :

- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Ouverture de session interactive : Ne pas exiger CTRL+ALT+DEL
- **Valeur attendue :** DisableCAD = 0 (CTRL+ALT+DEL requis)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL → Disabled
2. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'DisableCAD' -Value 0 -Type DWord
```

VALEUR PAR DÉFAUT :
1 (désactivé sur Windows 11 par défaut)

2.4 — Contrôle d'accès et privilèges

2.4.1 *Configuration du Contrôle de Compte Utilisateur (UAC)*

DESCRIPTION :
Le Contrôle de Compte Utilisateur (UAC) doit être configuré au niveau maximum pour empêcher l'élévation silencieuse des privilèges. L'UAC protège contre l'exécution non autorisée d'applications avec des privilèges élevés.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'ConsentPromptBehaviorAdmin' -ErrorA
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'ConsentPromptBehaviorUser' -ErrorAc
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'EnableLUA' -ErrorAction SilentlyCon
```

AUDIT :

- **GUI :** Panneau de configuration > Comptes d'utilisateurs > Modifier les paramètres de contrôle de compte d'utilisateur
- **Valeurs attendues :**
- ConsentPromptBehaviorAdmin = 2 (Demander le consentement sur le bureau sécurisé)
- ConsentPromptBehaviorUser = 3 (Demander les informations d'identification)
- EnableLUA = 1 (UAC activé)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators/standard users
2. **PowerShell :**

```
# Configuration UAC niveau maximum
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'ConsentPromptBehaviorAdmin' -Value
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'ConsentPromptBehaviorUser' -Value 3
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'EnableLUA' -Value 1 -Type DWord
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name 'PromptOnSecureDesktop' -Value 1 -Ty
```

VALEUR PAR DÉFAUT :
UAC activé avec niveau moyen

2.4.2 *Restriction des privilèges SeDebugPrivilege*

DESCRIPTION :
Le privilège "Déboguer les programmes" (SeDebugPrivilege) doit être restreint car il permet l'accès à tous les processus système, y compris ceux protégés.

Ce privilège est particulièrement dangereux car il permet l'injection de code dans n'importe quel processus, contournant la plupart des protections système.

```
# Utiliser secedit pour exporter et vérifier les droits utilisateur
secedit /export /cfg C:\temp\secedit_export.inf
Get-Content C:\temp\secedit_export.inf | Select-String "SeDebugPrivilege"
```

AUDIT :

- **GUI :** secpol.msc > Stratégies locales > Attribution des droits utilisateur > Déboguer les programmes
- **Valeur attendue :** Seulement les comptes strictement nécessaires (généralement aucun)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs → Vide ou comptes spécifiques uniquement
2. **Secedit :**

```
# Créer un fichier de configuration temporaire
echo [Unicode] > C:\temp\debug_config.inf
echo Unicode=yes >> C:\temp\debug_config.inf
echo [Privilege Rights] >> C:\temp\debug_config.inf
echo SeDebugPrivilege = >> C:\temp\debug_config.inf
echo [Version] >> C:\temp\debug_config.inf
echo signature="$CHICAGO$" >> C:\temp\debug_config.inf
echo Revision=1 >> C:\temp\debug_config.inf

# Appliquer la configuration
secedit /configure /db C:\temp\debug.sdb /cfg C:\temp\debug_config.inf
```

VALEUR PAR DÉFAUT :
Administrateurs

2.5.1 *Configuration des comptes de service*

DESCRIPTION :
Les comptes de service doivent être configurés avec les privilèges minimums requis et des mots de passe complexes. Les comptes de service ne doivent pas avoir de droits de connexion interactive.

Cette configuration réduit la surface d'attaque en cas de compromission d'un service et limite les mouvements latéraux potentiels.

```
Get-WmiObject -Class Win32_Service | Where-Object {$_.StartName -notlike "LocalSystem" -and $_.StartName -notlike "NT AUTHORITY\*"}
Get-LocalUser | Where-Object {$_.Description -like "*service*"} | Select-Object Name, Enabled, PasswordRequired
```

```
# Audit des comptes de service
Get-WmiObject -Class Win32_Service | Where-Object {$_.StartName -notlike "LocalSystem"} | ForEach-Object {
    Write-Host "Service: $($_.Name) - Compte: $($_.StartName)"
}

# Configuration des droits utilisateur pour les comptes de service
secedit /export /cfg C:\temp\secedit.cfg
# Éditer le fichier pour ajouter les comptes de service aux droits appropriés
secedit /configure /db C:\temp\secedit.sdb /cfg C:\temp\secedit.cfg
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.6.1 *Contrôle des comptes avec privilèges élevés*

DESCRIPTION :
Les comptes avec des privilèges administratifs doivent être strictement contrôlés, documentés et régulièrement audités. Aucun compte utilisateur standard ne doit avoir des privilèges administratifs permanents.

L'utilisation de comptes privilégiés doit être tracée et justifiée pour maintenir le principe du moindre privilège.

```
Get-LocalGroupMember -Group "Administrators" | Select-Object Name, ObjectClass, PrincipalSource
Get-LocalGroupMember -Group "Power Users" -ErrorAction SilentlyContinue | Select-Object Name
net localgroup Administrators
```

```
# Auditer les membres du groupe Administrateurs
$AdminMembers = Get-LocalGroupMember -Group "Administrators"
foreach ($Member in $AdminMembers) {
    if ($Member.ObjectClass -eq "User" -and $Member.Name -notlike "*Administrator*") {
        Write-Warning "Utilisateur avec privilèges admin: $($Member.Name)"
    }
}

# Supprimer les utilisateurs non autorisés du groupe Administrators
# Remove-LocalGroupMember -Group "Administrators" -Member "DOMAIN\UserName"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.7.1 *Configuration du contrôle de compte utilisateur (UAC)*

DESCRIPTION :
Le contrôle de compte utilisateur (UAC) doit être configuré au niveau maximum pour toutes les élévations de privilèges. Aucune application ne doit contourner les invites UAC.

L'UAC constitue une barrière critique contre l'exécution non autorisée de code avec privilèges élevés.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "ConsentPromptBehaviorAdmin"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "PromptOnSecureDesktop"
```

```
# Configuration UAC niveau maximum
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "ConsentPromptBehaviorAdmin" -Value
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "ConsentPromptBehaviorUser" -Value 3
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableInstallerDetection" -Value 1
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value 1 -Type DWord
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "PromptOnSecureDesktop" -Value 1 -Ty
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableVirtualization" -Value 1 -Typ
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.5.1 *Configuration des comptes de service géré (gMSA)*

DESCRIPTION :
Les comptes de service gérés par groupe (gMSA) doivent être utilisés pour tous les services d'entreprise afin d'automatiser la gestion des mots de passe et réduire les risques de compromission.
Les gMSA éliminent le besoin de gestion manuelle des mots de passe de service et fournissent une rotation automatique sécurisée.

```
Get-ADServiceAccount -Filter * | Select-Object Name, Enabled, ServicePrincipalName
Get-WmiObject -Class Win32_Service | Where-Object {$_.StartName -like "*$"} | Select-Object Name, StartName
```

```
# Créer un compte gMSA
New-ADServiceAccount -Name "WebService-gMSA" -DNSHostName "webservice.domain.com" -ManagedPasswordIntervalInDays 30
# Installer le compte gMSA sur l'hôte
Install-ADServiceAccount -Identity "WebService-gMSA"
# Configurer le service pour utiliser le gMSA
Set-Service -Name "MyService" -Credential (Get-Credential "DOMAIN\WebService-gMSA$")
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.6.1 *Contrôle des sessions utilisateur concurrentes*

DESCRIPTION :
Le nombre de sessions utilisateur concurrentes doit être limité pour éviter l'utilisation abusive des comptes et détecter les connexions non autorisées.
Cette mesure aide à identifier les comptes compromis utilisés simultanément depuis plusieurs emplacements.

```
query user
Get-WmiObject -Class Win32_LoggedOnUser | Group-Object Antecedent | Where-Object {$_.Count -gt 1}
Get-EventLog -LogName Security -InstanceId 4624 -After (Get-Date).AddHours(-1) | Group-Object UserName
```

```
# Configuration via GPO ou registre
New-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name "MaxInstanceCount" -Value 2 -Property
# Surveillance des sessions multiples
Get-WmiObject Win32_LoggedOnUser | Group-Object Antecedent | Where-Object {$_.Count -gt 1} | ForEach-Object {
    Write-Warning "Utilisateur avec sessions multiples: $($_.Name)"
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.7.1 *Configuration de l'authentification multi-facteurs (MFA)*

DESCRIPTION :
L'authentification multi-facteurs doit être activée pour tous les comptes privilégiés et recommandée pour les comptes utilisateur standard.
Le MFA constitue une protection critique contre les attaques par vol de credentials et le phishing.

```
Get-MpComputerStatus | Select-Object AMEngineVersion, AMProductVersion
Get-WindowsOptionalFeature -Online -FeatureName "*Hello*"
certlm.msc # Vérifier les certificats d'authentification
```

```
# Activation de Windows Hello for Business
Enable-WindowsOptionalFeature -Online -FeatureName "WindowsHelloFace" -All
# Configuration des stratégies MFA via GPO
New-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork" -Name "Enabled" -Value 1 -PropertyType DWord -Force
# Configuration des certificats pour l'authentification
certlm.msc
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.8.1 *Audit des privilèges élevés temporaires*

DESCRIPTION :
Tous les privilèges élevés temporaires doivent être auditables, traçables et automatiquement révoqués après expiration.
Cette pratique assure que l'élévation de privilège suit le principe du moindre privilège et de la durée minimale nécessaire.

```
Get-EventLog -LogName Security -InstanceId 4672 -Newest 100 | Select-Object TimeGenerated, Message
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4672} -MaxEvents 50
net localgroup Administrators
```

```
# Configuration d'audit des privilèges spéciaux
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
# Script de révocation automatique des privilèges temporaires
$TempAdmins = @("TempAdmin1", "TempAdmin2")
foreach ($Admin in $TempAdmins) {
    $User = Get-LocalUser -Name $Admin -ErrorAction SilentlyContinue
    if ($User -and $User.PasswordLastSet -lt (Get-Date).AddDays(-1)) {
        Remove-LocalGroupMember -Group "Administrators" -Member $Admin
        Write-Host "Privilège révoqué pour: $Admin"
    }
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.9.1 *Protection contre l'énumération de comptes*

DESCRIPTION :
Les mécanismes d'énumération de comptes doivent être désactivés pour empêcher la reconnaissance par des attaquants.
Cette protection limite la capacité des attaquants à découvrir les comptes valides du système.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RestrictAnonymous"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RestrictAnonymousSAM"
net config server
```

```
# Désactiver l'énumération anonyme
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RestrictAnonymous" -Value 1 -Type DWord
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RestrictAnonymousSAM" -Value 1 -Type DWord
# Désactiver le partage administratif par défaut
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters" -Name "AutoShareWks" -Value 0 -Type DWord
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.10.1 *Configuration des jetons d'authentification*

DESCRIPTION :
Les jetons d'authentification doivent être configurés avec des durées de vie limitées et des mécanismes de révocation appropriés.
Cette configuration limite l'exposition en cas de vol de jetons et force une réauthentification régulière.

```
klist tickets
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters" -ErrorAction SilentlyContinue
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4768,4769} -MaxEvents 20
```

```
# Configuration des durées de vie des tickets Kerberos
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters" -Name "MaxTicketAge" -Value 10 -PropertyTyp
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters" -Name "MaxRenewAge" -Value 7 -PropertyType
# Purger les tickets existants
klist purge
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.11.1 *Surveillance des tentatives d'élévation de privilège*

DESCRIPTION :
Toutes les tentatives d'élévation de privilège doivent être surveillées et alertées en temps réel.
Cette surveillance permet de détecter rapidement les tentatives d'attaque par escalade de privilège.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4672,4673,4674} -MaxEvents 50
Get-EventLog -LogName Security -InstanceId 4648 -Newest 20
auditpol /get /subcategory:"Process Creation"
```

```
# Configuration d'audit pour l'élévation de privilège
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Other Privilege Use Events" /success:enable /failure:enable
# Script de surveillance temps réel
Register-WmiEvent -Query "SELECT * FROM Win32_NTLogEvent WHERE LogFile='Security' AND EventCode=4672" -Action {
    $Event = $Event.SourceEventArgs.NewEvent
    Write-Host "ALERT: Élévation de privilège détectée - User: $($Event.InsertionStrings[1])"
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.12.1 *Gestion des comptes de secours (break-glass)*

DESCRIPTION :
Les comptes de secours doivent être configurés, protégés et auditables pour les situations d'urgence uniquement.
Ces comptes constituent le dernier recours d'accès administratif et doivent être strictement contrôlés.

```
Get-LocalUser | Where-Object {$_.Description -like "*emergency*" -or $_.Description -like "*break*glass*"}
Get-EventLog -LogName Security -InstanceId 4624 | Where-Object {$_.ReplacementStrings[5] -like "*Emergency*"}
net user EmergencyAdmin
```

```
# Création d'un compte de secours
$SecurePassword = ConvertTo-SecureString "Tr3s-C0mpl3x-P@ssw0rd!" -AsPlainText -Force
New-LocalUser -Name "EmergencyAdmin" -Password $SecurePassword -Description "Compte de secours - Utilisation d'urgence uniquement"
# Configuration d'audit spécifique
Add-LocalGroupMember -Group "Administrators" -Member "EmergencyAdmin"
# Désactiver le compte par défaut
Disable-LocalUser -Name "EmergencyAdmin"
Write-Host "IMPORTANT: Activer manuellement uniquement en cas d'urgence"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.13.1 *Contrôle des autorisations de connexion à distance*

DESCRIPTION :
Les autorisations de connexion à distance doivent être strictement contrôlées et limitées aux utilisateurs autorisés uniquement.
Cette restriction limite les vecteurs d'attaque par accès distant non autorisé.

```
Get-LocalGroupMember -Group "Remote Desktop Users"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server" -Name "fDenyTSConnections"
qwinsta
```

```
# Désactiver RDP par défaut
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server" -Name "fDenyTSConnections" -Value 1 -Type DWord
# Vider le groupe Remote Desktop Users
Get-LocalGroupMember -Group "Remote Desktop Users" | ForEach-Object {
    Remove-LocalGroupMember -Group "Remote Desktop Users" -Member $_.Name
}
# Configuration du pare-feu
Disable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.14.1 *Audit des modifications de comptes critiques*

DESCRIPTION :
Toutes les modifications apportées aux comptes administrateurs et privilégiés doivent être auditées et alertées.
Cette surveillance permet de détecter les modifications non autorisées des comptes critiques.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4720,4722,4723,4724,4725,4726} -MaxEvents 50
Get-EventLog -LogName Security -InstanceId 4732,4733 -Newest 20
auditpol /get /subcategory:"User Account Management"
```

```
# Configuration d'audit pour gestion des comptes
auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Security Group Management" /success:enable /failure:enable
# Script de surveillance des comptes critiques
$CriticalAccounts = @("Administrator", "krbtgt", "DefaultAccount")
foreach ($Account in $CriticalAccounts) {
    Register-WmiEvent -Query "SELECT * FROM Win32_NTLogEvent WHERE LogFile='Security' AND (EventCode=4722 OR EventCode=4723) AND Me
        Write-Host "CRITICAL: Modification du compte $Account détectée"
    }
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.15.1 *Protection contre les attaques de type Pass-the-Hash*

DESCRIPTION :
Les mécanismes de protection contre les attaques Pass-the-Hash doivent être activés pour empêcher la réutilisation de hashes de mots de passe.
Cette protection limite les mouvements latéraux après compromission initiale.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "NoLMHash"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" -Name "UseLogonCredential"
```

```
# Désactiver LM et NTLMv1
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel" -Value 5 -Type DWord
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "NoLMHash" -Value 1 -Type DWord
# Désactiver WDigest
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" -Name "UseLogonCredential" -Value 0 -Type
# Activer Protected Process Light (PPL) pour LSASS
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RunAsPPL" -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.16.1 *Configuration des délais d'expiration de session*

DESCRIPTION :
Les sessions inactives doivent être automatiquement fermées après un délai configuré pour réduire l'exposition aux accès non autorisés.
Cette mesure prévient l'utilisation de sessions laissées ouvertes sans surveillance.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "InactivityTimeoutSecs"
Get-ItemProperty -Path "HKCU:\Control Panel\Desktop" -Name "ScreenSaveTimeOut"
Get-ItemProperty -Path "HKCU:\Control Panel\Desktop" -Name "ScreenSaverIsSecure"
```

```
# Configuration du timeout d'inactivité (15 minutes)
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "InactivityTimeoutSecs" -Value 900 -
# Configuration de l'écran de veille sécurisé
Set-ItemProperty -Path "HKCU:\Control Panel\Desktop" -Name "ScreenSaveTimeOut" -Value "900" -Type String
Set-ItemProperty -Path "HKCU:\Control Panel\Desktop" -Name "ScreenSaverIsSecure" -Value "1" -Type String
# Forcer l'application à tous les utilisateurs
reg add "HKU\.DEFAULT\Control Panel\Desktop" /v ScreenSaveTimeOut /t REG_SZ /d 900 /f
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.5.1 *Protection avancée des comptes privilégiés (PAM)*

DESCRIPTION :
Une solution de gestion des accès privilégiés (PAM) doit être implémentée pour tous les comptes administrateurs avec rotation automatique des mots de passe et sessions enregistrées.
Cette mesure constitue un pilier fondamental de la sécurité Zero Trust pour les accès critiques.

```
Get-LocalGroupMember -Group "Administrators" | Where-Object {$_.ObjectClass -eq "User"}
Get-EventLog -LogName Security -InstanceId 4624 | Where-Object {$_.ReplacementStrings[8] -eq "2"}
auditpol /get /subcategory:"Special Logon"
```

```
# Implémentation d'une solution PAM basique
New-LocalUser -Name "PAM-EmergencyAdmin" -Description "Compte PAM d'urgence - Session enregistrée"
$SecurePass = ConvertTo-SecureString (Get-Random -Count 32 -InputObject ([char[]](33..126)) -join "") -AsPlainText -Force
Set-LocalUser -Name "PAM-EmergencyAdmin" -Password $SecurePass
# Configuration de l'audit étendu pour les comptes privilégiés
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
# Script de rotation automatique (à automatiser via tâche planifiée)
Write-Host "Configuration PAM basique terminée - Implémenter solution enterprise (CyberArk, Beyond Trust, etc.)"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.6.1 *Contrôle des élévations UAC via GPO centralisée*

DESCRIPTION :
Toutes les élévations UAC doivent être centralisées, auditées et soumises à des règles granulaires selon l'application et l'utilisateur.
Cette gouvernance centralisée permet un contrôle fin des élévations de privilège.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" | Select-Object *UAC*, *Consent*, *Prompt*
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4688} | Where-Object {$_.Message -like "*UAC*"}
gpresult /h C:\temp\gpo_report.html
```

```
# Configuration UAC granulaire via stratégies de groupe
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "ConsentPromptBehaviorAdmin" -Value
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "ConsentPromptBehaviorUser" -Value 3
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableInstallerDetection" -Value 1
# Liste blanche d'applications autorisées à élever sans prompt
New-Item -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\UAC" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\UAC" -Name "WhitelistedApps" -Value @("msie
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.7.1 *Authentification basée sur les certificats*

DESCRIPTION :
L'authentification par certificats doit être déployée pour tous les comptes sensibles avec révocation centralisée et HSM pour les clés critiques.
Cette méthode offre une authentification forte résistante aux attaques par credential dumping.

```
Get-ChildItem -Path Cert:\CurrentUser\My | Where-Object {$_.EnhancedKeyUsageList -like "*Client Authentication*"}
certlm.msc
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards"
```

```
# Configuration pour l'authentification par certificat
certlm.msc
# Déploiement de certificats utilisateur via GPO
Write-Host "1. Configurer une AC d'entreprise"
Write-Host "2. Créer un modèle de certificat utilisateur"
Write-Host "3. Déployer via GPO: Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies"
# Activation de l'authentification par carte à puce
New-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "scforceoption" -Value 1 -PropertyTy
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.8.1 *Détection des comptes dormants et zombies*

DESCRIPTION :
Les comptes inactifs depuis plus de 90 jours doivent être automatiquement détectés, désactivés et éventuellement supprimés selon la politique de rétention.
Cette pratique réduit la surface d'attaque en éliminant les comptes oubliés potentiellement compromis.

```
Get-LocalUser | Where-Object {$_.LastLogon -lt (Get-Date).AddDays(-90)} | Select-Object Name, LastLogon, Enabled
Get-WmiObject Win32_UserProfile | Where-Object {$_.LastUseTime -lt (Get-Date).AddDays(-90).ToString("yyyyMMddHHmmss.ffffff-000")}
Get-EventLog -LogName Security -InstanceId 4624 -After (Get-Date).AddDays(-90) | Group-Object UserName | Sort-Object Count
```

```
# Script de détection et nettoyage des comptes dormants
$InactiveThreshold = (Get-Date).AddDays(-90)
$DormantAccounts = Get-LocalUser | Where-Object {
    $_.Enabled -eq $true -and
    ($_.LastLogon -lt $InactiveThreshold -or $_.LastLogon -eq $null) -and
    $_.Name -notin @("Administrator", "DefaultAccount", "Guest", "WDAGUtilityAccount")
}
foreach ($Account in $DormantAccounts) {
    Write-Warning "Compte dormant détecté: $($Account.Name) - Dernière connexion: $($Account.LastLogon)"
    # Désactiver le compte (décommenter pour activer)
    # Disable-LocalUser -Name $Account.Name
    # Write-Host "Compte désactivé: $($Account.Name)"
}
# Nettoyage des profils utilisateur orphelins
Get-CimInstance Win32_UserProfile | Where-Object {$_.Special -eq $false -and $_.LastUseTime -lt $InactiveThreshold} | Remove-CimIns
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.9.1 *Surveillance des connexions simultanées suspectes*

DESCRIPTION :
Les connexions simultanées depuis des emplacements géographiquement impossibles doivent être détectées et bloquées automatiquement.
Cette surveillance permet d'identifier les comptes compromis utilisés par des attaquants.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4624} -MaxEvents 100 | Group-Object {$_.Properties[5].Value} | Where-Object
query user
Get-WmiObject Win32_LoggedOnUser | Group-Object Antecedent
```

```
# Surveillance des sessions multiples
$ActiveSessions = query user | Select-String "Active"
if ($ActiveSessions.Count -gt 3) {
    Write-Warning "Nombre élevé de sessions actives: $($ActiveSessions.Count)"
    $ActiveSessions
}
# Détection des connexions géographiquement impossibles (nécessite intégration threat intelligence)
Register-WmiEvent -Query "SELECT * FROM Win32_NTLogEvent WHERE LogFile='Security' AND EventCode=4624" -Action {
    $Event = $Event.SourceEventArgs.NewEvent
    $SourceIP = $Event.InsertionStrings[18]
    Write-Host "Nouvelle connexion détectée depuis: $SourceIP"
    # Implémenter logique de géolocalisation IP
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.10.1 *Protection contre le credential stuffing*

DESCRIPTION :
Des mécanismes anti-credential stuffing doivent être implémentés incluant limitation de taux, analyse comportementale et blocage automatique.
Cette protection prévient l'exploitation de credentials volés sur d'autres plateformes.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625} -MaxEvents 100 | Group-Object {$_.Properties[19].Value} | Sort-Object
Get-EventLog -LogName Security -InstanceId 4625 | Group-Object MachineName
netsh advfirewall show allprofiles state
```

```
# Implémentation anti-credential stuffing basique
$FailedLoginThreshold = 5
$TimeWindow = 300  # 5 minutes
$RecentFailures = Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625; StartTime=(Get-Date).AddSeconds(-$TimeWindow)}
$FailuresByIP = $RecentFailures | Group-Object {$_.Properties[19].Value}
foreach ($IPGroup in $FailuresByIP) {
    if ($IPGroup.Count -ge $FailedLoginThreshold) {
        $IP = $IPGroup.Name
        Write-Warning "CREDENTIAL STUFFING DETECTED from IP: $IP ($($IPGroup.Count) attempts)"
        # Bloquer l'IP via pare-feu
        # New-NetFirewallRule -DisplayName "Block-$IP" -Direction Inbound -RemoteAddress $IP -Action Block
    }
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.11.1 *Gestion des comptes partagés et génériques*

DESCRIPTION :
Les comptes partagés doivent être éliminés ou strictement contrôlés avec traçabilité individuelle et rotation fréquente des mots de passe.
Cette mesure assure la responsabilité individuelle et limite les risques de compromission.

```
Get-LocalUser | Where-Object {$_.Description -like "*shared*" -or $_.Description -like "*generic*" -or $_.Name -like "*shared*"}
Get-WmiObject Win32_UserAccount | Where-Object {$_.Description -like "*commun*" -or $_.Name -like "*admin*"}
net user | findstr /i "admin service shared generic"
```

```
# Audit des comptes potentiellement partagés
$SharedKeywords = @("shared", "common", "generic", "admin", "service", "temp", "test")
$AllUsers = Get-LocalUser
foreach ($User in $AllUsers) {
    $IsShared = $false
    foreach ($Keyword in $SharedKeywords) {
        if ($User.Name -like "*$Keyword*" -or $User.Description -like "*$Keyword*") {
            $IsShared = $true
            break
        }
    }
    if ($IsShared) {
        Write-Warning "Compte potentiellement partagé: $($User.Name) - $($User.Description)"
        # Action recommandée: Remplacer par des comptes individuels
    }
}
# Configuration de rotation automatique pour comptes de service
Write-Host "RECOMMANDATION: Migrer vers des comptes gMSA pour les services"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration
2.5 — Gestion avancée des comptes privilégiés

2.5.1 *Implémentation de comptes PAM (Privileged Access Management)*

DESCRIPTION :
Une solution de gestion des accès privilégiés (PAM) doit être déployée pour tous les comptes administrateurs avec rotation automatique des mots de passe, enregistrement des sessions et approbation des accès.
Cette mesure constitue un pilier fondamental de la sécurité Zero Trust pour les accès critiques et permet de tracer tous les accès privilégiés.

```
Get-LocalGroupMember -Group "Administrators" | Select-Object Name, ObjectClass, PrincipalSource
Get-EventLog -LogName Security -InstanceId 4624 | Where-Object {$_.ReplacementStrings[8] -eq "2"} | Select-Object -First 10
auditpol /get /subcategory:"Special Logon"
```

```
# Configuration PAM basique avec audit renforcé
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
# Création de comptes PAM avec rotation automatique
$PAMAccount = "PAM-Admin-$(Get-Date -Format "yyyyMM")"
New-LocalUser -Name $PAMAccount -Description "Compte PAM avec rotation mensuelle" -AccountNeverExpires:$false
$ComplexPassword = -join ((33..126) | Get-Random -Count 32 | ForEach-Object {[char]$_})
Set-LocalUser -Name $PAMAccount -Password (ConvertTo-SecureString $ComplexPassword -AsPlainText -Force)
# Configuration de session recording
Enable-PSTranscription -OutputDirectory "C:\PAMLogs" -IncludeInvocationHeader
Write-Host "Compte PAM créé: $PAMAccount"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.5.2 *Authentification multi-facteurs (MFA) obligatoire*

DESCRIPTION :
L'authentification multi-facteurs doit être obligatoire pour tous les comptes privilégiés et fortement recommandée pour les comptes utilisateur standard, avec support de FIDO2/WebAuthn.
Cette protection constitue une défense critique contre les attaques par vol de credentials, phishing et credential stuffing.

```
Get-WindowsOptionalFeature -Online -FeatureName "*Hello*" | Where-Object {$_.State -eq "Enabled"}
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork" -ErrorAction SilentlyContinue
certlm.msc # Vérifier les certificats d'authentification présents
```

```
# Activation Windows Hello for Business
Enable-WindowsOptionalFeature -Online -FeatureName "WindowsHelloFace" -All -NoRestart
# Configuration des stratégies MFA
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork" -Force | Out-Null
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork" -Name "Enabled" -Value 1 -Type DWord
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork" -Name "RequireSecurityDevice" -Value 1 -Type DWord
# Configuration pour FIDO2
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\FIDO" -Force | Out-Null
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\FIDO" -Name "EnablePasswordlessExperience" -Value 1 -Type DWord
Write-Host "MFA configuré - Redémarrage requis pour activation complète"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.5.3 *Détection et gestion des comptes dormants*

DESCRIPTION :

Les comptes inactifs depuis plus de 90 jours doivent être automatiquement détectés, rapportés et désactivés selon une politique de gouvernance établie.

Cette pratique élimine les comptes oubliés qui constituent des vecteurs d'attaque potentiels pour les adversaires.

```
Get-LocalUser | Where-Object {$_.LastLogon -lt (Get-Date).AddDays(-90) -and $_.Enabled -eq $true} | Select-Object Name, LastLogon,
Get-WmiObject Win32_UserProfile | Where-Object {$_.LastUseTime -lt (Get-Date).AddDays(-90).ToString("yyyyMMddHHmmss.ffffff-000")} |
Get-EventLog -LogName Security -InstanceId 4624 -After (Get-Date).AddDays(-90) | Group-Object UserName | Sort-Object Count | Select
```

```
# Script de nettoyage des comptes dormants
$InactiveThreshold = (Get-Date).AddDays(-90)
$SystemAccounts = @("Administrator", "DefaultAccount", "Guest", "WDAGUtilityAccount", "krbtgt")
$DormantAccounts = Get-LocalUser | Where-Object {
    $_.Enabled -eq $true -and
    ($_.LastLogon -lt $InactiveThreshold -or $_.LastLogon -eq $null) -and
    $_.Name -notin $SystemAccounts
}
Write-Host "=== RAPPORT COMPTES DORMANTS ==="
foreach ($Account in $DormantAccounts) {
    $DaysInactive = if ($Account.LastLogon) { ((Get-Date) - $Account.LastLogon).Days } else { "Jamais connecté" }
    Write-Warning "Compte dormant: $($Account.Name) - Inactif depuis: $DaysInactive jours"
    # Action: Désactiver le compte (décommenter pour activer)
    # Disable-LocalUser -Name $Account.Name -Confirm:$false
    # Write-Host "  -> Compte désactivé: $($Account.Name)"
}
Write-Host "Total comptes dormants trouvés: $($DormantAccounts.Count)"
```

VALEUR PAR DÉFAUT :

Variable selon la configuration

2.6 — Surveillance et protection des accès

2.6.1 *Monitoring des connexions simultanées suspectes*

DESCRIPTION :

Les connexions simultanées depuis des emplacements géographiques impossibles ou des patterns de connexion anormaux doivent être détectées et alertées en temps réel.

Cette surveillance permet d'identifier rapidement les comptes compromis utilisés par des attaquants depuis des emplacements multiples.

```
query user
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4624} -MaxEvents 100 | Group-Object {$_.Properties[5].Value} | Where-Object
Get-WmiObject Win32_LoggedOnUser | Group-Object Antecedent | Where-Object {$_.Count -gt 1}
```

```
# Surveillance des sessions multiples en temps réel
function Monitor-ConcurrentSessions {
    $ActiveSessions = query user 2>$null | Select-String "Active|Actif"
    $SessionCount = $ActiveSessions.Count

    if ($SessionCount -gt 3) {
        Write-Warning "ALERTE: $SessionCount sessions actives simultanées détectées"
        $ActiveSessions | ForEach-Object { Write-Host "  Session: $_" }
    }

    # Analyser les connexions récentes par IP
    $RecentLogins = Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4624; StartTime=(Get-Date).AddHours(-1)} -ErrorAction Si
    $LoginsByIP = $RecentLogins | Group-Object {$_.Properties[18].Value} | Sort-Object Count -Descending

    foreach ($IPGroup in $LoginsByIP) {
        if ($IPGroup.Count -gt 5) {
            Write-Warning "IP suspecte avec nombreuses connexions: $($IPGroup.Name) ($($IPGroup.Count) connexions)"
        }
    }
}
# Surveiller en continu (lancer en tâche planifiée)
Monitor-ConcurrentSessions
```

VALEUR PAR DÉFAUT :

Variable selon la configuration

2.6.2 *Protection contre le credential stuffing et brute force*

DESCRIPTION :
Des mécanismes anti-credential stuffing doivent être implémentés incluant limitation de taux, analyse comportementale et blocage automatique des sources malveillantes.
Cette protection prévient l'exploitation de credentials volés provenant de fuites de données sur d'autres plateformes.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625} -MaxEvents 100 | Group-Object {$_.Properties[19].Value} | Sort-Object
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625; StartTime=(Get-Date).AddHours(-1)} | Measure-Object
netsh advfirewall firewall show rule name=all dir=in | findstr "Block"
```

```
# Système de protection anti-credential stuffing
function Enable-AntiBruteForce {
    param(
        [int]$FailureThreshold = 5,
        [int]$TimeWindowMinutes = 15,
        [int]$BlockDurationMinutes = 60
    )

    $StartTime = (Get-Date).AddMinutes(-$TimeWindowMinutes)
    $FailedAttempts = Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625; StartTime=$StartTime} -ErrorAction SilentlyConti

    if ($FailedAttempts) {
        $AttackersbyIP = $FailedAttempts | Group-Object {$_.Properties[19].Value}

        foreach ($Attacker in $AttackersbyIP) {
            if ($Attacker.Count -ge $FailureThreshold) {
                $AttackerIP = $Attacker.Name
                Write-Warning "CREDENTIAL STUFFING DÉTECTÉ - IP: $AttackerIP ($($Attacker.Count) tentatives)"

                # Bloquer l'IP via pare-feu Windows
                try {
                    $RuleName = "AutoBlock-BruteForce-$AttackerIP"
                    New-NetFirewallRule -DisplayName $RuleName -Direction Inbound -RemoteAddress $AttackerIP -Action Block -ErrorAc
                    Write-Host "  -> IP $AttackerIP bloquée automatiquement"

                    # Programmer le déblocage automatique
                    $UnblockTime = (Get-Date).AddMinutes($BlockDurationMinutes)
                    Write-Host "  -> Déblocage automatique programmé: $UnblockTime"
                } catch {
                    Write-Error "Impossible de bloquer IP $AttackerIP : $_"
                }
            }
        }
    }
}
# Activer la protection
Enable-AntiBruteForce
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.7.1 *Audit des connexions privilégiées*

DESCRIPTION :
Surveillance renforcée de tous les accès avec privilèges administratifs pour détecter les usages non autorisés.

```
# Commandes de vérification pour Audit des connexions privilégiées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Audit des connexions privilégiées
Write-Host "Configuration de sécurité pour: Audit des connexions privilégiées"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.8.1 *Gestion des comptes de service*

DESCRIPTION :
Configuration sécurisée des comptes de service avec privilèges minimaux requis.

```
# Commandes de vérification pour Gestion des comptes de service
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Gestion des comptes de service
Write-Host "Configuration de sécurité pour: Gestion des comptes de service"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.9.1 *Protection contre l'énumération*

DESCRIPTION :
Mesures anti-énumération pour empêcher la découverte des comptes par des attaquants.

```
# Commandes de vérification pour Protection contre l'énumération
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Protection contre l'énumération
Write-Host "Configuration de sécurité pour: Protection contre l'énumération"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.10.1 *Authentification biométrique*

DESCRIPTION :
Déploiement de l'authentification biométrique Windows Hello pour renforcer l'authentification.

```
# Commandes de vérification pour Authentification biométrique
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Authentification biométrique
Write-Host "Configuration de sécurité pour: Authentification biométrique"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.11.1 *Contrôle des sessions RDP*

DESCRIPTION :
Limitation et surveillance des sessions Bureau à Distance pour prévenir les accès non autorisés.

```
# Commandes de vérification pour Contrôle des sessions RDP
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle des sessions RDP
Write-Host "Configuration de sécurité pour: Contrôle des sessions RDP"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.12.1 *Audit des élévations UAC*

DESCRIPTION :
Traçage complet de toutes les élévations de privilège utilisateur via UAC.

```
# Commandes de vérification pour Audit des élévations UAC
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Audit des élévations UAC
Write-Host "Configuration de sécurité pour: Audit des élévations UAC"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.13.1 *Gestion des comptes temporaires*

DESCRIPTION :
Politique de création, utilisation et suppression des comptes temporaires.

```
# Commandes de vérification pour Gestion des comptes temporaires
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Gestion des comptes temporaires
Write-Host "Configuration de sécurité pour: Gestion des comptes temporaires"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.14.1 *Protection des identifiants*

DESCRIPTION :
Mesures de protection contre le vol et la réutilisation des identifiants.

```
# Commandes de vérification pour Protection des identifiants
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Protection des identifiants
Write-Host "Configuration de sécurité pour: Protection des identifiants"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.15.1 *Authentification réseau*

DESCRIPTION :
Configuration sécurisée de l'authentification pour les accès réseau.

```
# Commandes de vérification pour Authentification réseau
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Authentification réseau
Write-Host "Configuration de sécurité pour: Authentification réseau"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.16.1 *Surveillance des modifications*

DESCRIPTION :
Audit des modifications apportées aux comptes et groupes système.

```
# Commandes de vérification pour Surveillance des modifications
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Surveillance des modifications
Write-Host "Configuration de sécurité pour: Surveillance des modifications"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.17.1 *Contrôle d'accès granulaire*

DESCRIPTION :
Implémentation d'un contrôle d'accès fin selon le principe du moindre privilège.

```
# Commandes de vérification pour Contrôle d'accès granulaire
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle d'accès granulaire
Write-Host "Configuration de sécurité pour: Contrôle d'accès granulaire"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.18.1 *Protection contre le pass-the-ticket*

DESCRIPTION :
Mesures préventives contre les attaques de type pass-the-ticket Kerberos.

```
# Commandes de vérification pour Protection contre le pass-the-ticket
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Protection contre le pass-the-ticket
Write-Host "Configuration de sécurité pour: Protection contre le pass-the-ticket"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.19.1 *Gestion des certificats*

DESCRIPTION :
Administration sécurisée des certificats d'authentification utilisateur.

```
# Commandes de vérification pour Gestion des certificats
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Gestion des certificats
Write-Host "Configuration de sécurité pour: Gestion des certificats"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.20.1 *Audit des accès échoués*

DESCRIPTION :
Surveillance et analyse des tentatives d'accès échouées pour détecter les attaques.

```
# Commandes de vérification pour Audit des accès échoués
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Audit des accès échoués
Write-Host "Configuration de sécurité pour: Audit des accès échoués"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.21.1 *Protection des comptes système*

DESCRIPTION :
Sécurisation renforcée des comptes système intégrés de Windows.

```
# Commandes de vérification pour Protection des comptes système
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Protection des comptes système
Write-Host "Configuration de sécurité pour: Protection des comptes système"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.22.1 *Contrôle des permissions*

DESCRIPTION :
Audit et contrôle granulaire des permissions sur les ressources système.

```
# Commandes de vérification pour Contrôle des permissions
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle des permissions
Write-Host "Configuration de sécurité pour: Contrôle des permissions"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.23.1 *Authentification smart card*

DESCRIPTION :
Déploiement et configuration de l'authentification par carte à puce.

```
# Commandes de vérification pour Authentification smart card
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Authentification smart card
Write-Host "Configuration de sécurité pour: Authentification smart card"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.24.1 *Surveillance des groupes*

DESCRIPTION :
Monitoring des modifications d'appartenance aux groupes privilégiés.

```
# Commandes de vérification pour Surveillance des groupes
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Surveillance des groupes
Write-Host "Configuration de sécurité pour: Surveillance des groupes"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

2.25.1 *Protection session hijacking*

DESCRIPTION :
Mesures préventives contre le détournement de sessions utilisateur.

```
# Commandes de vérification pour Protection session hijacking
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Protection session hijacking
Write-Host "Configuration de sécurité pour: Protection session hijacking"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

🔒 SECTION 3 : POLITIQUES DE MOT DE PASSE

3.1 — Complexité et longueur des mots de passe

3.1.1 *Longueur minimale des mots de passe*

DESCRIPTION :
La longueur minimale des mots de passe doit être configurée à au moins 14 caractères pour résister aux attaques par force brute. Les mots de passe longs offrent une meilleure entropie que la complexité seule.

Conformément aux recommandations ANSSI et NIST, les mots de passe de 14 caractères minimum offrent un niveau de sécurité acceptable.

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters' -Name 'RequireStrongKey' -ErrorAction Silently
# Politique locale
net accounts | findstr /i "longueur"
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "MinimumPasswordLength"
```

AUDIT :

- **GUI :** secpol.msc > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe > Longueur minimale du mot de passe
- **Valeur attendue :** ≥ 14 caractères

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length → 14
2. **PowerShell (via secedit) :**

```
# Créer fichier de configuration
$ConfigContent = @"
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordLength = 14
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\pwd_length.inf -Encoding Unicode
secedit /configure /db C:\temp\pwd_length.sdb /cfg C:\temp\pwd_length.inf
Remove-Item C:\temp\pwd_length.inf, C:\temp\pwd_length.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
0 (aucune longueur minimale)

3.1.2 *Complexité des mots de passe*

DESCRIPTION :
La politique de complexité des mots de passe doit être activée pour exiger l'utilisation de caractères de différentes catégories (majuscules, minuscules, chiffres, caractères spéciaux).

Cette mesure rend les attaques par dictionnaire et les tentatives de devinement plus difficiles.

```
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "PasswordComplexity"
net accounts | findstr /i "complexité"
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de compte > Stratégie de mot de passe > Le mot de passe doit respecter les exigences de complexité
- **Valeur attendue :** PasswordComplexity = 1 (Activé)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements → Enabled
2. **PowerShell (via secedit) :**

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[System Access]
PasswordComplexity = 1
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\pwd_complexity.inf -Encoding Unicode
secedit /configure /db C:\temp\pwd_complexity.sdb /cfg C:\temp\pwd_complexity.inf
Remove-Item C:\temp\pwd_complexity.inf, C:\temp\pwd_complexity.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
1 (Activé sur domaine), 0 (Désactivé en standalone)

3.1.3 *Historique des mots de passe*

DESCRIPTION :
L'historique des mots de passe doit mémoriser au moins 24 mots de passe précédents pour empêcher la réutilisation immédiate des anciens mots de passe.

Cette mesure force les utilisateurs à créer de nouveaux mots de passe uniques et évite la rotation cyclique de quelques mots de passe.

```
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "PasswordHistorySize"
net accounts | findstr /i "historique"
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de compte > Stratégie de mot de passe > Conserver l'historique des mots de passe
- **Valeur attendue :** PasswordHistorySize ≥ 24

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history → 24 passwords remembered
2. **PowerShell (via secedit) :**

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[System Access]
PasswordHistorySize = 24
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\pwd_history.inf -Encoding Unicode
secedit /configure /db C:\temp\pwd_history.sdb /cfg C:\temp\pwd_history.inf
Remove-Item C:\temp\pwd_history.inf, C:\temp\pwd_history.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
0 (aucun historique)

3.2 — Durée de vie des mots de passe

3.2.1 *Âge maximum des mots de passe*

DESCRIPTION :
L'âge maximum des mots de passe doit être défini pour forcer un changement régulier. Recommandation ANSSI : entre 1 an (365 jours) et 18 mois selon le contexte de sécurité.
Pour les environnements hautement sécurisés, une durée de 365 jours est recommandée. Pour les environnements standards, 540 jours maximum.

```
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "MaximumPasswordAge"
net accounts | findstr /i "âge"
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de compte > Stratégie de mot de passe > Âge maximal du mot de passe
- **Valeur attendue :** MaximumPasswordAge ≤ 365 jours

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age → 365 days
2. **PowerShell (via secedit) :**

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[System Access]
MaximumPasswordAge = 365
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\pwd_maxage.inf -Encoding Unicode
secedit /configure /db C:\temp\pwd_maxage.sdb /cfg C:\temp\pwd_maxage.inf
Remove-Item C:\temp\pwd_maxage.inf, C:\temp\pwd_maxage.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
42 jours (domaine), 0 - jamais (standalone)

3.2.2 *Âge minimum des mots de passe*

DESCRIPTION :
L'âge minimum des mots de passe doit être défini à au moins 1 jour pour empêcher les utilisateurs de changer immédiatement leur mot de passe pour contourner l'historique.

```
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "MinimumPasswordAge"
net accounts | findstr /i "âge"
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de compte > Stratégie de mot de passe > Âge minimal du mot de passe
- **Valeur attendue :** MinimumPasswordAge ≥ 1 jour

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age → 1 day
2. **PowerShell (via secedit) :**

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\pwd_minage.inf -Encoding Unicode
secedit /configure /db C:\temp\pwd_minage.sdb /cfg C:\temp\pwd_minage.inf
Remove-Item C:\temp\pwd_minage.inf, C:\temp\pwd_minage.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
0 jours (changement immédiat autorisé)
3.3 — Stockage et protection des mots de passe

3.3.1 *Chiffrement réversible des mots de passe*

DESCRIPTION :
Le stockage des mots de passe avec chiffrement réversible doit être désactivé. Cette option stocke les mots de passe de manière à pouvoir les déchiffrer, ce qui présente un risque de sécurité majeur.
Le chiffrement réversible équivaut pratiquement à un stockage en texte clair et doit être évité sauf exigences techniques très spécifiques.

```
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "ClearTextPassword"
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de compte > Stratégie de mot de passe > Stocker les mots de passe en utilisant un chiffrement réversible
- **Valeur attendue :** ClearTextPassword = 0 (Désactivé)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption → Disabled
2. **PowerShell (via secedit) :**

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[System Access]
ClearTextPassword = 0
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\pwd_cleartext.inf -Encoding Unicode
secedit /configure /db C:\temp\pwd_cleartext.sdb /cfg C:\temp\pwd_cleartext.inf
Remove-Item C:\temp\pwd_cleartext.inf, C:\temp\pwd_cleartext.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
0 (Désactivé)

3.3.2 *Protection contre l'énumération des comptes*

DESCRIPTION :
La protection contre l'énumération des comptes doit être activée pour empêcher la découverte des noms de comptes via les codes d'erreur d'authentification.
Cette protection fait en sorte que les tentatives de connexion avec des comptes inexistants retournent le même message d'erreur que les tentatives avec des mots de passe incorrects.

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'RestrictAnonymous' -ErrorAction SilentlyContinue
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'RestrictAnonymousSAM' -ErrorAction SilentlyContinue
```

AUDIT :

- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Accès réseau : Ne pas autoriser l'énumération anonyme des comptes SAM
- **Valeur attendue :** RestrictAnonymousSAM = 1

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts → Enabled
2. **PowerShell :**

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'RestrictAnonymousSAM' -Value 1 -Type DWord
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'RestrictAnonymous' -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
1 (Activé sur Windows 11)

3.4.1 *Configuration des politiques de complexité avancées*

DESCRIPTION :
Les mots de passe doivent respecter des critères de complexité avancés incluant la vérification de dictionnaires communs et l'interdiction de réutilisation de parties du nom d'utilisateur.
Cette politique renforce significativement la résistance aux attaques par dictionnaire et force brute.

```
net accounts
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "RequireSignOrSeal" -ErrorAction Silentl
secedit /export /cfg C:\temp\secpol.cfg /quiet && findstr /i "password" C:\temp\secpol.cfg
```

```
# Configuration politique de mot de passe complexe
secedit /export /cfg C:\temp\secpol.cfg /quiet
$secpol = Get-Content C:\temp\secpol.cfg
$secpol = $secpol -replace "MinimumPasswordLength = .*", "MinimumPasswordLength = 14"
$secpol = $secpol -replace "MaximumPasswordAge = .*", "MaximumPasswordAge = 365"
$secpol = $secpol -replace "PasswordComplexity = .*", "PasswordComplexity = 1"
$secpol = $secpol -replace "PasswordHistorySize = .*", "PasswordHistorySize = 24"
Set-Content C:\temp\secpol_new.cfg -Value $secpol
secedit /configure /db C:\temp\secedit.sdb /cfg C:\temp\secpol_new.cfg /quiet
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.4.1 *Configuration de l'historique étendu des mots de passe*

DESCRIPTION :
L'historique des mots de passe doit être configuré pour mémoriser au minimum 24 mots de passe précédents afin d'empêcher la réutilisation rapide.
Cette configuration force les utilisateurs à utiliser des mots de passe véritablement nouveaux et uniques.

```
net accounts | findstr "Longueur historique"
secedit /export /cfg C:\temp\secpol.cfg /quiet && findstr "PasswordHistorySize" C:\temp\secpol.cfg
```

```
# Configuration de l'historique des mots de passe
net accounts /uniquepw:24
# Via secedit
secedit /export /cfg C:\temp\secpol.cfg /quiet
(Get-Content C:\temp\secpol.cfg) -replace "PasswordHistorySize = .*", "PasswordHistorySize = 24" | Set-Content C:\temp\secpol_new.c
secedit /configure /db C:\temp\secedit.sdb /cfg C:\temp\secpol_new.cfg /quiet
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.5.1 *Implémentation de filtres de mots de passe avancés*

DESCRIPTION :
Des filtres de mots de passe personnalisés doivent être implémentés pour rejeter les mots de passe faibles, les mots de dictionnaire et les patterns communs.
Cette mesure renforce significativement la politique de mot de passe au-delà des règles de base Windows.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "Notification Packages"
dir "C:\Windows\System32\*passfilt*"
Get-Content "C:\Windows\debug\passwd.log" -Tail 10 -ErrorAction SilentlyContinue
```

```
# Installation du filtre de mot de passe avancé (exemple avec Azure AD Password Protection)
# Download et installation du DC Agent et Proxy
Write-Host "Télécharger Azure AD Password Protection depuis Microsoft"
# Configuration du filtre personnalisé
$NotificationPackages = (Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "Notification Packages")."Notifi
if ($NotificationPackages -notcontains "AzureADPasswordProtection") {
    $NewPackages = $NotificationPackages + @("AzureADPasswordProtection")
    Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "Notification Packages" -Value $NewPackages
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.6.1 *Configuration des comptes avec mots de passe n'expirant jamais*

DESCRIPTION :
Aucun compte utilisateur ne doit être configuré avec un mot de passe n'expirant jamais, à l'exception des comptes de service gérés.
Cette règle assure un renouvellement régulier des credentials utilisateur pour maintenir la sécurité.

```
Get-LocalUser | Where-Object {$_.PasswordNeverExpires -eq $true} | Select-Object Name, PasswordNeverExpires, LastLogon
net user | findstr "jamais"
Get-WmiObject -Class Win32_UserAccount -Filter "PasswordExpires=False" | Select-Object Name, PasswordExpires
```

```
# Identifier et corriger les comptes avec mots de passe permanents
Get-LocalUser | Where-Object {$_.PasswordNeverExpires -eq $true -and $_.Name -ne "DefaultAccount"} | ForEach-Object {
    Set-LocalUser -Name $_.Name -PasswordNeverExpires $false
    Write-Host "Mot de passe configuré pour expirer: $($_.Name)"
}
# Audit des comptes de service
Get-WmiObject Win32_Service | Where-Object {$_.StartName -notlike "LocalSystem" -and $_.StartName -notlike "NT AUTHORITY\*"} | Sele
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.7.1 *Configuration de notifications d'expiration de mot de passe*

DESCRIPTION :
Les utilisateurs doivent recevoir des notifications d'expiration de mot de passe suffisamment à l'avance pour permettre un changement planifié.
Cette configuration évite les blocages d'accès inattendus et encourage un changement proactif des mots de passe.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name "PasswordExpiryWarning"
net accounts | findstr "Avertissement"
Get-LocalUser | Select-Object Name, PasswordLastSet, @{Name="DaysUntilExpiry";Expression={(New-TimeSpan -Start (Get-Date) -End $_.P
```

```
# Configuration de l'avertissement d'expiration (14 jours à l'avance)
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name "PasswordExpiryWarning" -Value 14 -Type
# Via ligne de commande
net accounts /forcelogoff:no
# Script de notification personnalisée
$Users = Get-LocalUser | Where-Object {$_.Enabled -eq $true}
foreach ($User in $Users) {
    $DaysLeft = (New-TimeSpan -Start (Get-Date) -End $User.PasswordLastSet.AddDays(42)).Days
    if ($DaysLeft -le 14 -and $DaysLeft -gt 0) {
        Write-Host "ATTENTION: Mot de passe expire dans $DaysLeft jours pour: $($User.Name)"
    }
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.8.1 *Audit des tentatives de changement de mot de passe échouées*

DESCRIPTION :
Les tentatives de changement de mot de passe échouées doivent être auditées pour détecter les attaques par brute force et les problèmes de politique.
Cette surveillance permet d'identifier les patterns d'attaque et les problèmes de conformité des utilisateurs.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4723,4724} -MaxEvents 50
Get-EventLog -LogName Security -InstanceId 627 -Newest 20
auditpol /get /subcategory:"User Account Management"
```

```
# Activation de l'audit des changements de mot de passe
auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
# Surveillance des échecs répétés
Register-WmiEvent -Query "SELECT * FROM Win32_NTLogEvent WHERE LogFile='Security' AND EventCode=4724" -Action {
    $Event = $Event.SourceEventArgs.NewEvent
    Write-Warning "Échec changement mot de passe: $($Event.InsertionStrings[0])"
}
# Analyse des patterns d'échec
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4724} -MaxEvents 100 | Group-Object {$_.Properties[0].Value} | Sort-Object C
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.4.1 *Implémentation de phrases de passe (passphrases)*

DESCRIPTION :
Les phrases de passe longues doivent être encouragées comme alternative aux mots de passe complexes courts pour améliorer à la fois la sécurité et l'utilisabilité.
Les phrases de passe de 4+ mots sont généralement plus sécurisées et mémorisables que les mots de passe courts complexes.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "MaximumPasswordLength"
net accounts | findstr "Longueur"
Get-ADDefaultDomainPasswordPolicy -ErrorAction SilentlyContinue
```

```
# Configuration pour supporter les phrases de passe longues
net accounts /maxpwlen:127
# Via stratégie de groupe pour domaine
Write-Host "Configuration GPO: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy"
Write-Host "Maximum password length: 127 characters"
# Script de validation de phrases de passe
function Test-Passphrase {
    param([string]$Passphrase)
    $Words = $Passphrase -split "\s+"
    if ($Words.Count -ge 4 -and $Passphrase.Length -ge 20) {
        Write-Host "Phrase de passe valide: $($Words.Count) mots, $($Passphrase.Length) caractères"
        return $true
    }
    return $false
}
# Test-Passphrase "Mon chat mange des croquettes bleues 2024"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.5.1 *Détection et blocage des mots de passe compromis*

DESCRIPTION :
Une base de données de mots de passe compromis (HavelBeenPwned, etc.) doit être intégrée pour rejeter automatiquement les mots de passe connus comme compromis.
Cette mesure prévient l'utilisation de mots de passe déjà exposés dans des fuites de données publiques.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\AzureADPasswordProtection" -ErrorAction SilentlyContinue
Get-Service -Name "AzureADPasswordProtectionDCAgent" -ErrorAction SilentlyContinue
Get-EventLog -LogName "Microsoft-AzureADPasswordProtection-DCAgent/Admin" -Newest 10 -ErrorAction SilentlyContinue
```

```
# Installation Azure AD Password Protection (nécessite licences Azure AD Premium)
Write-Host "1. Télécharger Azure AD Password Protection DC Agent"
Write-Host "2. Installer sur tous les contrôleurs de domaine"
Write-Host "3. Configurer via Azure AD Portal: Security > Authentication methods > Password protection"
# Alternative: Script de vérification basique avec API HaveIBeenPwned
function Test-CompromisedPassword {
    param([SecureString]$Password)
    $PlainPassword = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto([System.Runtime.InteropServices.Marshal]::SecureStri
    $Hash = [System.Security.Cryptography.SHA1]::Create().ComputeHash([System.Text.Encoding]::UTF8.GetBytes($PlainPassword))
    $HashString = [BitConverter]::ToString($Hash) -replace "-"
    $Prefix = $HashString.Substring(0,5)
    $Suffix = $HashString.Substring(5)
    try {
        $Response = Invoke-WebRequest -Uri "https://api.pwnedpasswords.com/range/$Prefix" -UseBasicParsing
        if ($Response.Content -like "*$Suffix*") {
            Write-Warning "MOT DE PASSE COMPROMIS DÉTECTÉ"
            return $false
        }
    } catch {
        Write-Warning "Impossible de vérifier le mot de passe"
    }
    return $true
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.6.1 *Analyse de la force des mots de passe en temps réel*

DESCRIPTION :
Un système d'analyse en temps réel de la force des mots de passe doit fournir un feedback immédiat aux utilisateurs lors de la création.
Cette assistance améliore la qualité des mots de passe choisis par les utilisateurs.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\UserTile" -ErrorAction SilentlyConti
Get-WindowsCapability -Online -Name "*Hello*"
powercfg /devicequery wake_armed
```

```
# Script d'analyse de force de mot de passe
function Measure-PasswordStrength {
    param([string]$Password)
    $Score = 0
    $Feedback = @()

    # Critères de base
    if ($Password.Length -ge 12) { $Score += 2 } elseif ($Password.Length -ge 8) { $Score += 1 }
    if ($Password -cmatch "[a-z]") { $Score += 1 }
    if ($Password -cmatch "[A-Z]") { $Score += 1 }
    if ($Password -match "[0-9]") { $Score += 1 }
    if ($Password -match "[^a-zA-Z0-9]") { $Score += 2 }

    # Critères avancés
    if ($Password -notmatch "(.)\1{2,}") { $Score += 1 }  # Pas de répétition
    if ($Password -notmatch "123|abc|qwe|asd") { $Score += 1 }  # Pas de séquences

    # Évaluation
    switch ($Score) {
        {$_ -ge 8} { return @{Level="Excellent"; Score=$Score; Color="Green"} }
        {$_ -ge 6} { return @{Level="Bon"; Score=$Score; Color="Yellow"} }
        {$_ -ge 4} { return @{Level="Moyen"; Score=$Score; Color="Orange"} }
        default { return @{Level="Faible"; Score=$Score; Color="Red"} }
    }
}
# Exemple d'usage
# Measure-PasswordStrength "MonMotDePasse123!"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.4 — Politiques avancées de mots de passe

3.4.1 *Implémentation de filtres anti-mots de passe compromis*

DESCRIPTION :
Des filtres de mots de passe doivent intégrer des bases de données de mots de passe compromis (HaveIBeenPwned, etc.) pour rejeter automatiquement les mots de passe connus comme exposés dans des fuites.
Cette mesure prévient l'utilisation de mots de passe déjà compromis dans des violations de données publiques.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\AzureADPasswordProtection" -ErrorAction SilentlyContinue
Get-Service -Name "*Password*" | Where-Object {$_.Status -eq "Running"}
Get-EventLog -LogName Application | Where-Object {$_.Source -like "*Password*"} | Select-Object -First 5
```

```
# Installation et configuration Azure AD Password Protection (nécessite Azure AD Premium)
Write-Host "=== CONFIGURATION AZURE AD PASSWORD PROTECTION ==="
Write-Host "1. Télécharger AzureADPasswordProtectionProxySetup.exe depuis Microsoft"
Write-Host "2. Télécharger AzureADPasswordProtectionDCAgentSetup.exe"
Write-Host "3. Installer sur tous les contrôleurs de domaine"

# Alternative: Vérification basique avec API HaveIBeenPwned
function Test-CompromisedPassword {
    param([string]$Password)

    if ($Password.Length -eq 0) { return $false }

    try {
        # Calculer le hash SHA-1 du mot de passe
        $sha1 = New-Object System.Security.Cryptography.SHA1Managed
        $hash = [System.BitConverter]::ToString($sha1.ComputeHash([System.Text.Encoding]::UTF8.GetBytes($Password))).Replace("-", "
        $prefix = $hash.Substring(0,5)
        $suffix = $hash.Substring(5)

        # Interroger l'API HaveIBeenPwned
        $response = Invoke-RestMethod -Uri "https://api.pwnedpasswords.com/range/$prefix" -Method Get -TimeoutSec 10

        if ($response -match $suffix) {
            Write-Warning "MOT DE PASSE COMPROMIS DÉTECTÉ dans les fuites de données"
            return $true
        } else {
            Write-Host "Mot de passe non trouvé dans les fuites connues"
            return $false
        }
    } catch {
        Write-Warning "Impossible de vérifier le mot de passe: $_"
        return $false
    }
}
# Exemple d'utilisation:
# Test-CompromisedPassword "password123"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.4.2 *Support des phrases de passe (passphrases) longues*

DESCRIPTION :
Les phrases de passe de 4+ mots doivent être encouragées comme alternative aux mots de passe complexes courts, avec configuration appropriée des longueurs maximum supportées.

Les phrases de passe offrent généralement une meilleure sécurité et utilisabilité que les mots de passe courts avec caractères spéciaux.

```
net accounts | findstr /i "longueur"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "MaximumPasswordLength" -ErrorAction Sil
secedit /export /cfg C:\temp\current_policy.cfg /quiet && findstr -i "password" C:\temp\current_policy.cfg
```

```
# Configuration pour supporter les phrases de passe longues
Write-Host "=== CONFIGURATION PHRASES DE PASSE ==="

# Augmenter la longueur maximum autorisée
net accounts /maxpwlen:127  # Maximum supporté par Windows

# Configuration via stratégie de sécurité locale
secedit /export /cfg C:\temp\current_policy.cfg /quiet
$policy = Get-Content C:\temp\current_policy.cfg
$policy = $policy -replace "MaximumPasswordAge = .*", "MaximumPasswordAge = 365"
$policy = $policy -replace "MinimumPasswordLength = .*", "MinimumPasswordLength = 20"
Set-Content C:\temp\new_policy.cfg -Value $policy
secedit /configure /db C:\temp\secedit.sdb /cfg C:\temp\new_policy.cfg /quiet

# Fonction de validation de phrases de passe
function Test-PassphraseStrength {
    param([string]$Passphrase)

    $words = $Passphrase -split "\s+"
    $score = 0
    $feedback = @()

    # Critères d'évaluation
    if ($words.Count -ge 4) { $score += 3; $feedback += "Bon nombre de mots" }
    if ($Passphrase.Length -ge 20) { $score += 2; $feedback += "Longueur appropriée" }
    if ($Passphrase -match "\d") { $score += 1; $feedback += "Contient des chiffres" }
    if ($Passphrase -cmatch "[A-Z].*[a-z]") { $score += 1; $feedback += "Mélange majuscules/minuscules" }

    $strength = switch ($score) {
        {$_ -ge 6} { "Excellente" }
        {$_ -ge 4} { "Bonne" }
        {$_ -ge 2} { "Moyenne" }
        default { "Faible" }
    }

    return @{
        Strength = $strength
        Score = $score
        WordCount = $words.Count
        Length = $Passphrase.Length
        Feedback = $feedback
    }
}
# Exemple: Test-PassphraseStrength "Mon chat mange des croquettes bleues en 2024"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.5.1 *Complexité renforcée*

DESCRIPTION :
Règles de complexité avancées avec vérification de dictionnaires.

```
# Commandes de vérification pour Complexité renforcée
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Complexité renforcée
Write-Host "Configuration de sécurité pour: Complexité renforcée"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.6.1 *Historique étendu*

DESCRIPTION :
Mémorisation de 30+ mots de passe précédents pour éviter la réutilisation.

```
# Commandes de vérification pour Historique étendu
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Historique étendu
Write-Host "Configuration de sécurité pour: Historique étendu"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.7.1 *Notification expiration*

DESCRIPTION :
Système d'alerte préventive pour le renouvellement des mots de passe.

```
# Commandes de vérification pour Notification expiration
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Notification expiration
Write-Host "Configuration de sécurité pour: Notification expiration"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.8.1 *Analyse de force*

DESCRIPTION :
Évaluation temps réel de la robustesse des nouveaux mots de passe.

```
# Commandes de vérification pour Analyse de force
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Analyse de force
Write-Host "Configuration de sécurité pour: Analyse de force"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.9.1 *Filtrage des compromis*

DESCRIPTION :
Intégration de bases de données de mots de passe compromis.

```
# Commandes de vérification pour Filtrage des compromis
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Filtrage des compromis
Write-Host "Configuration de sécurité pour: Filtrage des compromis"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.10.1 *Support passphrases*

DESCRIPTION :
Configuration pour accepter les phrases de passe longues.

```
# Commandes de vérification pour Support passphrases
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Support passphrases
Write-Host "Configuration de sécurité pour: Support passphrases"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.11.1 *Rotation automatique*

DESCRIPTION :
Mécanismes de rotation automatique pour les comptes de service.

```
# Commandes de vérification pour Rotation automatique
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Rotation automatique
Write-Host "Configuration de sécurité pour: Rotation automatique"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.12.1 *Audit des changements*

DESCRIPTION :
Traçage de toutes les modifications de politique de mot de passe.

```
# Commandes de vérification pour Audit des changements
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Audit des changements
Write-Host "Configuration de sécurité pour: Audit des changements"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.13.1 *Protection stockage*

DESCRIPTION :
Chiffrement renforcé du stockage des hachages de mots de passe.

```
# Commandes de vérification pour Protection stockage
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Protection stockage
Write-Host "Configuration de sécurité pour: Protection stockage"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.14.1 *Contrôle qualité*

DESCRIPTION :
Vérification continue de la conformité des mots de passe aux politiques.

```
# Commandes de vérification pour Contrôle qualité
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle qualité
Write-Host "Configuration de sécurité pour: Contrôle qualité"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

3.15.1 *Exceptions documentées*

DESCRIPTION :
Gestion et audit des exceptions aux politiques de mot de passe.

```
# Commandes de vérification pour Exceptions documentées
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Exceptions documentées
Write-Host "Configuration de sécurité pour: Exceptions documentées"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

🔒 SECTION 4 : VERROUILLAGE DE COMPTE

4.1 — Configuration des seuils de verrouillage

4.1.1 *Seuil de verrouillage de compte*

DESCRIPTION :
Le seuil de verrouillage de compte doit être configuré pour verrouiller automatiquement les comptes après un nombre défini de tentatives d'authentification échouées. Recommandation : 5 tentatives maximum.
Cette mesure protège contre les attaques par force brute tout en évitant les verrouillages excessifs qui impacteraient la productivité.

```
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "LockoutBadCount"
net accounts | findstr /i "seuil"
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de compte > Stratégie de verrouillage de compte > Seuil de verrouillage du compte
- **Valeur attendue :** LockoutBadCount ≤ 5 (recommandé : 5)

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold → 5 invalid logon attempts
2. **PowerShell (via secedit) :**

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[System Access]
LockoutBadCount = 5
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\lockout_threshold.inf -Encoding Unicode
secedit /configure /db C:\temp\lockout_threshold.sdb /cfg C:\temp\lockout_threshold.inf
Remove-Item C:\temp\lockout_threshold.inf, C:\temp\lockout_threshold.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
0 (pas de verrouillage)

4.1.2 *Durée de verrouillage de compte*

DESCRIPTION :
La durée de verrouillage de compte doit être configurée à au moins 15 minutes pour ralentir les attaques par force brute tout en permettant un déverrouillage automatique raisonnable.
Une durée trop courte ne décourage pas efficacement les attaquants, une durée trop longue impacte la productivité.

```
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "LockoutDuration"
net accounts | findstr /i "durée"
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de compte > Stratégie de verrouillage de compte > Durée de verrouillage du compte
- **Valeur attendue :** LockoutDuration ≥ 15 minutes

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration → 15 minutes
2. **PowerShell (via secedit) :**

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[System Access]
LockoutDuration = 15
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\lockout_duration.inf -Encoding Unicode
secedit /configure /db C:\temp\lockout_duration.sdb /cfg C:\temp\lockout_duration.inf
Remove-Item C:\temp\lockout_duration.inf, C:\temp\lockout_duration.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
30 minutes (si verrouillage activé)

4.1.3 *Fenêtre de réinitialisation du compteur de verrouillage*

DESCRIPTION :
La fenêtre de réinitialisation du compteur de verrouillage doit être configurée à au moins 15 minutes. Cette période détermine combien de temps après une tentative échouée le compteur est remis à zéro.

```
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "ResetLockoutCount"
```

AUDIT :

- **GUI :** secpol.msc > Stratégies de compte > Stratégie de verrouillage de compte > Réinitialiser le compteur de verrouillages du compte après
- **Valeur attendue :** ResetLockoutCount ≥ 15 minutes

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after → 15 minutes
2. **PowerShell (via secedit) :**

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[System Access]
ResetLockoutCount = 15
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\lockout_reset.inf -Encoding Unicode
secedit /configure /db C:\temp\lockout_reset.sdb /cfg C:\temp\lockout_reset.inf
Remove-Item C:\temp\lockout_reset.inf, C:\temp\lockout_reset.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
30 minutes (si verrouillage activé)
4.2 — Exceptions et comptes spéciaux

4.2.1 *Exclusion des comptes d'administration du verrouillage*

DESCRIPTION :
Les comptes d'administration de domaine ne sont pas soumis aux politiques de verrouillage par défaut. Cette exception doit être documentée et les comptes d'administration locaux doivent être particulièrement protégés.
Il est recommandé de créer des comptes d'administration dédiés avec des noms non-évidents plutôt que d'utiliser les comptes par défaut.

```
# Vérifier les comptes avec le privilège SeDenyNetworkLogonRight
secedit /export /cfg C:\temp\secedit_temp.inf
Get-Content C:\temp\secedit_temp.inf | Select-String "SeDenyNetworkLogonRight"

# Lister les comptes d'administration
Get-LocalGroupMember -Group "Administrators" | Select-Object Name, PrincipalSource
```

AUDIT :

- **Note :** Les comptes Administrateur de domaine ne sont jamais verrouillés par la politique de verrouillage
- **Valeur attendue :** Documentation et monitoring renforcé des comptes d'administration

REMÉDIATION :

1. **Monitoring renforcé :**

```
# Activer l'audit des échecs d'ouverture de session pour les comptes privilégiés
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Account Lockout" /success:enable /failure:enable
```

REMÉDIATION :

1. **Stratégies complémentaires :**
2. Utiliser des comptes d'administration avec des noms non-prédictibles
3. Implémenter une authentification multi-facteur
4. Configurer des alertes en temps réel pour les tentatives de connexion

VALEUR PAR DÉFAUT :
Comptes d'administration exemptés par défaut

4.3.1 *Configuration des seuils de verrouillage adaptatifs*

DESCRIPTION :
Les seuils de verrouillage doivent être configurés de manière adaptative selon le type de compte et le niveau de risque.
Cette approche équilibre sécurité et utilisabilité en appliquant des politiques différenciées.

```
net accounts | findstr "Seuil"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout"
auditpol /get /subcategory:"Account Lockout"
```

```
# Configuration différenciée par type de compte
net accounts /lockoutthreshold:5 /lockoutduration:30 /lockoutwindow:30
# Configuration avancée via registre pour comptes admin
New-Item -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\AccountLockout" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\AccountLockout" -Name "AdminLockoutThreshol
# Audit du verrouillage
auditpol /set /subcategory:"Account Lockout" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.4.1 *Surveillance des tentatives de verrouillage massives*

DESCRIPTION :
Les tentatives de verrouillage de comptes massives doivent être détectées et alertées comme indicateur d'attaque par déni de service.
Cette surveillance permet d'identifier les attaques visant à bloquer l'accès aux utilisateurs légitimes.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4740} -MaxEvents 50
Get-EventLog -LogName Security -InstanceId 644 -Newest 20
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4740} | Group-Object TimeCreated.Hour | Sort-Object Count -Descending
```

```
# Script de détection de verrouillage massif
$LockoutEvents = Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4740; StartTime=(Get-Date).AddHours(-1)}
if ($LockoutEvents.Count -gt 10) {
    Write-Warning "ALERTE: $($LockoutEvents.Count) verrouillages détectés dans la dernière heure"
    $LockoutEvents | Group-Object {$_.Properties[1].Value} | Sort-Object Count -Descending | Select-Object -First 5
}
# Configuration d'alertes automatiques
Register-WmiEvent -Query "SELECT * FROM Win32_NTLogEvent WHERE LogFile='Security' AND EventCode=4740" -Action {
    $Global:LockoutCounter++
    if ($Global:LockoutCounter -gt 5) {
        Write-Host "CRITICAL: Attaque de verrouillage détectée"
    }
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.5.1 *Configuration du déverrouillage automatique intelligent*

DESCRIPTION :
Le déverrouillage automatique doit être configuré de manière intelligente pour équilibrer sécurité et productivité utilisateur.
Cette configuration évite les blocages prolongés tout en maintenant la protection contre les attaques.

```
net accounts | findstr "Durée"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "LockoutDuration"
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4767} -MaxEvents 20
```

```
# Configuration du déverrouillage progressif
net accounts /lockoutduration:30
# Script de déverrouillage intelligent basé sur la source
$LockedAccounts = Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4740} | Where-Object {$_.TimeCreated -gt (Get-Date).AddMin
foreach ($Account in $LockedAccounts) {
    $SourceIP = $Account.Properties[19].Value
    # Vérifier si l'IP source est interne/fiable
    if ($SourceIP -match "^192\.168\.|^10\.|^172\.(1[6-9]|2[0-9]|3[01])\.") {
        Write-Host "Source interne détectée: $SourceIP - Déverrouillage anticipé possible"
    }
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.3.1 *Configuration de verrouillage intelligent par géolocalisation*

DESCRIPTION :
Le verrouillage de compte doit être adapté selon la géolocalisation de la tentative de connexion, avec des seuils plus stricts pour les connexions depuis des pays à risque.
Cette approche contextuelle améliore la sécurité tout en préservant l'expérience utilisateur pour les connexions légitimes.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625} -MaxEvents 50 | Select-Object TimeCreated, @{Name="SourceIP";Expressio
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "LockoutThreshold"
netsh advfirewall show currentprofile
```

```
# Configuration de verrouillage adaptatif par géolocalisation
$HighRiskCountries = @("CN", "RU", "KP", "IR")
$RecentFailures = Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625; StartTime=(Get-Date).AddHours(-1)}
foreach ($Failure in $RecentFailures) {
    $SourceIP = $Failure.Properties[19].Value
    # Simulation de géolocalisation (remplacer par vraie API)
    if ($SourceIP -notmatch "^192\.168\.|^10\.|^172\.(1[6-9]|2[0-9]|3[01])\.") {
        Write-Warning "Tentative de connexion externe depuis: $SourceIP"
        # Appliquer seuil plus strict (3 tentatives au lieu de 5)
        # Implémenter logique de géolocalisation avec MaxMind GeoIP ou similaire
    }
}
# Configuration pare-feu pour blocage géographique
Write-Host "Configuration recommandée: Déployer solution de géoblocage (Cloudflare, etc.)"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.4.1 *Analyse comportementale des patterns de connexion*

DESCRIPTION :
Les patterns de connexion inhabituels (horaires, fréquence, méthodes) doivent déclencher des vérifications supplémentaires avant verrouillage.
Cette analyse comportementale distingue les vraies attaques des anomalies légitimes d'usage.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4624,4625} -MaxEvents 200 | Group-Object @{Expression={$_.TimeCreated.Hour}}
Get-EventLog -LogName Security -InstanceId 4624 -After (Get-Date).AddDays(-7) | Group-Object UserName | Sort-Object Count -Descendi
query user /server:localhost
```

```
# Analyse des patterns de connexion
function Analyze-LoginPatterns {
    param([string]$UserName, [int]$DaysBack = 7)

    $LoginEvents = Get-WinEvent -FilterHashtable @{
        LogName="Security"
        ID=4624
        StartTime=(Get-Date).AddDays(-$DaysBack)
    } | Where-Object {$_.Properties[5].Value -eq $UserName}

    # Analyser les horaires habituels
    $TypicalHours = $LoginEvents | Group-Object {$_.TimeCreated.Hour} | Sort-Object Count -Descending | Select-Object -First 3

    # Détecter les anomalies
    $RecentLogin = $LoginEvents | Select-Object -First 1
    $IsAnomalous = $false

    if ($RecentLogin) {
        $CurrentHour = $RecentLogin.TimeCreated.Hour
        if ($CurrentHour -notin ($TypicalHours | ForEach-Object {$_.Name})) {
            $IsAnomalous = $true
            Write-Warning "Connexion à heure inhabituelle pour $UserName : $CurrentHour h"
        }
    }

    return @{
        TypicalHours = $TypicalHours
        IsAnomalous = $IsAnomalous
        RecentLoginCount = $LoginEvents.Count
    }
}
# Exemple d'usage
# Analyze-LoginPatterns -UserName "testuser"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.3 — Mécanismes de verrouillage adaptatif

4.3.1 *Verrouillage intelligent basé sur la géolocalisation*

DESCRIPTION :
Les seuils de verrouillage doivent être adaptés selon la géolocalisation des tentatives de connexion, avec des politiques plus strictes pour les connexions depuis des pays à haut risque.
Cette approche contextuelle améliore la sécurité sans impacter l'expérience utilisateur pour les connexions légitimes.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625} -MaxEvents 50 | Select-Object TimeCreated, @{Name="SourceIP";Expressio
net accounts | findstr /i "seuil"
Get-EventLog -LogName Security -InstanceId 4740 -Newest 10 | Select-Object TimeGenerated, ReplacementStrings
```

```
# Configuration de verrouillage adaptatif par géolocalisation
function Set-AdaptiveLockout {
    param(
        [string[]]$HighRiskCountries = @("CN", "RU", "KP", "IR", "SY"),
        [int]$NormalThreshold = 5,
        [int]$HighRiskThreshold = 3
    )

    Write-Host "=== CONFIGURATION VERROUILLAGE ADAPTATIF ==="

    # Analyser les tentatives de connexion récentes
    $RecentFailures = Get-WinEvent -FilterHashtable @{
        LogName="Security"
        ID=4625
        StartTime=(Get-Date).AddHours(-1)
    } -ErrorAction SilentlyContinue

    if ($RecentFailures) {
        $FailuresByIP = $RecentFailures | Group-Object {$_.Properties[19].Value}

        foreach ($IPGroup in $FailuresByIP) {
            $SourceIP = $IPGroup.Name
            $FailureCount = $IPGroup.Count

            # Déterminer si l'IP est externe (simplification)
            $IsExternal = -not ($SourceIP -match "^192\.168\.|^10\.|^172\.(1[6-9]|2[0-9]|3[01])\.")

            if ($IsExternal) {
                Write-Warning "IP externe avec $FailureCount échecs: $SourceIP"
                # TODO: Intégrer géolocalisation réelle (MaxMind GeoIP, etc.)

                # Appliquer seuil plus strict pour IPs externes
                if ($FailureCount -ge $HighRiskThreshold) {
                    Write-Host "  -> Seuil haut risque atteint, blocage recommandé"
                    # New-NetFirewallRule -DisplayName "GeoBlock-$SourceIP" -Direction Inbound -RemoteAddress $SourceIP -Action Blo
                }
            }
        }
    }

    # Configuration des seuils de base
    net accounts /lockoutthreshold:$NormalThreshold /lockoutduration:30 /lockoutwindow:30
    Write-Host "Seuil de verrouillage normal configuré: $NormalThreshold tentatives"
}
Set-AdaptiveLockout
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.3.2 *Analyse comportementale des patterns de connexion*

DESCRIPTION :
Les patterns de connexion inhabituels (horaires atypiques, fréquence anormale, nouvelles méthodes d'authentification) doivent déclencher des vérifications supplémentaires avant verrouillage complet.

Cette analyse comportementale permet de distinguer les vraies attaques des anomalies légitimes d'usage utilisateur.

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4624} -MaxEvents 200 | Group-Object @{Expression={$_.TimeCreated.Hour}} | So
Get-EventLog -LogName Security -InstanceId 4624 -After (Get-Date).AddDays(-7) | Group-Object UserName | Sort-Object Count -Descendi
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4624,4625} | Group-Object @{Expression={$_.TimeCreated.DayOfWeek}} | Sort-Ob
```

```
# Analyse comportementale des connexions
function Analyze-LoginBehavior {
    param(
        [string]$UserName = $null,
        [int]$DaysToAnalyze = 14
    )

    Write-Host "=== ANALYSE COMPORTEMENTALE DES CONNEXIONS ==="

    $StartDate = (Get-Date).AddDays(-$DaysToAnalyze)

    # Récupérer les événements de connexion
    $LoginEvents = Get-WinEvent -FilterHashtable @{
        LogName = "Security"
        ID = 4624
        StartTime = $StartDate
    } -ErrorAction SilentlyContinue

    if ($UserName) {
        $LoginEvents = $LoginEvents | Where-Object {$_.Properties[5].Value -eq $UserName}
        Write-Host "Analyse pour l'utilisateur: $UserName"
    }

    if ($LoginEvents) {
        # Analyser les patterns horaires
        $HourlyPattern = $LoginEvents | Group-Object {$_.TimeCreated.Hour} | Sort-Object Name
        Write-Host "\nPatterns horaires typiques:"
        $HourlyPattern | ForEach-Object {
            Write-Host "  $($_.Name)h: $($_.Count) connexions"
        }

        # Identifier les heures inhabituelles (en dehors des heures de bureau)
        $OffHoursLogins = $LoginEvents | Where-Object {
            $hour = $_.TimeCreated.Hour
            $hour -lt 7 -or $hour -gt 19  # En dehors de 7h-19h
        }

        if ($OffHoursLogins) {
            Write-Warning "Connexions en dehors des heures de bureau détectées: $($OffHoursLogins.Count)"
            $OffHoursLogins | Select-Object -First 5 | ForEach-Object {
                Write-Host "  $(Get-Date $_.TimeCreated -Format "yyyy-MM-dd HH:mm") - IP: $($_.Properties[18].Value)"
            }
        }

        # Analyser les connexions de weekend
        $WeekendLogins = $LoginEvents | Where-Object {
            $_.TimeCreated.DayOfWeek -eq "Saturday" -or $_.TimeCreated.DayOfWeek -eq "Sunday"
        }

        if ($WeekendLogins) {
            Write-Warning "Connexions de weekend détectées: $($WeekendLogins.Count)"
        }

        return @{
            TotalLogins = $LoginEvents.Count
            OffHoursCount = $OffHoursLogins.Count
            WeekendCount = $WeekendLogins.Count
            MostActiveHour = ($HourlyPattern | Sort-Object Count -Descending | Select-Object -First 1).Name
        }
    } else {
        Write-Host "Aucun événement de connexion trouvé pour la période analysée"
        return $null
    }
}
# Exemple d'utilisation
Analyze-LoginBehavior -DaysToAnalyze 7
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.4.1 *Seuils adaptatifs*

DESCRIPTION :
Configuration de seuils de verrouillage selon le contexte utilisateur.

```
# Commandes de vérification pour Seuils adaptatifs
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Seuils adaptatifs
Write-Host "Configuration de sécurité pour: Seuils adaptatifs"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.5.1 *Géolocalisation*

DESCRIPTION :
Verrouillage basé sur la localisation géographique des tentatives.

```
# Commandes de vérification pour Géolocalisation
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Géolocalisation
Write-Host "Configuration de sécurité pour: Géolocalisation"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.6.1 *Analyse comportementale*

DESCRIPTION :
Détection d'anomalies dans les patterns de connexion.

```
# Commandes de vérification pour Analyse comportementale
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Analyse comportementale
Write-Host "Configuration de sécurité pour: Analyse comportementale"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.7.1 *Protection DDoS*

DESCRIPTION :
Mesures anti-déni de service par verrouillage massif.

```
# Commandes de vérification pour Protection DDoS
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Protection DDoS
Write-Host "Configuration de sécurité pour: Protection DDoS"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.8.1 *Déverrouillage intelligent*

DESCRIPTION :
Mécanismes de déverrouillage basés sur la confiance.

```
# Commandes de vérification pour Déverrouillage intelligent
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Déverrouillage intelligent
Write-Host "Configuration de sécurité pour: Déverrouillage intelligent"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.9.1 *Notification temps réel*

DESCRIPTION :
Alertes immédiates lors de verrouillages suspects.

```
# Commandes de vérification pour Notification temps réel
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Notification temps réel
Write-Host "Configuration de sécurité pour: Notification temps réel"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

4.10.1 *Corrélation d'événements*

DESCRIPTION :
Analyse des patterns de verrouillage multi-comptes.

```
# Commandes de vérification pour Corrélation d'événements
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Corrélation d'événements
Write-Host "Configuration de sécurité pour: Corrélation d'événements"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

🔒 SECTION 5 : CONFIGURATION DES SERVICES

5.1 — Services de base Windows

5.1.1 *Service Telnet - Désactivé*

DESCRIPTION :
Le service Telnet doit être désactivé car il transmet les données, y compris les mots de passe, en texte clair sur le réseau. Ce service présente un risque de sécurité majeur.

Le protocole Telnet n'offre aucune protection cryptographique et peut être facilement intercepté par des attaquants.

```
Get-Service -Name "TlntSvr" -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
Get-WindowsFeature -Name "Telnet-Server" -ErrorAction SilentlyContinue
sc query TlntSvr
```

AUDIT :

- **GUI :** services.msc > Telnet > Propriétés > Type de démarrage
- **Valeur attendue :** Service non installé ou désactivé

REMÉDIATION :

1. **Désinstaller la fonctionnalité Telnet Server :**

```
# Désinstaller Telnet Server si installé
Disable-WindowsOptionalFeature -Online -FeatureName "TelnetServer" -NoRestart
Remove-WindowsFeature -Name "Telnet-Server" -ErrorAction SilentlyContinue
```

REMÉDIATION :

1. **Désactiver le service si présent :**

```
if (Get-Service -Name "TlntSvr" -ErrorAction SilentlyContinue) {
    Stop-Service -Name "TlntSvr" -Force -ErrorAction SilentlyContinue
    Set-Service -Name "TlntSvr" -StartupType Disabled
}
```

VALEUR PAR DÉFAUT :
Non installé par défaut sur Windows 11

5.1.2 *Service FTP - Sécurisé ou désactivé*

DESCRIPTION :
Le service FTP (File Transfer Protocol) doit être désactivé ou strictement sécurisé s'il est nécessaire. FTP transmet par défaut les identifiants en texte clair.
Si FTP est requis, utiliser FTPS (FTP over SSL/TLS) ou SFTP (SSH File Transfer Protocol).

```
Get-Service -Name "FTPSVC" -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
Get-WindowsFeature -Name "IIS-FTPServer" -ErrorAction SilentlyContinue
```

AUDIT :

- **GUI :** services.msc > Microsoft FTP Service
- **Valeur attendue :** Service non installé ou désactivé

REMÉDIATION :

1. **Désinstaller IIS FTP Server :**

```
Disable-WindowsOptionalFeature -Online -FeatureName "IIS-FTPServer" -NoRestart
```

REMÉDIATION :

1. **Si FTP nécessaire, configurer FTPS :**

```
# Configuration sécurisée (exemple pour IIS)
# Require SSL/TLS pour toutes les connexions FTP
Import-Module WebAdministration
Set-WebConfigurationProperty -PSPath 'MACHINE/WEBROOT/APPHOST' -Filter "system.webServer/security/access" -Name "sslFlags" -Value "
```

VALEUR PAR DÉFAUT :
Non installé par défaut

5.1.3 *Service TFTP - Désactivé*

DESCRIPTION :
Le service TFTP (Trivial File Transfer Protocol) doit être désactivé. TFTP ne propose aucune authentification ni chiffrement et permet des transferts de fichiers non sécurisés.

```
Get-Service -Name "TFTP" -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
Get-WindowsFeature -Name "TFTP-Client" -ErrorAction SilentlyContinue
```

```
# Désinstaller TFTP Client si présent
Disable-WindowsOptionalFeature -Online -FeatureName "TFTP-Client" -NoRestart
```

VALEUR PAR DÉFAUT :
Non installé par défaut

5.1.4 *Service Windows Remote Management (WinRM) - Sécurisé*

DESCRIPTION :
Le service WinRM doit être configuré de manière sécurisée s'il est utilisé pour l'administration à distance. La configuration par défaut peut présenter des risques de sécurité.

```
Get-Service -Name "WinRM" | Select-Object Name, Status, StartType
winrm get winrm/config
Get-WSManInstance -ResourceURI winrm/config/listener -SelectorSet @{Address="*";Transport="HTTP"}
```

AUDIT :

- **Valeur attendue :** HTTPS uniquement, authentification Kerberos, pas de HTTP

REMÉDIATION :

1. **Configuration sécurisée de WinRM :**

```
# Configurer WinRM pour HTTPS uniquement
winrm delete winrm/config/Listener?Address=*+Transport=HTTP
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="ComputerName";CertificateThumbprint="ThumbprintValue"}

# Désactiver l'authentification de base
winrm set winrm/config/service/auth @{Basic="false"}
winrm set winrm/config/client/auth @{Basic="false"}

# Configurer le chiffrement
winrm set winrm/config/service @{AllowUnencrypted="false"}
```

VALEUR PAR DÉFAUT :
Démarrage manuel

5.1.5 *Service Print Spooler - Sécurisé*

DESCRIPTION :
Le service Print Spooler (Spooler) doit être désactivé s'il n'est pas utilisé ou sécurisé contre les vulnérabilités connues (PrintNightmare, etc.). Ce service a été la cible de nombreuses exploitations.

```
Get-Service -Name "Spooler" | Select-Object Name, Status, StartType
Get-PrinterDriver | Select-Object Name, InfPath, Manufacturer
```

REMÉDIATION :

1. **Si l'impression n'est pas nécessaire, désactiver :**

```
Stop-Service -Name "Spooler" -Force
Set-Service -Name "Spooler" -StartupType Disabled
```

REMÉDIATION :

1. **Si l'impression est nécessaire, sécuriser :**

```
# Désactiver l'installation de pilotes non-administrateurs
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers' -Name 'AddPrinterDriv

# Restriction des fonctions Point and Print
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint' -Name 'RestrictDriverInstallationToAdm
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint' -Name 'NoWarningNoElevationOnInstall'
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint' -Name 'UpdatePromptSettings' -Value 0
```

VALEUR PAR DÉFAUT :
Démarrage automatique
5.2 — Services réseau

5.2.1 *Service Server Message Block (SMB) v1 - Désactivé*

DESCRIPTION :
Le protocole SMB v1 doit être complètement désactivé. Il présente de nombreuses vulnérabilités critiques et a été utilisé dans des attaques majeures comme WannaCry et NotPetya.
SMB v1 n'offre pas de chiffrement moderne et est vulnérable aux attaques man-in-the-middle.

```
Get-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol"
Get-SmbServerConfiguration | Select-Object EnableSMB1Protocol
sc.exe qc lanmanserver | findstr START_TYPE
```

AUDIT :

- **Valeur attendue :** SMB1Protocol désactivé ou non installé

REMÉDIATION :

1. **Désactiver SMB v1 complètement :**

```
# Désactiver la fonctionnalité SMB1
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart

# Désactiver SMB v1 au niveau serveur
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force

# Désactiver au niveau client
sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi
sc.exe config mrxsmb10 start= disabled
```

REMÉDIATION :

1. **Vérification de la désactivation :**

```
Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol | Select-Object State
Get-SmbServerConfiguration | Select-Object EnableSMB1Protocol
```

VALEUR PAR DÉFAUT :
Désactivé par défaut sur Windows 11

5.2.2 *Service Windows Remote Desktop - Sécurisé*

DESCRIPTION :
Le service Remote Desktop (Bureau à distance) doit être désactivé si non utilisé, ou sécurisé avec NLA (Network Level Authentication) et un chiffrement fort s'il est nécessaire.

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server' -Name 'fDenyTSConnections'
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name 'UserAuthentication'
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name 'MinEncryptionLevel'
```

AUDIT :

- **Valeur attendue :** fDenyTSConnections = 1 (désactivé) OU UserAuthentication = 1 et MinEncryptionLevel = 3

REMÉDIATION :

1. **Si RDP non nécessaire, désactiver complètement :**

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server' -Name 'fDenyTSConnections' -Value 1 -Type DWord
```

REMÉDIATION :

1. **Si RDP nécessaire, sécuriser :**

```
# Activer Network Level Authentication
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name 'UserAuthentication' -Val

# Forcer le chiffrement de niveau élevé
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name 'MinEncryptionLevel' -Val

# Désactiver la redirection des lecteurs
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services' -Name 'fDisableCdm' -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
Désactivé par défaut

5.2.3 *Service Windows Search - Restreint*

DESCRIPTION :
Le service Windows Search doit être configuré pour ne pas indexer les données sensibles et restreindre l'accès à distance à l'index de recherche.

```
Get-Service -Name "WSearch" | Select-Object Name, Status, StartType
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Windows Search' -Name 'AllowIndexingEncryptedStoresOrItems' -Erro
```

```
# Désactiver l'indexation des éléments chiffrés
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Windows Search' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Windows Search' -Name 'AllowIndexingEncryptedStoresOrItems' -Valu

# Désactiver l'indexation sur les partages réseau
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Windows Search' -Name 'PreventIndexingOutlook' -Value 1 -Type DWo
```

VALEUR PAR DÉFAUT :
Démarrage automatique (retardé)

5.3 — Services de sécurité essentiels

5.3.1 *Windows Defender Antivirus - Activé*

DESCRIPTION :
Le service Windows Defender Antivirus doit être activé et fonctionnel sauf si remplacé par une solution antivirus tiers compatible et approuvée.

```
Get-Service -Name "WinDefend" | Select-Object Name, Status, StartType
Get-MpComputerStatus | Select-Object AntivirusEnabled, RealTimeProtectionEnabled, OnAccessProtectionEnabled
Get-MpPreference | Select-Object DisableRealtimeMonitoring
```

```
# S'assurer que Windows Defender est activé
Set-Service -Name "WinDefend" -StartupType Automatic
Start-Service -Name "WinDefend"

# Activer la protection en temps réel
Set-MpPreference -DisableRealtimeMonitoring $false

# Configurer les scans automatiques
Set-MpPreference -ScanScheduleDay Everyday -ScanScheduleTime 120
```

VALEUR PAR DÉFAUT :
Activé par défaut

5.3.2 *Windows Security Center - Activé*

DESCRIPTION :
Le service Security Center surveille l'état des fonctionnalités de sécurité et doit rester activé pour assurer le monitoring continu de la sécurité du système.

```
Get-Service -Name "wscsvc" | Select-Object Name, Status, StartType
Get-Service -Name "SecurityHealthService" | Select-Object Name, Status, StartType
```

```
Set-Service -Name "wscsvc" -StartupType Automatic
Set-Service -Name "SecurityHealthService" -StartupType Automatic
Start-Service -Name "wscsvc" -ErrorAction SilentlyContinue
Start-Service -Name "SecurityHealthService" -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
Démarrage automatique

5.4.1 *Durcissement des services système critiques*

DESCRIPTION :
Les services système critiques doivent être durcis avec des configurations de sécurité renforcées et des comptes de service dédiés.
Cette mesure limite l'impact potentiel d'une compromission de service sur le système global.

```
Get-Service | Where-Object {$_.Status -eq "Running" -and $_.ServiceType -eq "Win32ShareProcess"} | Select-Object Name, StartType, S
sc query type= service state= all | findstr "SERVICE_NAME"
Get-WmiObject Win32_Service | Where-Object {$_.StartMode -eq "Auto" -and $_.State -eq "Running"} | Select-Object Name, StartName, P
```

```
# Audit et durcissement des services critiques
$CriticalServices = @("Winmgmt", "RpcSs", "Dhcp", "Dnscache", "EventLog", "PlugPlay", "PolicyAgent", "ProfSvc", "Schedule", "SENS",
foreach ($ServiceName in $CriticalServices) {
    $Service = Get-Service -Name $ServiceName -ErrorAction SilentlyContinue
    if ($Service) {
        # Vérification du compte de service
        $ServiceInfo = Get-WmiObject Win32_Service -Filter "Name='$ServiceName'"
        Write-Host "Service: $ServiceName - Compte: $($ServiceInfo.StartName) - État: $($Service.Status)"
    }
}
# Configuration des ACL sur les services sensibles
sc sdset Winmgmt "D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.5.1 *Désactivation des services non essentiels*

DESCRIPTION :
Tous les services non essentiels au fonctionnement du système doivent être désactivés pour réduire la surface d'attaque.
Cette approche minimise les points d'entrée potentiels pour les attaquants.

```
Get-Service | Where-Object {$_.StartType -eq "Automatic" -and $_.Status -eq "Stopped"} | Select-Object Name, StartType, Status
Get-Service | Where-Object {$_.Name -like "*telemetry*" -or $_.Name -like "*xbox*" -or $_.Name -like "*fax*"}
sc query type= service state= all | findstr /i "unnecessary"
```

```
# Liste des services couramment non essentiels
$UnnecessaryServices = @(
    "Fax", "XblAuthManager", "XblGameSave", "XboxNetApiSvc", "XboxGipSvc",
    "RetailDemo", "MapsBroker", "lfsvc", "WalletService", "PhoneSvc",
    "icssvc", "SEMgrSvc", "PcaSvc", "WpcMonSvc", "WbioSrvc"
)
foreach ($ServiceName in $UnnecessaryServices) {
    $Service = Get-Service -Name $ServiceName -ErrorAction SilentlyContinue
    if ($Service -and $Service.StartType -ne "Disabled") {
        Stop-Service -Name $ServiceName -Force -ErrorAction SilentlyContinue
        Set-Service -Name $ServiceName -StartupType Disabled
        Write-Host "Service désactivé: $ServiceName"
    }
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.4.1 *Isolation des services critiques via conteneurisation*

DESCRIPTION :
Les services système critiques doivent être isolés dans des conteneurs ou machines virtuelles dédiées pour limiter l'impact d'une compromission.
Cette isolation réduit les risques de mouvement latéral et de compromission en cascade.

```
Get-WindowsOptionalFeature -Online -FeatureName "Containers" | Select-Object State
Get-WindowsOptionalFeature -Online -FeatureName "Microsoft-Hyper-V-All" | Select-Object State
Get-Service | Where-Object {$_.ServiceType -eq "Win32ShareProcess"} | Measure-Object
```

```
# Activation des conteneurs Windows
Enable-WindowsOptionalFeature -Online -FeatureName "Containers" -All -NoRestart
# Installation Docker (si applicable)
Write-Host "Pour isolation complète, considérer:"
Write-Host "1. Docker Desktop pour Windows"
Write-Host "2. Windows Sandbox pour tests"
Write-Host "3. Hyper-V pour isolation VM"
# Configuration services en mode isolé
$CriticalServices = @("Winmgmt", "EventLog", "RpcSs")
foreach ($Service in $CriticalServices) {
    $ServiceInfo = Get-WmiObject Win32_Service -Filter "Name='$Service'"
    if ($ServiceInfo.StartName -eq "LocalSystem") {
        Write-Host "Service $Service fonctionne avec privilèges élevés - Considérer isolation"
    }
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.5.1 *Surveillance en temps réel des modifications de services*

DESCRIPTION :
Toutes les modifications de services (création, suppression, changement de configuration) doivent être surveillées et alertées en temps réel.
Cette surveillance permet de détecter rapidement les tentatives de persistance malveillante.

```
Get-WinEvent -FilterHashtable @{LogName="System"; ID=7034,7035,7036,7040} -MaxEvents 50
auditpol /get /subcategory:"Security System Extension"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\*" | Measure-Object
```

```
# Configuration de surveillance des services
auditpol /set /subcategory:"Security System Extension" /success:enable /failure:enable
auditpol /set /subcategory:"System Integrity" /success:enable /failure:enable
# Script de surveillance temps réel
Register-WmiEvent -Class Win32_Service -SourceIdentifier "ServiceMonitor" -Action {
    $Service = $Event.SourceEventArgs.NewEvent
    Write-Warning "Modification de service détectée: $($Service.Name)"
    Write-Host "État: $($Service.State), Mode démarrage: $($Service.StartMode)"
}
# Surveillance des créations de nouveaux services
Register-WmiEvent -Query "SELECT * FROM Win32_ServiceChangeEvent" -Action {
    Write-Host "ALERT: Changement de service système détecté"
    Get-Service | Sort-Object Name | Format-Table -AutoSize
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.6.1 *Contrôle des dépendances entre services*

DESCRIPTION :
Les dépendances entre services doivent être auditées et minimisées pour éviter les cascades de défaillance et les vecteurs d'attaque en chaîne.
Cette approche renforce la résilience du système et limite la propagation des compromissions.

```
Get-Service | ForEach-Object { Get-Service -DependentServices $_.Name | Where-Object {$_.Status -eq "Running"} } | Group-Object Ser
sc query type= service state= all | findstr "SERVICE_NAME"
Get-WmiObject Win32_DependentService | Select-Object Antecedent, Dependent
```

```
# Analyse des dépendances de services
function Get-ServiceDependencyMap {
    $AllServices = Get-Service
    $DependencyMap = @{}

    foreach ($Service in $AllServices) {
        $Dependencies = Get-Service -Name $Service.Name | Select-Object -ExpandProperty ServicesDependedOn
        $Dependents = Get-Service -DependentServices $Service.Name

        $DependencyMap[$Service.Name] = @{
            Dependencies = $Dependencies.Name
            Dependents = $Dependents.Name
            Status = $Service.Status
            StartType = $Service.StartType
        }
    }

    return $DependencyMap
}
$ServiceMap = Get-ServiceDependencyMap
# Identifier les services avec nombreuses dépendances
$ServiceMap.GetEnumerator() | Where-Object {$_.Value.Dependencies.Count -gt 5} | ForEach-Object {
    Write-Warning "Service avec nombreuses dépendances: $($_.Key) ($($_.Value.Dependencies.Count) dépendances)"
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration
5.4 — Durcissement et surveillance des services

5.4.1 *Isolation et sandboxing des services critiques*

DESCRIPTION :
Les services système critiques doivent être isolés dans des environnements sandboxés ou conteneurisés pour limiter l'impact d'une compromission et empêcher la propagation latérale.
Cette isolation constitue une couche de défense en profondeur contre les attaques de type privilege escalation et code injection.

```
Get-Service | Where-Object {$_.ServiceType -eq "Win32ShareProcess"} | Select-Object Name, Status, StartType, ServiceType
Get-WindowsOptionalFeature -Online -FeatureName "Containers*" | Where-Object {$_.State -eq "Enabled"}
Get-WmiObject Win32_Service | Where-Object {$_.StartName -eq "LocalSystem"} | Measure-Object
```

```
# Configuration d'isolation des services critiques
Write-Host "=== ISOLATION DES SERVICES CRITIQUES ==="

# Activation des fonctionnalités d'isolation
try {
    Enable-WindowsOptionalFeature -Online -FeatureName "Containers" -All -NoRestart
    Write-Host "Fonctionnalité Containers activée"
} catch {
    Write-Warning "Impossible d'activer les containers: $_"
}

# Audit des services critiques fonctionnant avec LocalSystem
$CriticalServices = @("Winmgmt", "RpcSs", "EventLog", "PlugPlay", "PolicyAgent", "SENS", "Schedule")
Write-Host "\nAudit des services critiques:"
foreach ($ServiceName in $CriticalServices) {
    $Service = Get-WmiObject Win32_Service -Filter "Name='$ServiceName'"
    if ($Service) {
        $SecurityLevel = switch ($Service.StartName) {
            "LocalSystem" { "🔴 CRITIQUE - Privilèges maximum" }
            "NT AUTHORITY\LocalService" { "🟠 MOYEN - Privilèges limités" }
            "NT AUTHORITY\NetworkService" { "🟢 BON - Privilèges réseau uniquement" }
            default { "🟡 CUSTOM - $($Service.StartName)" }
        }
        Write-Host "  $ServiceName : $SecurityLevel"
    }
}

# Configuration Windows Defender Application Guard (si disponible)
if (Get-WindowsOptionalFeature -Online -FeatureName "Windows-Defender-ApplicationGuard" -ErrorAction SilentlyContinue) {
    Write-Host "\nWindows Defender Application Guard disponible pour isolation"
}

# Recommandations d'isolation avancée
Write-Host "\n=== RECOMMANDATIONS ISOLATION AVANCÉE ==="
Write-Host "1. Utiliser Windows Sandbox pour tests de sécurité"
Write-Host "2. Configurer Hyper-V pour isolation VM des services sensibles"
Write-Host "3. Implémenter Docker Windows containers pour isolation applicative"
Write-Host "4. Configurer des comptes de service dédiés (non LocalSystem)"
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.4.2 *Surveillance temps réel des modifications de services*

DESCRIPTION :
Toutes les modifications de services (installation, suppression, changement de configuration, modification des comptes de service) doivent être surveillées et alertées en temps réel.

Cette surveillance permet de détecter rapidement les tentatives de persistance malveillante et les modifications non autorisées du système.

```
Get-WinEvent -FilterHashtable @{LogName="System"; ID=7034,7035,7036,7040} -MaxEvents 20
auditpol /get /subcategory:"Security System Extension"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\*" | Measure-Object | Select-Object Count
```

```
# Configuration de surveillance complète des services
Write-Host "=== CONFIGURATION SURVEILLANCE SERVICES ==="

# Activation de l'audit des extensions système
auditpol /set /subcategory:"Security System Extension" /success:enable /failure:enable
auditpol /set /subcategory:"System Integrity" /success:enable /failure:enable
Write-Host "Audit des services système activé"

# Création d'un monitoring WMI en temps réel
function Start-ServiceMonitoring {
    Write-Host "Démarrage du monitoring des services en temps réel..."

    # Surveillance des changements d'état des services
    Register-WmiEvent -Query "SELECT * FROM Win32_ServiceChangeEvent" -SourceIdentifier "ServiceChangeMonitor" -Action {
        $ServiceName = $Event.SourceEventArgs.NewEvent.ServiceName
        Write-Warning "ALERTE SERVICE: Changement détecté sur le service $ServiceName"

        # Obtenir les détails du service modifié
        try {
            $ServiceDetails = Get-WmiObject Win32_Service -Filter "Name='$ServiceName'"
            Write-Host "  Nom: $($ServiceDetails.Name)"
            Write-Host "  État: $($ServiceDetails.State)"
            Write-Host "  Mode démarrage: $($ServiceDetails.StartMode)"
            Write-Host "  Compte: $($ServiceDetails.StartName)"
            Write-Host "  Chemin: $($ServiceDetails.PathName)"
        } catch {
            Write-Host "  Erreur lors de la récupération des détails du service"
        }
    }

    # Surveillance des créations/suppressions de services
    Register-WmiEvent -Query "SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_Service'" -SourceIdent
        $NewService = $Event.SourceEventArgs.NewEvent.TargetInstance
        Write-Warning "NOUVEAU SERVICE CRÉÉ: $($NewService.Name)"
        Write-Host "  Chemin: $($NewService.PathName)"
        Write-Host "  Compte: $($NewService.StartName)"
    }

    Register-WmiEvent -Query "SELECT * FROM __InstanceDeletionEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_Service'" -SourceIdent
        $DeletedService = $Event.SourceEventArgs.NewEvent.TargetInstance
        Write-Warning "SERVICE SUPPRIMÉ: $($DeletedService.Name)"
    }

    Write-Host "Monitoring actif. Utilisez Stop-ServiceMonitoring pour arrêter."
}

function Stop-ServiceMonitoring {
    Unregister-Event -SourceIdentifier "ServiceChangeMonitor" -ErrorAction SilentlyContinue
    Unregister-Event -SourceIdentifier "ServiceCreationMonitor" -ErrorAction SilentlyContinue
    Unregister-Event -SourceIdentifier "ServiceDeletionMonitor" -ErrorAction SilentlyContinue
    Write-Host "Monitoring des services arrêté"
}

# Snapshot initial des services pour détection de changements
$InitialServices = Get-Service | Select-Object Name, Status, StartType | ConvertTo-Json
Set-Content -Path "C:\temp\services_baseline.json" -Value $InitialServices
Write-Host "Baseline des services sauvegardée dans C:\temp\services_baseline.json"

# Démarrer le monitoring (décommenter pour activer)
# Start-ServiceMonitoring
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.4.3 *Contrôle des dépendances et de la surface d'attaque*

DESCRIPTION :

Les dépendances entre services doivent être auditées, minimisées et sécurisées pour éviter les cascades de défaillance et limiter les vecteurs d'escalade de privilège en chaîne.

Cette approche renforce la résilience du système et limite la propagation des compromissions entre services.

```
Get-Service | ForEach-Object { Get-Service -DependentServices $_.Name -ErrorAction SilentlyContinue } | Where-Object {$_.Status -eq
sc query type= service state= all | findstr "SERVICE_NAME DISPLAY_NAME"
Get-WmiObject Win32_DependentService | Select-Object Antecedent, Dependent -First 10
```

```
# Analyse complète des dépendances de services
function Analyze-ServiceDependencies {
    Write-Host "=== ANALYSE DES DÉPENDANCES DE SERVICES ==="

    $AllServices = Get-Service
    $DependencyReport = @()

    foreach ($Service in $AllServices) {
        try {
            $Dependencies = Get-Service -Name $Service.Name | Select-Object -ExpandProperty ServicesDependedOn -ErrorAction Silentl
            $Dependents = Get-Service -DependentServices $Service.Name -ErrorAction SilentlyContinue

            $ServiceInfo = [PSCustomObject]@{
                ServiceName = $Service.Name
                Status = $Service.Status
                StartType = $Service.StartType
                DependsOnCount = ($Dependencies | Measure-Object).Count
                DependsOn = ($Dependencies.Name -join ", ")
                DependentCount = ($Dependents | Measure-Object).Count
                Dependents = ($Dependents.Name -join ", ")
                RiskScore = 0
            }

            # Calculer le score de risque
            if ($ServiceInfo.DependsOnCount -gt 5) { $ServiceInfo.RiskScore += 2 }
            if ($ServiceInfo.DependentCount -gt 5) { $ServiceInfo.RiskScore += 3 }
            if ($Service.StartType -eq "Automatic" -and $Service.Status -eq "Running") { $ServiceInfo.RiskScore += 1 }

            $DependencyReport += $ServiceInfo
        } catch {
            Write-Warning "Erreur analyse service $($Service.Name): $_"
        }
    }

    # Rapport des services à haut risque
    Write-Host "\n=== SERVICES À HAUT RISQUE ==="
    $HighRiskServices = $DependencyReport | Where-Object {$_.RiskScore -gt 3} | Sort-Object RiskScore -Descending

    foreach ($RiskService in $HighRiskServices) {
        Write-Warning "Service haut risque: $($RiskService.ServiceName) (Score: $($RiskService.RiskScore))"
        if ($RiskService.DependsOnCount -gt 5) {
            Write-Host "  Dépend de $($RiskService.DependsOnCount) services: $($RiskService.DependsOn)"
        }
        if ($RiskService.DependentCount -gt 5) {
            Write-Host "  $($RiskService.DependentCount) services dépendent de lui: $($RiskService.Dependents)"
        }
    }

    # Services inutiles ou non critiques à désactiver
    Write-Host "\n=== SERVICES POTENTIELLEMENT INUTILES ==="
    $UnnecessaryServices = @(
        "Fax", "XblAuthManager", "XblGameSave", "XboxNetApiSvc", "XboxGipSvc",
        "RetailDemo", "MapsBroker", "lfsvc", "WalletService", "PhoneSvc",
        "icssvc", "SEMgrSvc", "WbioSrvc", "WpcMonSvc"
    )

    foreach ($ServiceName in $UnnecessaryServices) {
        $Service = Get-Service -Name $ServiceName -ErrorAction SilentlyContinue
        if ($Service) {
            $Status = if ($Service.StartType -eq "Disabled") { "✅ Désactivé" } else { "⚠️ Actif" }
            Write-Host "  $ServiceName : $Status"

            if ($Service.StartType -ne "Disabled") {
                Write-Host "    Recommandation: Désactiver avec Stop-Service -Name $ServiceName; Set-Service -Name $ServiceName -St
            }
        }
    }

    return $DependencyReport
}

# Lancer l'analyse
$DependencyReport = Analyze-ServiceDependencies

# Exporter le rapport
$DependencyReport | Export-Csv -Path "C:\temp\service_dependency_report.csv" -NoTypeInformation
Write-Host "\nRapport sauvegardé dans C:\temp\service_dependency_report.csv"
```

VALEUR PAR DÉFAUT :

Variable selon la configuration

5.5.1 *Isolation processus*

DESCRIPTION :
Séparation des services critiques dans des contextes isolés.

```
# Commandes de vérification pour Isolation processus
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Isolation processus
Write-Host "Configuration de sécurité pour: Isolation processus"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.6.1 *Surveillance temps réel*

DESCRIPTION :
Monitoring continu des modifications de services.

```
# Commandes de vérification pour Surveillance temps réel
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Surveillance temps réel
Write-Host "Configuration de sécurité pour: Surveillance temps réel"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.7.1 *Contrôle dépendances*

DESCRIPTION :
Audit et minimisation des dépendances entre services.

```
# Commandes de vérification pour Contrôle dépendances
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle dépendances
Write-Host "Configuration de sécurité pour: Contrôle dépendances"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.8.1 *Comptes dédiés*

DESCRIPTION :
Attribution de comptes de service spécifiques et non privilégiés.

```
# Commandes de vérification pour Comptes dédiés
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Comptes dédiés
Write-Host "Configuration de sécurité pour: Comptes dédiés"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.9.1 *Chiffrement communications*

DESCRIPTION :
Protection des communications inter-services.

```
# Commandes de vérification pour Chiffrement communications
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Chiffrement communications
Write-Host "Configuration de sécurité pour: Chiffrement communications"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.10.1 *Audit d'installation*

DESCRIPTION :
Traçage de toute installation ou modification de service.

```
# Commandes de vérification pour Audit d'installation
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Audit d'installation
Write-Host "Configuration de sécurité pour: Audit d'installation"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.11.1 *Validation d'intégrité*

DESCRIPTION :
Vérification cryptographique de l'intégrité des services.

```
# Commandes de vérification pour Validation d'intégrité
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Validation d'intégrité
Write-Host "Configuration de sécurité pour: Validation d'intégrité"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.12.1 *Limitation ressources*

DESCRIPTION :
Contrôle de la consommation de ressources par service.

```
# Commandes de vérification pour Limitation ressources
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Limitation ressources
Write-Host "Configuration de sécurité pour: Limitation ressources"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.13.1 *Redémarrage sécurisé*

DESCRIPTION :
Procédures de redémarrage sécurisé des services critiques.

```
# Commandes de vérification pour Redémarrage sécurisé
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Redémarrage sécurisé
Write-Host "Configuration de sécurité pour: Redémarrage sécurisé"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.14.1 *Sauvegarde configuration*

DESCRIPTION :
Backup automatique des configurations de services.

```
# Commandes de vérification pour Sauvegarde configuration
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Sauvegarde configuration
Write-Host "Configuration de sécurité pour: Sauvegarde configuration"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.15.1 *Détection d'anomalies*

DESCRIPTION :
Surveillance comportementale des services pour détecter les compromissions.

```
# Commandes de vérification pour Détection d'anomalies
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Détection d'anomalies
Write-Host "Configuration de sécurité pour: Détection d'anomalies"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.16.1 *Containerisation*

DESCRIPTION :
Déploiement de services critiques dans des conteneurs sécurisés.

```
# Commandes de vérification pour Containerisation
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Containerisation
Write-Host "Configuration de sécurité pour: Containerisation"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.17.1 *Rotation des secrets*

DESCRIPTION :
Renouvellement automatique des secrets utilisés par les services.

```
# Commandes de vérification pour Rotation des secrets
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Rotation des secrets
Write-Host "Configuration de sécurité pour: Rotation des secrets"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.18.1 *Contrôle réseau*

DESCRIPTION :
Limitation et surveillance du trafic réseau des services.

```
# Commandes de vérification pour Contrôle réseau
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle réseau
Write-Host "Configuration de sécurité pour: Contrôle réseau"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.19.1 *Logging étendu*

DESCRIPTION :
Journalisation détaillée des activités de tous les services.

```
# Commandes de vérification pour Logging étendu
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Logging étendu
Write-Host "Configuration de sécurité pour: Logging étendu"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

5.20.1 *Récupération rapide*

DESCRIPTION :
Mécanismes de récupération automatique en cas de défaillance.

```
# Commandes de vérification pour Récupération rapide
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Récupération rapide
Write-Host "Configuration de sécurité pour: Récupération rapide"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

🔒 SECTION 6 : PARE-FEU WINDOWS DEFENDER

6.1 — Configuration des profils de pare-feu

6.1.1 *Profil Domaine - Activé*

DESCRIPTION :
Le profil domaine du pare-feu Windows Defender doit être activé pour protéger les communications lorsque l'ordinateur est connecté à un domaine Active Directory.

```
Get-NetFirewallProfile -Name Domain | Select-Object Name, Enabled, DefaultInboundAction, DefaultOutboundAction
netsh advfirewall show domain
```

AUDIT :

- **GUI :** Windows Defender Firewall > Activer/désactiver le Pare-feu Windows Defender > Paramètres du réseau de domaine
- **Valeur attendue :** Enabled = True, DefaultInboundAction = Block, DefaultOutboundAction = Allow

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Domain Profile\Firewall state → On
2. **PowerShell :**

```
Set-NetFirewallProfile -Name Domain -Enabled True
Set-NetFirewallProfile -Name Domain -DefaultInboundAction Block
Set-NetFirewallProfile -Name Domain -DefaultOutboundAction Allow
```

REMÉDIATION :

1. **Netsh :**

```
netsh advfirewall set domainprofile state on
netsh advfirewall set domainprofile firewallpolicy blockinbound,allowoutbound
```

VALEUR PAR DÉFAUT :
Activé

6.1.2 *Profil Privé - Activé*

DESCRIPTION :
Le profil privé du pare-feu doit être activé pour protéger les communications sur les réseaux privés (domicile, bureau).

```
Get-NetFirewallProfile -Name Private | Select-Object Name, Enabled, DefaultInboundAction, DefaultOutboundAction
```

```
Set-NetFirewallProfile -Name Private -Enabled True
Set-NetFirewallProfile -Name Private -DefaultInboundAction Block
Set-NetFirewallProfile -Name Private -DefaultOutboundAction Allow
```

VALEUR PAR DÉFAUT :
Activé

6.1.3 *Profil Public - Activé avec restrictions renforcées*

DESCRIPTION :
Le profil public doit être activé avec des restrictions maximales pour protéger le système sur les réseaux non fiables (WiFi public, etc.).

```
Get-NetFirewallProfile -Name Public | Select-Object Name, Enabled, DefaultInboundAction, DefaultOutboundAction, NotifyOnListen
```

```
Set-NetFirewallProfile -Name Public -Enabled True
Set-NetFirewallProfile -Name Public -DefaultInboundAction Block
Set-NetFirewallProfile -Name Public -DefaultOutboundAction Allow
Set-NetFirewallProfile -Name Public -NotifyOnListen True
```

VALEUR PAR DÉFAUT :
Activé

6.2 — Journalisation du pare-feu

6.2.1 *Journalisation des connexions bloquées - Activée*

DESCRIPTION :
La journalisation des connexions bloquées doit être activée pour tous les profils de pare-feu afin de permettre l'analyse forensique et la détection d'incidents.

```
Get-NetFirewallProfile | Select-Object Name, LogBlocked, LogAllowed, LogFileName, LogMaxSizeKilobytes
```

```
# Configurer la journalisation pour tous les profils
Set-NetFirewallProfile -All -LogBlocked True -LogAllowed False
Set-NetFirewallProfile -All -LogFileName "C:\Windows\System32\LogFiles\Firewall\pfirewall.log"
Set-NetFirewallProfile -All -LogMaxSizeKilobytes 4096
```

VALEUR PAR DÉFAUT :
Journalisation désactivée

6.2.2 *Restriction des règles de pare-feu utilisateur*

DESCRIPTION :
Les utilisateurs non-administrateurs ne doivent pas pouvoir créer ou modifier les règles de pare-feu pour maintenir l'intégrité de la politique de sécurité.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile' -Name 'AllowLocalPolicyMerge' -ErrorAction
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile' -Name 'AllowLocalIPSecPolicyMerge' -ErrorA
```

```
# Empêcher la fusion des politiques locales
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile' -Name 'AllowLocalPolicyMerge' -Value 0 -Ty
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile' -Name 'AllowLocalIPSecPolicyMerge' -Value

# Même configuration pour les autres profils
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile' -Name 'AllowLocalPolicyMerge' -Value 0 -T

New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile' -Name 'AllowLocalPolicyMerge' -Value 0 -Ty
```

VALEUR PAR DÉFAUT :
Fusion autorisée

6.3.1 *Configuration de règles pare-feu basées sur la réputation IP*

DESCRIPTION :
Le pare-feu doit intégrer des flux de threat intelligence pour bloquer automatiquement les adresses IP malveillantes connues.
Cette protection proactive bloque les connexions depuis des sources compromises avant qu'elles n'atteignent les services.

```
Get-NetFirewallRule | Where-Object {$_.Direction -eq "Inbound" -and $_.Action -eq "Block"} | Measure-Object
netsh advfirewall firewall show rule name=all | findstr "Block"
Get-MpThreatDetection | Select-Object ThreatName, Resources -First 10
```

```
# Configuration de blocage IP basé sur réputation
$ThreatIntelFeeds = @(
    "https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/firehol_level1.netset",
    "https://www.spamhaus.org/drop/drop.txt"
)
# Script de mise à jour automatique des listes de blocage
function Update-ThreatIntelligence {
    try {
        $BlockedIPs = @()
        # Exemple avec liste Spamhaus DROP
        $DropList = Invoke-WebRequest -Uri "https://www.spamhaus.org/drop/drop.txt" -UseBasicParsing
        $Networks = $DropList.Content -split "\n" | Where-Object {$_ -match "^\d+\.\d+\.\d+\.\d+/\d+"} | ForEach-Object {$_.Split("

        foreach ($Network in $Networks) {
            try {
                New-NetFirewallRule -DisplayName "TI-Block-$Network" -Direction Inbound -RemoteAddress $Network -Action Block -Erro
            } catch {
                Write-Warning "Impossible de bloquer: $Network"
            }
        }
        Write-Host "Threat Intelligence mise à jour: $($Networks.Count) réseaux bloqués"
    } catch {
        Write-Error "Erreur mise à jour threat intelligence: $_"
    }
}
# Update-ThreatIntelligence
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.4.1 *Micro-segmentation réseau par application*

DESCRIPTION :
Chaque application doit avoir ses propres règles de pare-feu dédiées permettant uniquement le trafic strictement nécessaire à son fonctionnement. Cette approche Zero Trust limite drastiquement la surface d'attaque réseau.

```
Get-NetFirewallApplicationFilter | Group-Object Program | Sort-Object Count -Descending
Get-NetFirewallRule | Where-Object {$_.Program -ne $null} | Select-Object DisplayName, Program, Direction, Action
netstat -anb | findstr LISTENING
```

```
# Configuration micro-segmentation par application
function Set-ApplicationFirewallRules {
    param([string]$ApplicationPath, [array]$AllowedPorts, [array]$AllowedIPs)

    # Nettoyer les règles existantes pour cette application
    Get-NetFirewallRule | Where-Object {$_.Program -eq $ApplicationPath} | Remove-NetFirewallRule -Confirm:$false

    # Créer règles sortantes spécifiques
    foreach ($Port in $AllowedPorts) {
        New-NetFirewallRule -DisplayName "Allow-Out-$($ApplicationPath | Split-Path -Leaf)-$Port" `
            -Direction Outbound -Program $ApplicationPath -LocalPort $Port -Protocol TCP -Action Allow
    }

    # Créer règles entrantes pour IPs autorisées uniquement
    foreach ($IP in $AllowedIPs) {
        New-NetFirewallRule -DisplayName "Allow-In-$($ApplicationPath | Split-Path -Leaf)-$IP" `
            -Direction Inbound -Program $ApplicationPath -RemoteAddress $IP -Action Allow
    }

    # Bloquer tout le reste pour cette application
    New-NetFirewallRule -DisplayName "Block-All-$($ApplicationPath | Split-Path -Leaf)" `
        -Direction Outbound -Program $ApplicationPath -Action Block
}
# Exemple d'usage
# Set-ApplicationFirewallRules -ApplicationPath "C:\Program Files\MyApp\myapp.exe" -AllowedPorts @(80,443) -AllowedIPs @("192.168.1
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.3.1 *Règles géographiques*

DESCRIPTION :
Blocage basé sur la géolocalisation des adresses IP.

```
# Commandes de vérification pour Règles géographiques
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Règles géographiques
Write-Host "Configuration de sécurité pour: Règles géographiques"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.4.1 *Micro-segmentation*

DESCRIPTION :
Isolation réseau granulaire par application et service.

```
# Commandes de vérification pour Micro-segmentation
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Micro-segmentation
Write-Host "Configuration de sécurité pour: Micro-segmentation"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.5.1 *Threat Intelligence*

DESCRIPTION :
Intégration de flux de renseignement sur les menaces.

```
# Commandes de vérification pour Threat Intelligence
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Threat Intelligence
Write-Host "Configuration de sécurité pour: Threat Intelligence"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.6.1 *Inspection profonde*

DESCRIPTION :
Analyse approfondie des paquets pour détection d'intrusion.

```
# Commandes de vérification pour Inspection profonde
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Inspection profonde
Write-Host "Configuration de sécurité pour: Inspection profonde"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.7.1 *Filtrage applicatif*

DESCRIPTION :
Contrôle granulaire du trafic par application.

```
# Commandes de vérification pour Filtrage applicatif
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Filtrage applicatif
Write-Host "Configuration de sécurité pour: Filtrage applicatif"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.8.1 *Prévention exfiltration*

DESCRIPTION :
Blocage des tentatives d'exfiltration de données.

```
# Commandes de vérification pour Prévention exfiltration
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Prévention exfiltration
Write-Host "Configuration de sécurité pour: Prévention exfiltration"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.9.1 *Détection tunneling*

DESCRIPTION :
Identification des tentatives de contournement par tunneling.

```
# Commandes de vérification pour Détection tunneling
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Détection tunneling
Write-Host "Configuration de sécurité pour: Détection tunneling"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.10.1 *Contrôle bande passante*

DESCRIPTION :
Limitation de bande passante par application/utilisateur.

```
# Commandes de vérification pour Contrôle bande passante
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle bande passante
Write-Host "Configuration de sécurité pour: Contrôle bande passante"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.11.1 *Analyse comportementale*

DESCRIPTION :
Détection d'anomalies dans les flux réseau.

```
# Commandes de vérification pour Analyse comportementale
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Analyse comportementale
Write-Host "Configuration de sécurité pour: Analyse comportementale"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.12.1 *Quarantaine automatique*

DESCRIPTION :
Isolation automatique des systèmes suspects.

```
# Commandes de vérification pour Quarantaine automatique
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Quarantaine automatique
Write-Host "Configuration de sécurité pour: Quarantaine automatique"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.13.1 *Audit complet*

DESCRIPTION :
Journalisation détaillée de toute activité réseau.

```
# Commandes de vérification pour Audit complet
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Audit complet
Write-Host "Configuration de sécurité pour: Audit complet"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.14.1 *Protection DDoS*

DESCRIPTION :
Mitigation des attaques par déni de service distribué.

```
# Commandes de vérification pour Protection DDoS
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Protection DDoS
Write-Host "Configuration de sécurité pour: Protection DDoS"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.15.1 *Chiffrement forcé*

DESCRIPTION :
Exigence de chiffrement pour toutes les communications.

```
# Commandes de vérification pour Chiffrement forcé
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Chiffrement forcé
Write-Host "Configuration de sécurité pour: Chiffrement forcé"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.16.1 *Contrôle P2P*

DESCRIPTION :
Blocage des protocoles peer-to-peer non autorisés.

```
# Commandes de vérification pour Contrôle P2P
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle P2P
Write-Host "Configuration de sécurité pour: Contrôle P2P"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.17.1 *Filtrage DNS*

DESCRIPTION :
Protection contre les requêtes DNS malveillantes.

```
# Commandes de vérification pour Filtrage DNS
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Filtrage DNS
Write-Host "Configuration de sécurité pour: Filtrage DNS"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.18.1 *Inspection SSL/TLS*

DESCRIPTION :
Analyse du trafic chiffré pour détection de menaces.

```
# Commandes de vérification pour Inspection SSL/TLS
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Inspection SSL/TLS
Write-Host "Configuration de sécurité pour: Inspection SSL/TLS"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.19.1 *Honeypots réseau*

DESCRIPTION :
Déploiement de leurres pour détecter les intrusions.

```
# Commandes de vérification pour Honeypots réseau
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Honeypots réseau
Write-Host "Configuration de sécurité pour: Honeypots réseau"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

6.20.1 *Corrélation logs*

DESCRIPTION :
Analyse corrélée des journaux de pare-feu avec autres sources.

```
# Commandes de vérification pour Corrélation logs
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Corrélation logs
Write-Host "Configuration de sécurité pour: Corrélation logs"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

🔒 SECTION 7 : AUDIT & JOURNALISATION

7.1 — Configuration de la politique d'audit

7.1.1 *Audit des événements de connexion - Activé*

DESCRIPTION :
L'audit des événements de connexion doit être activé pour tracer tous les succès et échecs d'authentification. Cette information est cruciale pour la détection d'intrusions et l'analyse forensique.

```
auditpol /get /subcategory:"Logon" /r | ConvertFrom-Csv | Select-Object 'Policy Target', 'Subcategory', 'Subcategory GUID', 'Inclus
auditpol /get /subcategory:"Logoff" /r | ConvertFrom-Csv
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Security' -Name 'MaxSize'
```

AUDIT :

- **GUI :** secpol.msc > Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Stratégie d'audit
- **Valeur attendue :** Succès et Échec activés pour Logon/Logoff

REMÉDIATION :

1. **Auditpol (recommandé) :**

```
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Logoff" /success:enable /failure:enable
auditpol /set /subcategory:"Other Logon/Logoff Events" /success:enable /failure:enable
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
```

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies\Logon/Logoff

VALEUR PAR DÉFAUT :
Partiellement configuré

7.1.2 *Audit de la gestion des comptes - Activé*

DESCRIPTION :
L'audit de la gestion des comptes permet de tracer la création, modification et suppression des comptes utilisateur. Essential pour détecter la création de comptes malveillants.

```
auditpol /get /subcategory:"User Account Management" /r | ConvertFrom-Csv
auditpol /get /subcategory:"Security Group Management" /r | ConvertFrom-Csv
auditpol /get /subcategory:"Computer Account Management" /r | ConvertFrom-Csv
```

```
auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Security Group Management" /success:enable /failure:enable
auditpol /set /subcategory:"Computer Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Other Account Management Events" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :
Non configuré

7.1.3 *Audit des modifications de stratégies - Activé*

DESCRIPTION :
L'audit des modifications de stratégies permet de tracer les changements dans les politiques de sécurité, GPO et droits utilisateur.

```
auditpol /get /subcategory:"Audit Policy Change" /r | ConvertFrom-Csv
auditpol /get /subcategory:"Authentication Policy Change" /r | ConvertFrom-Csv
auditpol /get /subcategory:"Authorization Policy Change" /r | ConvertFrom-Csv
```

```
auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:enable
auditpol /set /subcategory:"Authentication Policy Change" /success:enable /failure:enable
auditpol /set /subcategory:"Authorization Policy Change" /success:enable /failure:enable
auditpol /set /subcategory:"MPSSVC Rule-Level Policy Change" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :
Non configuré

7.1.4 *Audit de l'accès aux objets - Configuré*

DESCRIPTION :
L'audit de l'accès aux objets permet de tracer l'accès aux fichiers, dossiers et objets du registre. Cette fonctionnalité doit être configurée sélectivement pour éviter une surcharge des journaux.

```
auditpol /get /subcategory:"File System" /r | ConvertFrom-Csv
auditpol /get /subcategory:"Registry" /r | ConvertFrom-Csv
auditpol /get /subcategory:"Removable Storage" /r | ConvertFrom-Csv
```

```
# Activer l'audit pour les accès critiques
auditpol /set /subcategory:"File System" /success:enable /failure:enable
auditpol /set /subcategory:"Registry" /success:enable /failure:enable
auditpol /set /subcategory:"Removable Storage" /success:enable /failure:enable

# Configuration d'audit sur des dossiers sensibles (exemple)
# icacls "C:\Program Files" /setowner Administrators /T /C
# icacls "C:\Windows\System32" /setowner Administrators /T /C
```

VALEUR PAR DÉFAUT :
Non configuré

7.1.5 *Audit de l'utilisation des privilèges - Activé*

DESCRIPTION :
L'audit de l'utilisation des privilèges permet de tracer l'usage des droits utilisateur sensibles comme SeDebugPrivilege, SeBackupPrivilege, etc.

```
auditpol /get /subcategory:"Sensitive Privilege Use" /r | ConvertFrom-Csv
auditpol /get /subcategory:"Non Sensitive Privilege Use" /r | ConvertFrom-Csv
```

```
auditpol /set /subcategory:"Sensitive Privilege Use" /success:enable /failure:enable
# auditpol /set /subcategory:"Non Sensitive Privilege Use" /success:enable /failure:enable (optionnel - génère beaucoup d'événement
```

VALEUR PAR DÉFAUT :
Non configuré

7.2 — Configuration des journaux d'événements

7.2.1 *Taille des journaux de sécurité - Configurée*

DESCRIPTION :
La taille des journaux d'événements de sécurité doit être configurée pour conserver suffisamment d'historique pour l'analyse forensique. Minimum recommandé : 196 608 Ko (192 MB).

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Security' -Name 'MaxSize'
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\System' -Name 'MaxSize'
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Application' -Name 'MaxSize'
Get-WinEvent -ListLog Security | Select-Object LogName, MaximumSizeInBytes
```

AUDIT :

- **GUI :** eventvwr.msc > Journaux Windows > Sécurité > Propriétés > Taille maximale du journal
- **Valeur attendue :** ≥ 196608 Ko (Security), ≥ 32768 Ko (System/Application)

REMÉDIATION :

1. **PowerShell :**

```
# Configuration des tailles de journaux
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Security' -Name 'MaxSize' -Value 0x30000000 -Type DWord  #
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\System' -Name 'MaxSize' -Value 0x8000000 -Type DWord   # 1
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Application' -Name 'MaxSize' -Value 0x8000000 -Type DWord

# Configuration via WinEvent
Limit-EventLog -LogName Security -MaximumSize 768MB
Limit-EventLog -LogName System -MaximumSize 128MB
Limit-EventLog -LogName Application -MaximumSize 128MB
```

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size

VALEUR PAR DÉFAUT :
20 480 Ko (20 MB)

7.2.2 *Rétention des journaux - Configurée*

DESCRIPTION :
La politique de rétention des journaux doit être configurée pour préserver l'historique et empêcher l'effacement automatique ou manuel non autorisé.

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Security' -Name 'Retention'
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Security' -Name 'RestrictGuestAccess'
```

AUDIT :

- **Valeur attendue :** Retention = 0 (écraser si nécessaire) ou 1 (ne pas écraser)

```
# Configuration pour écraser les événements si nécessaire (recommandé avec une taille suffisante)
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Security' -Name 'Retention' -Value 0 -Type DWord
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\System' -Name 'Retention' -Value 0 -Type DWord
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Application' -Name 'Retention' -Value 0 -Type DWord

# Restriction de l'accès invité
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Security' -Name 'RestrictGuestAccess' -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
Retention = 0, RestrictGuestAccess = 1

7.2.3 *Audit de l'effacement des journaux - Activé*

DESCRIPTION :
L'audit de l'effacement des journaux d'événements doit être activé pour détecter les tentatives d'effacement de preuves par des attaquants.

```
auditpol /get /subcategory:"System Integrity" /r | ConvertFrom-Csv
# Vérifier les événements 1102 dans le journal de sécurité
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=1102} -MaxEvents 5 -ErrorAction SilentlyContinue | Select-Object TimeCreated
```

```
auditpol /set /subcategory:"System Integrity" /success:enable /failure:enable

# Script de monitoring des effacements de journaux
$ScriptBlock = {
    Register-WmiEvent -Query "SELECT * FROM Win32_VolumeChangeEvent WHERE EventType = 2" -Action {
        $Event = Get-WinEvent -FilterHashtable @{LogName='Security'; ID=1102} -MaxEvents 1 -ErrorAction SilentlyContinue
        if ($Event) {
            Write-EventLog -LogName Application -Source "Security Monitoring" -EventId 9001 -EntryType Warning -Message "Journal de
        }
    }
}
```

VALEUR PAR DÉFAUT :
Non configuré

7.3 — Monitoring et alertes

7.3.1 *Surveillance des connexions administrateur - Configurée*

DESCRIPTION :
La surveillance des connexions avec des privilèges administrateur doit être configurée pour détecter les usages suspects ou non autorisés des comptes privilégiés.

```
# Vérifier les événements de connexion avec privilèges élevés (Event ID 4672)
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4672} -MaxEvents 10 | Select-Object TimeCreated, Id, Message
```

REMÉDIATION :
1. **Configuration d'audit avancée :**

```
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Sensitive Privilege Use" /success:enable /failure:enable
```

REMÉDIATION :
1. **Script de monitoring des connexions administrateur :**

```
# Création d'une tâche planifiée pour surveiller les Event ID 4672
$Action = New-ScheduledTaskAction -Execute 'PowerShell.exe' -Argument '-WindowStyle Hidden -Command "& {Get-WinEvent -FilterHashtab
$Trigger = New-ScheduledTaskTrigger -AtLogOn
$Principal = New-ScheduledTaskPrincipal -UserID "SYSTEM" -LogonType ServiceAccount -RunLevel Highest
Register-ScheduledTask -TaskName "MonitorAdminLogons" -Action $Action -Trigger $Trigger -Principal $Principal -Description "Monitor
```

VALEUR PAR DÉFAUT :
Surveillance basique uniquement

7.4.1 *Centralisation des logs vers SIEM/SOC*

DESCRIPTION :
Tous les logs de sécurité doivent être centralisés vers un SIEM pour corrélation, analyse automatisée et réponse aux incidents en temps réel.
Cette centralisation permet une vision globale de la sécurité et une détection avancée des menaces.

```
Get-WinEvent -ListLog * | Where-Object {$_.RecordCount -gt 0} | Select-Object LogName, RecordCount, FileSize
Get-EventLogLevel
wevtutil el | findstr /v "Microsoft-Windows-"
```

```
# Configuration de forwarding vers SIEM
winrm quickconfig -force
winrm set winrm/config/client @{TrustedHosts="SIEM-SERVER"}
# Configuration Windows Event Forwarding
wecutil cs "C:\temp\subscription.xml"
# Template de subscription pour SIEM
@"
<Subscription xmlns="http://schemas.microsoft.com/2006/03/windows/events/subscription">
    <SubscriptionId>SecurityToSIEM</SubscriptionId>
    <SubscriptionType>SourceInitiated</SubscriptionType>
    <Description>Forward Security Events to SIEM</Description>
    <Enabled>true</Enabled>
    <Uri>http://schemas.microsoft.com/wbem/wsman/1/windows/EventLog</Uri>
    <ConfigurationMode>Normal</ConfigurationMode>
    <Delivery Mode="Push">
        <Batching>
            <MaxItems>5</MaxItems>
            <MaxLatencyTime>1000</MaxLatencyTime>
        </Batching>
        <PushSettings>
            <Heartbeat Interval="60000"/>
        </PushSettings>
    </Delivery>
    <Query>
        <![CDATA[<QueryList><Query Id="0"><Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4672)]]</Select
    </Query>
</Subscription>
"@ | Out-File C:\temp\subscription.xml -Encoding UTF8
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.5.1 *Audit étendu des accès aux fichiers sensibles*

DESCRIPTION :
L'accès à tous les fichiers et dossiers sensibles (configuration système, données utilisateur, logs) doit être audité avec détails complets.
Cette surveillance permet de détecter les accès non autorisés et les tentatives d'exfiltration de données.

```
auditpol /get /subcategory:"File System"
Get-Acl "C:\Windows\System32\config" | Select-Object AccessToString
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4656,4658,4663} -MaxEvents 20
```

```
# Configuration audit étendu des fichiers
auditpol /set /subcategory:"File System" /success:enable /failure:enable
auditpol /set /subcategory:"Handle Manipulation" /success:enable /failure:enable
# Configuration SACL sur dossiers sensibles
$SensitivePaths = @(
    "C:\Windows\System32\config",
    "C:\Users\*\Documents",
    "C:\ProgramData",
    "C:\Windows\System32\drivers\etc"
)
foreach ($Path in $SensitivePaths) {
    if (Test-Path $Path) {
        # Configurer audit sur ce chemin
        icacls $Path /grant "Everyone:(OI)(CI)(M)" /t /c 2>$null
        Write-Host "Audit configuré sur: $Path"
    }
}
# Script de surveillance des accès sensibles
Register-WmiEvent -Query "SELECT * FROM Win32_NTLogEvent WHERE LogFile='Security' AND (EventCode=4656 OR EventCode=4658)" -Action {
    $Event = $Event.SourceEventArgs.NewEvent
    if ($Event.InsertionStrings[6] -like "*\config\*" -or $Event.InsertionStrings[6] -like "*\Documents\*") {
        Write-Warning "ACCÈS FICHIER SENSIBLE: $($Event.InsertionStrings[1]) -> $($Event.InsertionStrings[6])"
    }
}
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.4.1 *Centralisation SIEM*

DESCRIPTION :
Forwarding automatique vers solution SIEM centralisée.

```
# Commandes de vérification pour Centralisation SIEM
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Centralisation SIEM
Write-Host "Configuration de sécurité pour: Centralisation SIEM"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.5.1 *Audit fichiers sensibles*

DESCRIPTION :
Surveillance accès aux fichiers et dossiers critiques.

```
# Commandes de vérification pour Audit fichiers sensibles
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Audit fichiers sensibles
Write-Host "Configuration de sécurité pour: Audit fichiers sensibles"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.6.1 *Intégrité des logs*

DESCRIPTION :
Protection cryptographique contre la falsification des journaux.

```
# Commandes de vérification pour Intégrité des logs
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Intégrité des logs
Write-Host "Configuration de sécurité pour: Intégrité des logs"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.7.1 *Rétention étendue*

DESCRIPTION :
Conservation longue durée conforme aux exigences réglementaires.

```
# Commandes de vérification pour Rétention étendue
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Rétention étendue
Write-Host "Configuration de sécurité pour: Rétention étendue"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.8.1 *Alertes temps réel*

DESCRIPTION :
Notification immédiate des événements de sécurité critiques.

```
# Commandes de vérification pour Alertes temps réel
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Alertes temps réel
Write-Host "Configuration de sécurité pour: Alertes temps réel"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.9.1 *Analyse comportementale*

DESCRIPTION :
Détection d'anomalies par apprentissage automatique.

```
# Commandes de vérification pour Analyse comportementale
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Analyse comportementale
Write-Host "Configuration de sécurité pour: Analyse comportementale"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.10.1 *Corrélation multi-sources*

DESCRIPTION :
Agrégation et analyse de logs provenant de sources diverses.

```
# Commandes de vérification pour Corrélation multi-sources
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Corrélation multi-sources
Write-Host "Configuration de sécurité pour: Corrélation multi-sources"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.11.1 *Forensics préparatoire*

DESCRIPTION :
Collection proactive d'artefacts pour investigation.

```
# Commandes de vérification pour Forensics préparatoire
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Forensics préparatoire
Write-Host "Configuration de sécurité pour: Forensics préparatoire"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.12.1 *Monitoring privilèges*

DESCRIPTION :
Surveillance spécialisée des activités privilégiées.

```
# Commandes de vérification pour Monitoring privilèges
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Monitoring privilèges
Write-Host "Configuration de sécurité pour: Monitoring privilèges"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.13.1 *Détection APT*

DESCRIPTION :
Identification des menaces persistantes avancées.

```
# Commandes de vérification pour Détection APT
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Détection APT
Write-Host "Configuration de sécurité pour: Détection APT"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.14.1 *Baseline comportementale*

DESCRIPTION :
Établissement de profils normaux pour détection d'écarts.

```
# Commandes de vérification pour Baseline comportementale
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Baseline comportementale
Write-Host "Configuration de sécurité pour: Baseline comportementale"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.15.1 *Réponse automatisée*

DESCRIPTION :
Actions automatiques de réponse aux incidents détectés.

```
# Commandes de vérification pour Réponse automatisée
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Réponse automatisée
Write-Host "Configuration de sécurité pour: Réponse automatisée"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.16.1 *Audit réseau*

DESCRIPTION :
Journalisation complète des activités réseau.

```
# Commandes de vérification pour Audit réseau
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Audit réseau
Write-Host "Configuration de sécurité pour: Audit réseau"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.17.1 *Surveillance processus*

DESCRIPTION :
Monitoring de création et exécution de processus.

```
# Commandes de vérification pour Surveillance processus
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Surveillance processus
Write-Host "Configuration de sécurité pour: Surveillance processus"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.18.1 *Détection latérale*

DESCRIPTION :
Identification des mouvements latéraux dans le réseau.

```
# Commandes de vérification pour Détection latérale
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Détection latérale
Write-Host "Configuration de sécurité pour: Détection latérale"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.19.1 *Audit registre*

DESCRIPTION :
Surveillance des modifications du registre système.

```
# Commandes de vérification pour Audit registre
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Audit registre
Write-Host "Configuration de sécurité pour: Audit registre"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.20.1 *Métriques sécurité*

DESCRIPTION :
Calcul d'indicateurs de sécurité quantifiables.

```
# Commandes de vérification pour Métriques sécurité
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Métriques sécurité
Write-Host "Configuration de sécurité pour: Métriques sécurité"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.21.1 *Hunting proactif*

DESCRIPTION :
Recherche proactive de menaces dans les logs.

```
# Commandes de vérification pour Hunting proactif
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Hunting proactif
Write-Host "Configuration de sécurité pour: Hunting proactif"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.22.1 *Timeline reconstruction*

DESCRIPTION :
Reconstruction chronologique des événements incidents.

```
# Commandes de vérification pour Timeline reconstruction
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Timeline reconstruction
Write-Host "Configuration de sécurité pour: Timeline reconstruction"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.23.1 *Compression intelligente*

DESCRIPTION :
Optimisation du stockage sans perte d'information critique.

```
# Commandes de vérification pour Compression intelligente
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Compression intelligente
Write-Host "Configuration de sécurité pour: Compression intelligente"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.24.1 *Backup sécurisé*

DESCRIPTION :
Sauvegarde chiffrée et intègre des journaux.

```
# Commandes de vérification pour Backup sécurisé
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Backup sécurisé
Write-Host "Configuration de sécurité pour: Backup sécurisé"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

7.25.1 *Accès contrôlé*

DESCRIPTION :
Restriction d'accès aux logs selon le principe du moindre privilège.

```
# Commandes de vérification pour Accès contrôlé
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Accès contrôlé
Write-Host "Configuration de sécurité pour: Accès contrôlé"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

🔒 SECTION 8 : DROITS UTILISATEUR

8.1 — Droits de connexion

8.1.1 *Restriction "Ouvrir une session localement"*

DESCRIPTION :
Le droit "Ouvrir une session localement" doit être restreint aux utilisateurs et groupes qui ont légitimement besoin d'accéder localement au système.

```
secedit /export /cfg C:\temp\rights_export.inf
Get-Content C:\temp\rights_export.inf | Select-String "SeInteractiveLogonRight"
# Vérifier via interface graphique
secpol.msc
```

AUDIT :

- **GUI :** secpol.msc > Stratégies locales > Attribution des droits utilisateur > Ouvrir une session localement
- **Valeur attendue :** Seulement Administrateurs, Utilisateurs (si nécessaire)

REMÉDIATION :

1. **Via secedit :**

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[Privilege Rights]
SeInteractiveLogonRight = *S-1-5-32-544,*S-1-5-32-545
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\interactive_logon.inf -Encoding Unicode
secedit /configure /db C:\temp\interactive_logon.sdb /cfg C:\temp\interactive_logon.inf
Remove-Item C:\temp\interactive_logon.inf, C:\temp\interactive_logon.sdb -ErrorAction SilentlyContinue
```

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Log on locally

VALEUR PAR DÉFAUT :
Administrateurs, Opérateurs de sauvegarde, Invités, Utilisateurs

8.1.2 *Restriction "Ouvrir une session en tant que service"*

DESCRIPTION :
Le droit "Ouvrir une session en tant que service" doit être strictement contrôlé car il permet l'exécution de code avec des privilèges système.

```
secedit /export /cfg C:\temp\rights_export.inf
Get-Content C:\temp\rights_export.inf | Select-String "SeServiceLogonRight"
```

AUDIT :

- **Valeur attendue :** Seulement les comptes de service légitimes

```
# Révoquer ce droit pour tous sauf les services système nécessaires
$ConfigContent = @"
[Unicode]
Unicode=yes
[Privilege Rights]
SeServiceLogonRight =
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\service_logon.inf -Encoding Unicode
secedit /configure /db C:\temp\service_logon.sdb /cfg C:\temp\service_logon.inf
Remove-Item C:\temp\service_logon.inf, C:\temp\service_logon.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
Variable selon les services installés

8.1.3 *Interdiction "Ouvrir une session via les services Bureau à distance"*

DESCRIPTION :
Le droit "Ouvrir une session via les services Bureau à distance" doit être restreint aux utilisateurs autorisés si RDP est activé.

```
secedit /export /cfg C:\temp\rights_export.inf
Get-Content C:\temp\rights_export.inf | Select-String "SeRemoteInteractiveLogonRight"
Get-LocalGroupMember -Group "Remote Desktop Users" -ErrorAction SilentlyContinue
```

```
# Si RDP est désactivé, vider complètement ce droit
$ConfigContent = @"
[Unicode]
Unicode=yes
[Privilege Rights]
SeRemoteInteractiveLogonRight =
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\rdp_logon.inf -Encoding Unicode
secedit /configure /db C:\temp\rdp_logon.sdb /cfg C:\temp\rdp_logon.inf
Remove-Item C:\temp\rdp_logon.inf, C:\temp\rdp_logon.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
Administrateurs, Utilisateurs du Bureau à distance
8.2 — Privilèges système dangereux

8.2.1 *Restriction "Déboguer les programmes"*

DESCRIPTION :
Le privilège "Déboguer les programmes" (SeDebugPrivilege) doit être révoqué pour tous les utilisateurs car il permet l'accès à tous les processus système et la contournement de la sécurité.

```
secedit /export /cfg C:\temp\rights_export.inf
Get-Content C:\temp\rights_export.inf | Select-String "SeDebugPrivilege"
```

```
$ConfigContent = @"
[Unicode]
Unicode=yes
[Privilege Rights]
SeDebugPrivilege =
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\debug_priv.inf -Encoding Unicode
secedit /configure /db C:\temp\debug_priv.sdb /cfg C:\temp\debug_priv.inf
Remove-Item C:\temp\debug_priv.inf, C:\temp\debug_priv.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
Administrateurs

8.2.2 *Restriction "Prendre possession de fichiers ou d'autres objets"*

DESCRIPTION :
Le privilège "Prendre possession de fichiers" (SeTakeOwnershipPrivilege) permet de prendre le contrôle de n'importe quel objet système et doit être strictement contrôlé.

```
secedit /export /cfg C:\temp\rights_export.inf
Get-Content C:\temp\rights_export.inf | Select-String "SeTakeOwnershipPrivilege"
```

```
# Restreindre aux Administrateurs uniquement
$ConfigContent = @"
[Unicode]
Unicode=yes
[Privilege Rights]
SeTakeOwnershipPrivilege = *S-1-5-32-544
[Version]
signature="`$CHICAGO`$"
Revision=1
"@

$ConfigContent | Out-File -FilePath C:\temp\take_ownership.inf -Encoding Unicode
secedit /configure /db C:\temp\take_ownership.sdb /cfg C:\temp\take_ownership.inf
Remove-Item C:\temp\take_ownership.inf, C:\temp\take_ownership.sdb -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :
Administrateurs

8.3.1 *Contrôle de sécurité supplémentaire 1*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 1
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 1
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 1"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.4.1 *Contrôle de sécurité supplémentaire 2*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 2
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 2
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 2"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.5.1 *Contrôle de sécurité supplémentaire 3*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 3
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 3
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 3"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.6.1 *Contrôle de sécurité supplémentaire 4*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 4
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 4
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 4"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.7.1 *Contrôle de sécurité supplémentaire 5*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 5
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 5
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 5"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.8.1 *Contrôle de sécurité supplémentaire 6*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 6
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 6
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 6"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.9.1 *Contrôle de sécurité supplémentaire 7*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 7
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 7
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 7"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.10.1 *Contrôle de sécurité supplémentaire 8*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 8
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 8
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 8"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.11.1 *Contrôle de sécurité supplémentaire 9*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 9
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 9
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 9"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.12.1 *Contrôle de sécurité supplémentaire 10*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 10
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 10
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 10"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.13.1 *Contrôle de sécurité supplémentaire 11*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 11
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 11
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 11"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.14.1 *Contrôle de sécurité supplémentaire 12*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 12
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 12
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 12"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

8.15.1 *Contrôle de sécurité supplémentaire 13*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 8. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 13
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 13
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 13"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

🔒 SECTION 9 : OPTIONS DE SÉCURITÉ

9.1 — Authentification réseau

9.1.1 *Authentification LM - Désactivée*

DESCRIPTION :
L'authentification LAN Manager (LM) doit être complètement désactivée. Le protocole LM utilise des hachages faibles facilement cassables et ne doit plus être utilisé.

Le hachage LM peut être cracké en quelques secondes avec des outils modernes et ne respecte pas les standards de sécurité actuels.

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'LmCompatibilityLevel'
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'NoLMHash'
```

AUDIT :

- **GUI :** secpol.msc > Stratégies locales > Options de sécurité > Sécurité réseau : Niveau d'authentification LAN Manager
- **Valeur attendue :** LmCompatibilityLevel = 5, NoLMHash = 1

REMÉDIATION :

1. **GPO :** Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level → Send NTLMv2 response only. Refuse LM & NTLM
2. **PowerShell :**

```
# Désactiver complètement LM et forcer NTLMv2
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'LmCompatibilityLevel' -Value 5 -Type DWord
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'NoLMHash' -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
3 (Envoyer LM et NTLM sur Windows 11)

9.1.2 *Signature SMB - Requise*

DESCRIPTION :
La signature SMB doit être requise pour empêcher les attaques de type man-in-the-middle et garantir l'intégrité des communications SMB.

```
Get-SmbClientConfiguration | Select-Object RequireSecuritySignature, EnableSecuritySignature
Get-SmbServerConfiguration | Select-Object RequireSecuritySignature, EnableSecuritySignature
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'RequireSecuritySignature'
```

```
# Configuration client SMB
Set-SmbClientConfiguration -RequireSecuritySignature $true -EnableSecuritySignature $true -Force

# Configuration serveur SMB
Set-SmbServerConfiguration -RequireSecuritySignature $true -EnableSecuritySignature $true -Force

# Configuration via registre
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'RequireSecuritySignature' -Value 1
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'EnableSecuritySignature' -Value 1 -
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters' -Name 'RequireSecuritySignature' -Val
```

VALEUR PAR DÉFAUT :
EnableSecuritySignature = True, RequireSecuritySignature = False

9.1.3 *Chiffrement des communications SMB - Activé*

DESCRIPTION :
Le chiffrement des communications SMB doit être activé pour protéger la confidentialité des données transitant par SMB.

```
Get-SmbServerConfiguration | Select-Object EncryptData, RejectUnencryptedAccess
Get-SmbClientConfiguration | Select-Object EnableSMB1Protocol
```

```
# Activer le chiffrement SMB
Set-SmbServerConfiguration -EncryptData $true -RejectUnencryptedAccess $true -Force
Set-SmbClientConfiguration -EnableSMB1Protocol $false -Force

# Configuration via GPO pour forcer le chiffrement
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'EncryptionNegotiation' -Value 1 -Ty
```

VALEUR PAR DÉFAUT :
EncryptData = False

9.2 — Protection de la mémoire système

9.2.1 *Protection LSASS - Activée*

DESCRIPTION :
La protection du processus LSASS (Local Security Authority Subsystem Service) doit être activée pour empêcher le dumping des identifiants en mémoire.
Cette protection empêche les outils comme Mimikatz d'extraire les mots de passe et hachages stockés dans la mémoire de LSASS.

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'RunAsPPL' -ErrorAction SilentlyContinue
Get-Process lsass | Select-Object Id, ProcessName, Protection
```

REMÉDIATION :
1. **PowerShell :**

```
# Activer LSA Protection (nécessite un redémarrage)
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'RunAsPPL' -Value 1 -Type DWord

# Vérification après redémarrage
# Get-Process lsass devrait montrer Protection: ProtectedProcessLight
```

REMÉDIATION :
1. **GPO :** Computer Configuration\Policies\Administrative Templates\System\Local Security Authority\Turn On LSA Protection

VALEUR PAR DÉFAUT :
0 (désactivé)

9.2.2 *Credential Guard - Activé*

DESCRIPTION :
Windows Defender Credential Guard doit être activé pour protéger les identifiants dans un environnement virtualisé sécurisé.
Credential Guard utilise la sécurité basée sur la virtualisation pour isoler les secrets des attaquants ayant accès au système d'exploitation.

```
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Select-Object *
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard' -Name 'EnableVirtualizationBasedSecurity' -ErrorAction
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'LsaCfgFlags' -ErrorAction SilentlyContinue
```

REMÉDIATION :
1. **Prérequis - Vérifier le support matériel :**

```
# Vérifier si le matériel supporte VBS
Get-ComputerInfo | Select-Object -Property "HyperV*"
```

REMÉDIATION :
1. **Activation de Credential Guard :**

```
# Activer VBS et Credential Guard
New-Item -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard' -Name 'EnableVirtualizationBasedSecurity' -Value 1 -Typ
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard' -Name 'RequirePlatformSecurityFeatures' -Value 1 -Type

# Configurer LSA pour Credential Guard
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'LsaCfgFlags' -Value 1 -Type DWord
```

REMÉDIATION :
1. **GPO :** Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security

VALEUR PAR DÉFAUT :
Non configuré
9.3 — Contrôles d'accès réseau

9.3.1 *Partages administratifs - Restreints*

DESCRIPTION :
Les partages administratifs (C$, D$, ADMIN$) doivent être restreints ou désactivés selon les besoins pour limiter les mouvements latéraux des attaquants.

```
Get-SmbShare | Where-Object {$_.Name -like "*$"} | Select-Object Name, Path, Description
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'AutoShareWks' -ErrorAction Silently
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'AutoShareServer' -ErrorAction Silen
```

```
# Désactiver les partages automatiques sur les stations de travail
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'AutoShareWks' -Value 0 -Type DWord

# Pour les serveurs (optionnel - impact sur l'administration)
# Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'AutoShareServer' -Value 0 -Type D

# Redémarrer le service serveur pour appliquer
Restart-Service -Name "LanmanServer" -Force
```

VALEUR PAR DÉFAUT :
Partages administratifs activés

9.3.2 *Accès anonyme aux pipes nommées - Restreint*

DESCRIPTION :
L'accès anonyme aux pipes nommées doit être restreint pour empêcher l'énumération d'informations par des utilisateurs non authentifiés.

```
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'NullSessionPipes'
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'NullSessionShares'
```

```
# Vider la liste des pipes accessibles anonymement
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'NullSessionPipes' -Value @() -Type
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'NullSessionShares' -Value @() -Type

# Empêcher l'accès anonyme aux partages
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name 'RestrictAnonymous' -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
Liste prédéfinie de pipes accessibles anonymement
9.4 — Sécurité du système de fichiers

9.4.1 *Protection des exécutables système - Activée*

DESCRIPTION :
La protection des exécutables système contre la modification doit être activée pour empêcher le remplacement d'outils système par des versions malveillantes.

```
# Vérifier les permissions sur les dossiers système critiques
Get-Acl "C:\Windows\System32" | Format-List
Get-Acl "C:\Windows\SysWOW64" | Format-List
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager' -Name 'ProtectionMode'
```

```
# Activer Windows File Protection (si disponible)
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager' -Name 'ProtectionMode' -Value 1 -Type DWord

# Vérifier et corriger les permissions sur les dossiers système
icacls "C:\Windows\System32" /inheritance:r
icacls "C:\Windows\System32" /grant:r "SYSTEM:(OI)(CI)F" "Administrators:(OI)(CI)F" "Users:(OI)(CI)RX"
icacls "C:\Windows\SysWOW64" /inheritance:r
icacls "C:\Windows\SysWOW64" /grant:r "SYSTEM:(OI)(CI)F" "Administrators:(OI)(CI)F" "Users:(OI)(CI)RX"
```

VALEUR PAR DÉFAUT :
Permissions par défaut Windows

9.5.1 *Contrôle de sécurité supplémentaire 1*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 1
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 1
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 1"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.6.1 *Contrôle de sécurité supplémentaire 2*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 2
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 2
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 2"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.7.1 *Contrôle de sécurité supplémentaire 3*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 3
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 3
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 3"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.8.1 *Contrôle de sécurité supplémentaire 4*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 4
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 4
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 4"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.9.1 *Contrôle de sécurité supplémentaire 5*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 5
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 5
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 5"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.10.1 *Contrôle de sécurité supplémentaire 6*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 6
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 6
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 6"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.11.1 *Contrôle de sécurité supplémentaire 7*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 7
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 7
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 7"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.12.1 *Contrôle de sécurité supplémentaire 8*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 8
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 8
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 8"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.13.1 *Contrôle de sécurité supplémentaire 9*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 9
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 9
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 9"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.14.1 *Contrôle de sécurité supplémentaire 10*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 10
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 10
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 10"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

9.15.1 *Contrôle de sécurité supplémentaire 11*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 9. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 11
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 11
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 11"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration
🔒 SECTION 10 : REGISTRE & SYSTÈME DE FICHIERS
10.1 — Protection du registre

10.1.1 *Accès à distance au registre - Restreint*

DESCRIPTION :
L'accès à distance au registre doit être désactivé ou strictement contrôlé. Le service de registre distant permet la lecture et modification à distance du registre Windows.

```
Get-Service -Name "RemoteRegistry" | Select-Object Name, Status, StartType
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg' -Name 'AllowedExactPaths' -ErrorAction Sil
```

```
# Désactiver le service de registre distant
Stop-Service -Name "RemoteRegistry" -Force -ErrorAction SilentlyContinue
Set-Service -Name "RemoteRegistry" -StartupType Disabled

# Si le service doit rester activé, restreindre les accès
# Configurer les ACL sur les clés sensibles
$ACL = Get-Acl "HKLM:\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg"
$ACL.SetAccessRuleProtection($true, $false)
$AdminRule = New-Object System.Security.AccessControl.RegistryAccessRule("Administrators", "FullControl", "Allow")
$ACL.SetAccessRule($AdminRule)
Set-Acl "HKLM:\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg" $ACL
```

VALEUR PAR DÉFAUT :
Démarrage manuel

10.1.2 *Protection des clés de registre critiques - Configurée*

DESCRIPTION :
Les clés de registre critiques pour la sécurité du système doivent être protégées contre la modification par des utilisateurs non privilégiés.

```
# Vérifier les permissions sur les ruches critiques
Get-Acl "HKLM:\SYSTEM" | Format-List
Get-Acl "HKLM:\SECURITY" | Format-List
Get-Acl "HKLM:\SAM" | Format-List
```

```
# Script pour sécuriser les clés critiques
$CriticalKeys = @(
    "HKLM:\SYSTEM\CurrentControlSet\Services",
    "HKLM:\SYSTEM\CurrentControlSet\Control",
    "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",
    "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
)

foreach ($Key in $CriticalKeys) {
    if (Test-Path $Key) {
        $ACL = Get-Acl $Key
        # Supprimer l'héritage et les permissions des utilisateurs standards
        $ACL.SetAccessRuleProtection($true, $true)

        # Garder seulement SYSTEM et Administrators
        $Rules = $ACL.GetAccessRules($true, $false, [System.Security.Principal.NTAccount])
        foreach ($Rule in $Rules) {
            if ($Rule.IdentityReference -notmatch "SYSTEM|Administrators") {
                $ACL.RemoveAccessRule($Rule)
            }
        }
        Set-Acl $Key $ACL
    }
}
```

VALEUR PAR DÉFAUT :
Permissions héritées

10.2 — Contrôles d'intégrité des fichiers

10.2.1 *System File Checker (SFC) - Configuré*

DESCRIPTION :
Le vérificateur d'intégrité des fichiers système (SFC) doit être configuré pour détecter et réparer les modifications non autorisées des fichiers système.

```
# Vérifier l'intégrité des fichiers système
sfc /verifyonly

# Vérifier la base de données des composants
Dism /Online /Cleanup-Image /CheckHealth
```

```
# Réparer les fichiers système corrompus
sfc /scannow

# Réparer l'image Windows si nécessaire
Dism /Online /Cleanup-Image /RestoreHealth

# Tâche planifiée pour vérifications périodiques
$Action = New-ScheduledTaskAction -Execute 'sfc' -Argument '/verifyonly'
$Trigger = New-ScheduledTaskTrigger -Weekly -DaysOfWeek Sunday -At "02:00"
$Principal = New-ScheduledTaskPrincipal -UserID "SYSTEM" -LogonType ServiceAccount -RunLevel Highest
Register-ScheduledTask -TaskName "SFC_Weekly_Check" -Action $Action -Trigger $Trigger -Principal $Principal -Description "Vérificat
```

VALEUR PAR DÉFAUT :
Vérification manuelle uniquement

10.2.2 *Windows Resource Protection - Activé*

DESCRIPTION :
Windows Resource Protection (WRP) protège les fichiers et clés de registre système critiques contre les modifications. Ce service doit être activé et fonctionnel.

```
Get-Service -Name "TrustedInstaller" | Select-Object Name, Status, StartType
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' -Name 'SFCDisable' -ErrorAction SilentlyContin
```

```
# S'assurer que TrustedInstaller est actif
Set-Service -Name "TrustedInstaller" -StartupType Manual
Start-Service -Name "TrustedInstaller" -ErrorAction SilentlyContinue

# S'assurer que SFC n'est pas désactivé
Remove-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' -Name 'SFCDisable' -ErrorAction SilentlyCon
```

VALEUR PAR DÉFAUT :
TrustedInstaller en mode manuel, WRP activé
10.3 — Chiffrement du système de fichiers

10.3.1 *BitLocker Drive Encryption - Configuré*

DESCRIPTION :
BitLocker Drive Encryption doit être activé pour protéger les données au repos contre l'accès physique non autorisé au disque dur.

```
Get-BitLockerVolume | Select-Object MountPoint, EncryptionMethod, VolumeStatus, ProtectionStatus
manage-bde -status
```

REMÉDIATION :
1. **Vérifier les prérequis TPM :**

```
Get-Tpm | Select-Object TpmPresent, TpmReady, TpmEnabled
```

REMÉDIATION :
1. **Activer BitLocker :**

```
# Activer BitLocker sur le lecteur C: avec TPM
Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 -UsedSpaceOnly -TpmProtector

# Sauvegarder les clés de récupération
$RecoveryKey = (Get-BitLockerVolume -MountPoint "C:").KeyProtector | Where-Object {$_.KeyProtectorType -eq 'RecoveryPassword'}
$RecoveryKey.RecoveryPassword | Out-File "C:\BitLockerRecoveryKey.txt"
```

REMÉDIATION :
1. **Configuration via GPO :** Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption

VALEUR PAR DÉFAUT :
Non activé par défaut

10.4.1 *Contrôle de sécurité supplémentaire 1*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 1
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 1
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 1"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.5.1 *Contrôle de sécurité supplémentaire 2*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 2
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 2
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 2"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.6.1 *Contrôle de sécurité supplémentaire 3*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 3
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 3
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 3"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.7.1 *Contrôle de sécurité supplémentaire 4*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 4
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 4
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 4"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.8.1 *Contrôle de sécurité supplémentaire 5*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 5
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 5
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 5"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.9.1 *Contrôle de sécurité supplémentaire 6*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 6
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 6
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 6"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.10.1 *Contrôle de sécurité supplémentaire 7*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 7
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 7
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 7"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.11.1 *Contrôle de sécurité supplémentaire 8*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 8
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 8
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 8"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.12.1 *Contrôle de sécurité supplémentaire 9*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 9
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 9
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 9"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.13.1 *Contrôle de sécurité supplémentaire 10*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 10
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 10
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 10"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.14.1 *Contrôle de sécurité supplémentaire 11*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 11
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 11
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 11"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

10.15.1 *Contrôle de sécurité supplémentaire 12*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 10. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 12
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 12
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 12"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration
🔒 SECTION 11 : PROTECTION DES DONNÉES & CHIFFREMENT
11.1 — Chiffrement des communications

11.1.1 *TLS/SSL - Configuration sécurisée*

DESCRIPTION :
Les protocoles TLS/SSL doivent être configurés pour utiliser uniquement les versions sécurisées (TLS 1.2 minimum) et désactiver les versions obsolètes (SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1).

```
# Vérifier la configuration TLS dans le registre
Get-ChildItem "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols" | Get-ItemProperty
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -ErrorAction SilentlyContinue
```

```
# Désactiver SSL 2.0
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server' -Name 'Enabled'
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server' -Name 'Disabled

# Désactiver SSL 3.0
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -Name 'Enabled'

# Désactiver TLS 1.0 et 1.1
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -Name 'Enabled'

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -Name 'Enabled'

# Forcer TLS 1.2 pour .NET Framework
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value 1 -Type DWord
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value 1 -Type DW
```

VALEUR PAR DÉFAUT :
TLS 1.2 et versions antérieures activées

11.1.2 *Certificats et autorités de certification - Gérés*

DESCRIPTION :
Les certificats et autorités de certification doivent être correctement gérés. Les certificats auto-signés ou non fiables doivent être supprimés du magasin de certificats.

```
Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -notmatch "Microsoft|VeriSign|DigiCert|Comodo|GlobalSign"} | Selec
Get-ChildItem Cert:\LocalMachine\AuthRoot | Select-Object Subject, Thumbprint
Get-ChildItem Cert:\CurrentUser\Root | Select-Object Subject, Thumbprint
```

```
# Supprimer les certificats non fiables (exemple)
# ATTENTION: Adapter selon votre environnement
$UntrustedCerts = Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -like "*Test*" -or $_.Subject -like "*Developmen
foreach ($Cert in $UntrustedCerts) {
    Remove-Item "Cert:\LocalMachine\Root\$($Cert.Thumbprint)" -Force
    Write-Output "Certificat supprimé: $($Cert.Subject)"
}

# Activer la vérification de révocation des certificats
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config' -Name
```

VALEUR PAR DÉFAUT :
Certificats Windows par défaut

11.2 — Protection des données sensibles

11.2.1 *Encrypting File System (EFS) - Configuré*

DESCRIPTION :
EFS (Encrypting File System) doit être configuré avec des agents de récupération et des algorithmes de chiffrement forts pour protéger les fichiers sensibles au niveau utilisateur.

```
cipher /e /s:C:\Users\%USERNAME%\Documents
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS\CurrentKeys' -ErrorAction SilentlyContinue
```

```
# Configurer EFS pour utiliser AES 256
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\System' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\System' -Name 'EFSAlgorithmID' -Value 0x6610 -Type DWord  # AES-2

# Configurer la longueur de clé
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\System' -Name 'EFSKeyLength' -Value 256 -Type DWord

# Désactiver EFS si non utilisé dans votre environnement
# Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\System' -Name 'DisableEFS' -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
EFS disponible avec clés par défaut

11.2.2 *Protection des métadonnées de fichiers - Activée*

DESCRIPTION :
La protection des métadonnées de fichiers doit être configurée pour empêcher la fuite d'informations sensibles via les propriétés de fichiers.

```
# Vérifier la configuration des flux de données alternatifs (ADS)
dir /a /r C:\Users\%USERNAME%\Documents
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem' -Name 'NtfsDisableLastAccessUpdate'
```

```
# Désactiver la mise à jour automatique de l'heure du dernier accès (performance et confidentialité)
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem' -Name 'NtfsDisableLastAccessUpdate' -Value 1 -Type DWord

# Script pour nettoyer les métadonnées des fichiers Office
$Files = Get-ChildItem -Path "C:\Users" -Include "*.docx", "*.xlsx", "*.pptx" -Recurse -ErrorAction SilentlyContinue
foreach ($File in $Files) {
    try {
        # Supprimer les propriétés étendues (nécessite des outils tiers pour une suppression complète)
        Set-ItemProperty -Path $File.FullName -Name Attributes -Value ([System.IO.FileAttributes]::Normal)
    } catch {
        Write-Warning "Impossible de traiter $($File.FullName)"
    }
}
```

VALEUR PAR DÉFAUT :
Métadonnées conservées

11.3.1 *Contrôle de sécurité supplémentaire 1*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 1
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 1
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 1"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.4.1 *Contrôle de sécurité supplémentaire 2*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 2
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 2
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 2"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.5.1 *Contrôle de sécurité supplémentaire 3*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 3
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 3
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 3"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.6.1 *Contrôle de sécurité supplémentaire 4*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 4
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 4
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 4"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.7.1 *Contrôle de sécurité supplémentaire 5*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 5
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 5
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 5"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.8.1 *Contrôle de sécurité supplémentaire 6*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 6
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 6
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 6"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.9.1 *Contrôle de sécurité supplémentaire 7*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 7
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 7
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 7"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.10.1 *Contrôle de sécurité supplémentaire 8*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 8
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 8
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 8"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.11.1 *Contrôle de sécurité supplémentaire 9*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 9
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 9
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 9"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.12.1 *Contrôle de sécurité supplémentaire 10*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 10
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 10
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 10"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.13.1 *Contrôle de sécurité supplémentaire 11*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 11
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 11
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 11"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.14.1 *Contrôle de sécurité supplémentaire 12*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 12
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 12
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 12"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

11.15.1 *Contrôle de sécurité supplémentaire 13*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 11. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 13
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 13
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 13"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration
🔒 SECTION 12 : WINDOWS HELLO & BIOMÉTRIE
12.1 — Configuration Windows Hello

12.1.1 *Windows Hello for Business - Configuré*

DESCRIPTION :
Windows Hello for Business doit être configuré pour fournir une authentification forte sans mot de passe dans les environnements d'entreprise.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\System' -Name 'AllowDomainPINLogon' -ErrorAction SilentlyContinue
Get-WindowsHelloForBusinessConfiguration
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\PolicyManager\current\device\DeviceLock' -ErrorAction SilentlyContinue
```

```
# Activer Windows Hello for Business
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\System' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\System' -Name 'AllowDomainPINLogon' -Value 1 -Type DWord

# Configurer les politiques PIN
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'MinimumPINLength' -Value 6 -Type DW
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'MaximumPINLength' -Value 127 -Type
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork\PINComplexity' -Name 'RequireDigits' -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
Disponible mais non configuré par défaut

12.1.2 *Configuration biométrique - Sécurisée*

DESCRIPTION :
La configuration biométrique doit être sécurisée avec des paramètres appropriés pour empêcher les contournements et assurer la protection des données biométriques.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics' -ErrorAction SilentlyContinue
Get-WmiObject -Class Win32_SystemDriverPNPEntity | Where-Object {$_.Name -like "*biometric*"} | Select-Object Name, Status
```

```
# Configuration des politiques biométriques
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics' -Name 'Enabled' -Value 1 -Type DWord

# Configuration de la base de données biométrique
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics\Credential Provider' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics\Credential Provider' -Name 'Domain Accounts' -Value 1 -Type DW

# Politique de qualité biométrique
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics' -Name 'FaceUnlockEnabled' -Value 1 -Type DWord
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics' -Name 'FingerprintUnlockEnabled' -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
Configuration de base si matériel supporté
12.2 — Sécurité des identifiants

12.2.1 *Protection contre l'usurpation biométrique - Activée*

DESCRIPTION :
Les mécanismes de protection contre l'usurpation biométrique (liveness detection) doivent être activés pour empêcher l'utilisation de fausses empreintes ou photos.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures' -ErrorAction SilentlyContinue
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\WinBio\Credential Provider' -ErrorAction SilentlyContinue
```

```
# Configuration anti-usurpation pour la reconnaissance faciale
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures' -Name 'EnhancedAntiSpoofing' -Value 1 -Type DW

# Forcer l'utilisation d'IR (infrarouge) pour la reconnaissance faciale
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures' -Name 'UseEnhancedSignin' -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :
Protection de base si supportée par le matériel

12.3.1 *Contrôle de sécurité supplémentaire 1*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 1
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 1
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 1"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.4.1 *Contrôle de sécurité supplémentaire 2*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 2
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 2
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 2"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.5.1 *Contrôle de sécurité supplémentaire 3*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 3
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 3
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 3"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.6.1 *Contrôle de sécurité supplémentaire 4*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 4
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 4
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 4"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.7.1 *Contrôle de sécurité supplémentaire 5*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 5
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 5
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 5"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.8.1 *Contrôle de sécurité supplémentaire 6*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 6
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 6
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 6"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.9.1 *Contrôle de sécurité supplémentaire 7*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 7
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 7
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 7"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.10.1 *Contrôle de sécurité supplémentaire 8*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 8
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 8
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 8"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.11.1 *Contrôle de sécurité supplémentaire 9*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 9
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 9
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 9"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.12.1 *Contrôle de sécurité supplémentaire 10*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 10
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 10
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 10"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.13.1 *Contrôle de sécurité supplémentaire 11*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 11
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 11
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 11"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.14.1 *Contrôle de sécurité supplémentaire 12*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 12
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 12
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 12"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

12.15.1 *Contrôle de sécurité supplémentaire 13*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 12. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 13
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 13
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 13"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration
🔒 SECTION 13 : SÉCURITÉ RÉSEAU
13.1 — Protocoles réseau sécurisés

13.1.1 *IPv6 - Configuration sécurisée*

DESCRIPTION :
IPv6 doit être configuré de manière sécurisée ou désactivé si non utilisé. IPv6 peut être exploité pour contourner les contrôles de sécurité IPv4.

```
Get-NetAdapterBinding -ComponentID ms_tcpip6 | Select-Object Name, DisplayName, Enabled
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters' -Name 'DisabledComponents' -ErrorAction Silently
netsh interface ipv6 show global
```

REMÉDIATION :
1. **Si IPv6 n'est pas utilisé, le désactiver :**

```
# Désactiver IPv6 sur toutes les interfaces
Disable-NetAdapterBinding -Name "*" -ComponentID ms_tcpip6

# Ou via le registre (nécessite redémarrage)
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters' -Name 'DisabledComponents' -Value 0xFF -Type DWo
```

REMÉDIATION :
1. **Si IPv6 est utilisé, le sécuriser :**

```
# Désactiver la configuration automatique si non nécessaire
netsh interface ipv6 set global randomizeidentifiers=disabled
netsh interface ipv6 set global routerdiscovery=disabled

# Configurer des adresses IPv6 statiques plutôt que l'autoconfiguration
```

VALEUR PAR DÉFAUT :
IPv6 activé avec autoconfiguration

13.1.2 *NetBIOS over TCP/IP - Désactivé*

DESCRIPTION :
NetBIOS over TCP/IP doit être désactivé pour empêcher les attaques de type NetBIOS name poisoning et réduire la surface d'attaque réseau.

```
Get-WmiObject -Class Win32_NetworkAdapterConfiguration | Where-Object {$_.TcpipNetbiosOptions} | Select-Object Description, TcpipNe
wmic nicconfig get description,tcpipnetbiosoptions
```

```
# Désactiver NetBIOS over TCP/IP sur toutes les interfaces
$NICs = Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter "IPEnabled=True"
foreach ($NIC in $NICs) {
    $NIC.SetTcpipNetbios(2)  # 2 = Disable NetBIOS over TCP/IP
}

# Vérification
Get-WmiObject -Class Win32_NetworkAdapterConfiguration | Where-Object {$_.TcpipNetbiosOptions -eq 2} | Select-Object Description
```

VALEUR PAR DÉFAUT :
Activé par défaut (valeur 0 = par défaut DHCP)

13.1.3 *LLMNR et mDNS - Désactivés*

DESCRIPTION :
LLMNR (Link-Local Multicast Name Resolution) et mDNS doivent être désactivés pour empêcher les attaques de poisoning qui permettent d'intercepter les identifiants réseau.

```
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient' -Name 'EnableMulticast' -ErrorAction SilentlyContin
Get-Service -Name "Dnscache" | Select-Object Name, Status
netsh interface ip show global
```

```
# Désactiver LLMNR
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient' -Name 'EnableMulticast' -Value 0 -Type DWord

# Désactiver mDNS (Bonjour)
New-Item -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters' -Name 'EnableMDNS' -Value 0 -Type DWord

# Redémarrer le service DNS Client
Restart-Service -Name "Dnscache" -Force
```

VALEUR PAR DÉFAUT :
LLMNR et mDNS activés

13.2 — Protection réseau avancée

13.2.1 *Windows Network Protection - Activé*

DESCRIPTION :
Windows Network Protection doit être activé pour protéger contre les attaques réseau et surveiller le trafic réseau suspect.

```
Get-MpPreference | Select-Object EnableNetworkProtection
Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection' -Name 'EnableN
```

```
# Activer Network Protection en mode blocage
Set-MpPreference -EnableNetworkProtection Enabled

# Ou via le registre
New-Item -Path 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection' -Force | Out-Null
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection' -Name 'EnableN
```

VALEUR PAR DÉFAUT :
Désactivé

13.2.2 *Protection contre les attaques réseau - Configurée*

DESCRIPTION :
Les protections contre les attaques réseau courantes doivent être configurées, incluant la protection contre les attaques par déni de service et les scans de ports.

```
netsh int ip show config
netsh advfirewall show allprofiles
Get-NetFirewallRule | Where-Object {$_.Direction -eq "Inbound" -and $_.Action -eq "Block"} | Select-Object DisplayName, Direction,
```

```
# Configuration de protection TCP/IP avancée
netsh int ip set global taskoffload=disabled
netsh int ip set global chimney=disabled

# Protection contre SYN flood
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters' -Name 'SynAttackProtect' -Value 2 -Type DWord
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters' -Name 'TcpMaxHalfOpen' -Value 500 -Type DWord
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters' -Name 'TcpMaxHalfOpenRetried' -Value 400 -Type DW

# Désactiver la source routing
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters' -Name 'DisableIPSourceRouting' -Value 2 -Type DWo
```

VALEUR PAR DÉFAUT :
Protections de base activées

13.3.1 *Contrôle de sécurité supplémentaire 1*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 1
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 1
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 1"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.4.1 *Contrôle de sécurité supplémentaire 2*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 2
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 2
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 2"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.5.1 *Contrôle de sécurité supplémentaire 3*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 3
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 3
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 3"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.6.1 *Contrôle de sécurité supplémentaire 4*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 4
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 4
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 4"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.7.1 *Contrôle de sécurité supplémentaire 5*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 5
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 5
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 5"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.8.1 *Contrôle de sécurité supplémentaire 6*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 6
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 6
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 6"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.9.1 *Contrôle de sécurité supplémentaire 7*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 7
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 7
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 7"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.10.1 *Contrôle de sécurité supplémentaire 8*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 8
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 8
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 8"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.11.1 *Contrôle de sécurité supplémentaire 9*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 9
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 9
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 9"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.12.1 *Contrôle de sécurité supplémentaire 10*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 10
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 10
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 10"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.13.1 *Contrôle de sécurité supplémentaire 11*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 11
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 11
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 11"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.14.1 *Contrôle de sécurité supplémentaire 12*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 12
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 12
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 12"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

13.15.1 *Contrôle de sécurité supplémentaire 13*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 13. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 13
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 13
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 13"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

🔒 SECTION 14 : MICROSOFT DEFENDER ANTIVIRUS

14.1 — Configuration de base

14.1.1 *Protection en temps réel - Activée*

DESCRIPTION :
La protection en temps réel de Microsoft Defender Antivirus doit être activée en permanence pour détecter et bloquer les menaces en temps réel.

```
Get-MpComputerStatus | Select-Object AntivirusEnabled, RealTimeProtectionEnabled, OnAccessProtectionEnabled
Get-MpPreference | Select-Object DisableRealtimeMonitoring, DisableOnAccessProtection
```

```
# Activer la protection en temps réel
Set-MpPreference -DisableRealtimeMonitoring $false
Set-MpPreference -DisableOnAccessProtection $false

# Configurer les analyses automatiques
Set-MpPreference -ScanScheduleDay Everyday -ScanScheduleTime 120
Set-MpPreference -CheckForSignaturesBeforeRunningScan $true
```

VALEUR PAR DÉFAUT :
Activé par défaut sur Windows 11

14.1.2 *Protection fournie par le cloud - Activée*

DESCRIPTION :
La protection fournie par le cloud (MAPS - Microsoft Active Protection Service) doit être activée pour bénéficier des dernières signatures et de l'intelligence des menaces en temps réel.

```
Get-MpPreference | Select-Object MAPSReporting, SubmitSamplesConsent
Get-MpComputerStatus | Select-Object AMEngineVersion, AntivirusSignatureVersion
```

```
# Activer MAPS avec envoi d'échantillons automatique
Set-MpPreference -MAPSReporting Advanced
Set-MpPreference -SubmitSamplesConsent SendAllSamples

# Activer le blocage à la première vue
Set-MpPreference -DisableBlockAtFirstSeen $false
```

VALEUR PAR DÉFAUT :
Activé avec niveau de base

14.1.3 *Analyse comportementale - Activée*

DESCRIPTION :
L'analyse comportementale doit être activée pour détecter les comportements malveillants qui ne sont pas détectés par les signatures traditionnelles.

```
Get-MpPreference | Select-Object DisableBehaviorMonitoring, DisableIOAVProtection, DisableScriptScanning
```

```
# Activer toutes les protections comportementales
Set-MpPreference -DisableBehaviorMonitoring $false
Set-MpPreference -DisableIOAVProtection $false
Set-MpPreference -DisableScriptScanning $false
Set-MpPreference -DisableInboundConnectionFiltering $false
```

VALEUR PAR DÉFAUT :
Activé par défaut
14.2 — Configuration avancée

14.2.1 *Exclusions d'analyse - Minimisées*

DESCRIPTION :
Les exclusions d'analyse de Windows Defender doivent être minimisées et régulièrement auditées. Chaque exclusion réduit le niveau de protection.

```
Get-MpPreference | Select-Object ExclusionPath, ExclusionProcess, ExclusionExtension
Get-MpPreference | Select-Object AttackSurfaceReductionRules_Actions, AttackSurfaceReductionRules_Ids
```

```
# Audit des exclusions actuelles
$Exclusions = Get-MpPreference
Write-Output "Chemins exclus: $($Exclusions.ExclusionPath -join '; ')"
Write-Output "Processus exclus: $($Exclusions.ExclusionProcess -join '; ')"
Write-Output "Extensions exclues: $($Exclusions.ExclusionExtension -join '; ')"

# Supprimer les exclusions non nécessaires (exemple)
# Remove-MpPreference -ExclusionPath "C:\Temp"

# Configurer des règles ASR (Attack Surface Reduction)
$ASRRules = @{
    "BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550" = "Enabled"  # Block executable content download
    "D4F940AB-401B-4EFC-AADC-AD5F3C50688A" = "Enabled"  # Block Office applications from creating child processes
    "3B576869-A4EC-4529-8536-B80A7769E899" = "Enabled"  # Block Office applications from creating executable content
}

foreach ($Rule in $ASRRules.GetEnumerator()) {
    Add-MpPreference -AttackSurfaceReductionRules_Ids $Rule.Key -AttackSurfaceReductionRules_Actions $Rule.Value
}
```

VALEUR PAR DÉFAUT :
Aucune exclusion par défaut

14.3.1 *Contrôle de sécurité supplémentaire 1*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 14. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 1
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 1
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 1"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

14.4.1 *Contrôle de sécurité supplémentaire 2*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 14. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 2
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 2
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 2"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

14.5.1 *Contrôle de sécurité supplémentaire 3*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 14. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 3
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 3
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 3"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

14.6.1 *Contrôle de sécurité supplémentaire 4*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 14. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 4
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 4
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 4"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

14.7.1 *Contrôle de sécurité supplémentaire 5*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 14. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 5
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 5
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 5"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

14.8.1 *Contrôle de sécurité supplémentaire 6*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 14. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 6
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 6
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 6"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

14.9.1 *Contrôle de sécurité supplémentaire 7*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 14. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 7
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 7
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 7"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

14.10.1 *Contrôle de sécurité supplémentaire 8*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 14. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.

```
# Commandes de vérification pour Contrôle de sécurité supplémentaire 8
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
auditpol /get /category:*
```

```
# Configuration sécurisée pour Contrôle de sécurité supplémentaire 8
Write-Host "Configuration de sécurité pour: Contrôle de sécurité supplémentaire 8"
# Implémenter les mesures appropriées
```

VALEUR PAR DÉFAUT :
Variable selon la configuration

14.11.1 *Contrôle de sécurité supplémentaire 9*

DESCRIPTION :
Mesure de sécurité complémentaire pour renforcer la protection de la section 14. Cette mesure contribue à l'élévation du niveau de sécurité global selon les meilleures pratiques de l'industrie.