Checklist Sécurité WINDOWS SERVER 2025 — SERVEUR MEMBRE

Ayi NEDJIMI Consultants
ayinedjimi-consultants.fr
v1.0 — 2026-04-04 · 221 controles

Sommaire

Section 1 — POLITIQUE DE COMPTES (Account Policies)

1.1 — Politique de mot de passe (Password Policy)

1.1.1 *Appliquer l'historique des mots de passe* — Critique

MITRE ATT&CK : T1110.001 (Brute Force: Password Guessing)

DESCRIPTION :

Ce contrôle définit le nombre de mots de passe uniques qu'un utilisateur doit utiliser avant de pouvoir réutiliser un ancien mot de passe. La configuration à 24 mots de passe mémorisés empêche les utilisateurs de recycler continuellement les mêmes mots de passe. Sans cette protection, un attaquant ayant compromis un ancien mot de passe pourrait attendre que l'utilisateur y revienne. Ce paramètre est fondamental pour la politique de sécurité des identifiants selon l'ANSSI et le CIS.

Impact métier : La réutilisation de mots de passe expose l'organisation aux attaques par credential stuffing et permet à un attaquant de maintenir un accès persistant même après une rotation de mot de passe.

AUDIT :

- Ouvrir la console de stratégie de sécurité locale : `secpol.msc`
- Naviguer vers : Stratégies de compte > Stratégie de mot de passe
- Vérifier « Conserver l'historique des mots de passe »
- Via PowerShell :

```
# Vérification via secedit
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "PasswordHistorySize"
# Via net accounts
net accounts | findstr /i "historique\|history"
```

AUDIT :

- Valeur attendue : **24 mots de passe ou plus**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe > Conserver l'historique des mots de passe` → **24 mots de passe mémorisés**
2. Via PowerShell :

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

REMÉDIATION :

1. Via secedit : Modifier `PasswordHistorySize = 24` dans le fichier de configuration de sécurité
2. Via LGPO : `LGPO.exe /s secpol-baseline.inf`

VALEUR PAR DÉFAUT :

24 mots de passe mémorisés (dans un domaine Active Directory)

1.1.2 *Âge maximum du mot de passe* — Élevé

MITRE ATT&CK : T1110.002 (Brute Force: Password Cracking)

DESCRIPTION :

Ce paramètre détermine la durée maximale (en jours) pendant laquelle un mot de passe peut être utilisé avant que le système n'exige sa modification. Le CIS recommande une valeur entre 1 et 365 jours, tandis que l'ANSSI préconise un renouvellement tous les 90 jours pour les comptes à privilèges. Une rotation trop fréquente peut pousser les utilisateurs à choisir des mots de passe faibles ou prévisibles (incrémentation). Le NIST SP 800-63B moderne recommande de ne forcer la rotation que sur compromission avérée, mais les référentiels CIS et DISA STIG maintiennent cette exigence.

Impact métier : Un mot de passe non renouvelé indéfiniment augmente la fenêtre d'exploitation en cas de compromission non détectée.

AUDIT :

- Console `secpol.msc` > Stratégies de compte > Stratégie de mot de passe
- Via PowerShell :

```
net accounts | findstr /i "maximum\|Maximum"
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "MaximumPasswordAge"
# Pour les comptes AD :
Get-ADDefaultDomainPasswordPolicy | Select-Object MaxPasswordAge
```

AUDIT :

- Valeur attendue : **entre 1 et 365 jours** (recommandé : 60 à 90 jours pour comptes privilégiés)

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe > Durée de vie maximale du mot de passe` → **365 jours** (ou 60 pour les comptes à privilèges)
2. Via PowerShell :

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

REMÉDIATION :

1. Via registre (politique locale) : Configurer via secedit ou LGPO

VALEUR PAR DÉFAUT :

42 jours (dans un domaine Active Directory)

1.1.3 *Âge minimum du mot de passe* Élevé

MITRE ATT&CK : T1110.001 (Brute Force: Password Guessing)

DESCRIPTION :

L'âge minimum du mot de passe détermine le nombre de jours minimum qu'un utilisateur doit attendre avant de pouvoir modifier son mot de passe. Ce paramètre fonctionne en synergie avec l'historique des mots de passe : sans un âge minimum, un utilisateur pourrait changer son mot de passe 24 fois rapidement pour revenir à son mot de passe initial, contournant ainsi la politique d'historique. Le CIS recommande une valeur d'au moins 1 jour.

Impact métier : Sans ce contrôle, la politique d'historique des mots de passe devient inefficace, permettant le recyclage immédiat des mots de passe compromis.

AUDIT :

- Console `secpol.msc` > Stratégies de compte > Stratégie de mot de passe
- Via PowerShell :

```
net accounts | findstr /i "minimum\|Minimum"
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "MinimumPasswordAge"
```

AUDIT :

- Valeur attendue : **1 jour ou plus**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe > Durée de vie minimale du mot de passe` → **1 jour**
2. Via PowerShell :

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

VALEUR PAR DÉFAUT :

1 jour (dans un domaine Active Directory)

1.1.4 *Longueur minimale du mot de passe* Critique

MITRE ATT&CK : T1110.002 (Brute Force: Password Cracking)

DESCRIPTION :

La longueur minimale du mot de passe est le paramètre le plus déterminant pour la résistance aux attaques par force brute. Le CIS Benchmark v2.0.0 pour Windows Server 2025 recommande un minimum de 14 caractères, aligné avec les recommandations ANSSI et DISA STIG. Chaque caractère supplémentaire augmente exponentiellement le temps de craquage. Un mot de passe de 8 caractères peut être cracké en quelques heures avec du matériel moderne (GPU), tandis qu'un mot de passe de 14+ caractères nécessite des années.

Impact métier : Des mots de passe courts sont vulnérables aux attaques par force brute et dictionnaire. La compromission d'un seul compte peut entraîner un accès non autorisé aux ressources critiques.

AUDIT :

- Console `secpol.msc` > Stratégies de compte > Stratégie de mot de passe
- Via PowerShell :

```
net accounts | findstr /i "longueur\|length\|Minimum password"
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "MinimumPasswordLength"
# Vérification avancée pour Windows Server 2025
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SAM" -Name "MinimumPasswordLength" -ErrorAction SilentlyContinue
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\SAM\MinimumPasswordLength`
- Valeur attendue : **14 caractères ou plus**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe > Longueur minimale du mot de passe` → **14 caractères**
2. Via PowerShell :

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

REMÉDIATION :

1. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SAM" -Name "MinimumPasswordLength" -Value 14
```

VALEUR PAR DÉFAUT :

7 caractères (dans un domaine Active Directory)

1.1.5 *Le mot de passe doit respecter des exigences de complexité* Critique

MITRE ATT&CK : T1110.002 (Brute Force: Password Cracking)

DESCRIPTION :

Lorsque cette stratégie est activée, les mots de passe doivent contenir des caractères d'au moins trois des quatre catégories : lettres majuscules (A-Z), lettres minuscules (a-z), chiffres (0-9), et caractères spéciaux (!@#$%^&*). De plus, le mot de passe ne peut pas contenir le nom de l'utilisateur ni plus de deux caractères consécutifs du nom complet. Cette exigence réduit considérablement l'efficacité des attaques par dictionnaire.

Impact métier : Sans complexité, les utilisateurs choisissent des mots de passe prévisibles (noms, dates, mots du dictionnaire) facilement devinables par les outils d'attaque automatisés.

AUDIT :

- Console `secpol.msc` > Stratégies de compte > Stratégie de mot de passe
- Via PowerShell :

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "PasswordComplexity"
```

AUDIT :

- Valeur attendue : **Activé (1)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe > Le mot de passe doit respecter des exigences de complexité` → **Activé**
2. Via secedit : `PasswordComplexity = 1`

VALEUR PAR DÉFAUT :

Activé (dans un domaine Active Directory)

1.1.6 *Assouplir les limites de longueur minimale du mot de passe* Moyen

MITRE ATT&CK : T1110.002 (Brute Force: Password Cracking)

DESCRIPTION :

Ce paramètre, nouveau dans Windows Server 2019+ et maintenu dans Windows Server 2025, permet de configurer des longueurs minimales de mot de passe supérieures à 14 caractères via la stratégie de groupe traditionnelle. Sans ce paramètre activé, la longueur minimale est plafonnée à 14 caractères dans l'interface de GPO classique. L'activation de ce paramètre est un prérequis pour pouvoir appliquer des politiques de mots de passe plus longues (15, 16 caractères ou plus).

Impact métier : Limite la capacité à appliquer des politiques de mots de passe robustes au-delà de 14 caractères.

AUDIT :

- Via PowerShell :

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

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\SAM\RelaxMinimumPasswordLengthLimits`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe > Assouplir les limites de longueur minimale du mot de passe` → **Activé**
2. Via registre :

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

VALEUR PAR DÉFAUT :

Non défini

1.1.7 *Stocker les mots de passe en utilisant un chiffrement réversible* Critique

MITRE ATT&CK : T1003.002 (OS Credential Dumping: Security Account Manager)

DESCRIPTION :

Ce paramètre contrôle si Windows stocke les mots de passe dans un format réversible (essentiellement en texte clair chiffré). Cette option existe uniquement pour la compatibilité avec des protocoles d'authentification anciens (CHAP via accès distant, authentification Digest dans IIS). L'activation de ce paramètre équivaut à stocker les mots de passe en clair et représente un risque de sécurité critique. Si un attaquant accède à la base SAM ou NTDS.dit, il peut récupérer tous les mots de passe en clair.

Impact métier : Compromission totale de tous les identifiants en cas d'accès à la base de données de sécurité. Risque de violation de données massif.

AUDIT :

- Console `secpol.msc` > Stratégies de compte > Stratégie de mot de passe
- Via PowerShell :

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "ClearTextPassword"
```

AUDIT :

- Valeur attendue : **Désactivé (0)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe > Stocker les mots de passe en utilisant un chiffrement réversible` → **Désactivé**
2. Via secedit : `ClearTextPassword = 0`

VALEUR PAR DÉFAUT :

Désactivé

1.1.8 *Audit de longueur minimale du mot de passe* Moyen

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Ce paramètre d'audit, introduit dans les versions récentes de Windows, permet de journaliser les tentatives de création de mots de passe dont la longueur est inférieure à un seuil configuré. Il ne bloque pas la création du mot de passe mais génère un événement d'audit. Cela permet aux administrateurs d'identifier les comptes avec des mots de passe potentiellement trop courts avant d'appliquer une politique plus stricte, facilitant une transition en douceur.

Impact métier : Sans cet audit, il est impossible d'évaluer l'impact d'un durcissement de la politique de longueur de mot de passe avant son déploiement.

AUDIT :

- Via PowerShell :

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SAM" -Name "MinimumPasswordLengthAudit" -ErrorAction SilentlyContinu
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\SAM\MinimumPasswordLengthAudit`
- Valeur attendue : **14 ou plus**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe > Audit de longueur minimale du mot de passe` → **14**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SAM" -Name "MinimumPasswordLengthAudit" -Value 14 -Type DWord
```

VALEUR PAR DÉFAUT :

Non configuré

1.2 — Politique de verrouillage de compte (Account Lockout Policy)

1.2.1 *Durée de verrouillage des comptes* Critique

MITRE ATT&CK : T1110.003 (Brute Force: Password Spraying)

DESCRIPTION :

Ce paramètre détermine le nombre de minutes pendant lesquelles un compte reste verrouillé après avoir atteint le seuil de tentatives de connexion échouées. Le CIS recommande une durée d'au moins 15 minutes. Cette mesure ralentit considérablement les attaques par force brute automatisées et la pulvérisation de mots de passe. Une valeur de 0 signifie que le compte reste verrouillé jusqu'à ce qu'un administrateur le déverrouille manuellement, ce qui peut créer un vecteur de déni de service.

Impact métier : Sans verrouillage temporaire, les attaques par force brute peuvent s'exécuter sans interruption. Un verrouillage permanent (0) peut être exploité pour du déni de service contre des comptes critiques.

AUDIT :

- Console `secpol.msc` > Stratégies de compte > Stratégie de verrouillage du compte
- Via PowerShell :

```
net accounts | findstr /i "verrouillage\|lockout\|duration"
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "LockoutDuration"
```

AUDIT :

- Valeur attendue : **15 minutes ou plus**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de verrouillage du compte > Durée de verrouillage des comptes` → **15 minutes**
2. Via PowerShell :

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

VALEUR PAR DÉFAUT :

Non défini (car le seuil de verrouillage est à 0 par défaut)

1.2.2 *Seuil de verrouillage du compte* Critique

MITRE ATT&CK : T1110.003 (Brute Force: Password Spraying)

DESCRIPTION :

Ce paramètre définit le nombre de tentatives de connexion échouées autorisées avant le verrouillage du compte. Le CIS recommande un seuil entre 1 et 5 tentatives. Une valeur trop basse (1-2) peut entraîner des verrouillages accidentels fréquents, tandis qu'une valeur trop haute réduit l'efficacité de la protection. La valeur de 5 représente un bon compromis entre sécurité et utilisabilité. Ce paramètre est essentiel pour contrer les attaques par pulvérisation de mots de passe (password spraying).

Impact métier : Sans seuil de verrouillage, un attaquant peut tester un nombre illimité de mots de passe contre chaque compte sans déclencher d'alerte ni de blocage.

AUDIT :

- Console `secpol.msc` > Stratégies de compte > Stratégie de verrouillage du compte
- Via PowerShell :

```
net accounts | findstr /i "seuil\|threshold"
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "LockoutBadCount"
```

AUDIT :

- Valeur attendue : **entre 1 et 5 tentatives**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de verrouillage du compte > Seuil de verrouillage du compte` → **5 tentatives**
2. Via PowerShell :

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

VALEUR PAR DÉFAUT :

0 (verrouillage désactivé) — **NON CONFORME**

1.2.3 *Réinitialiser le compteur de verrouillage du compte après* Critique

MITRE ATT&CK : T1110.003 (Brute Force: Password Spraying)

DESCRIPTION :

Ce paramètre détermine le nombre de minutes après une tentative de connexion échouée avant que le compteur de tentatives échouées ne soit réinitialisé à 0. Cette valeur doit être inférieure ou égale à la durée de verrouillage. Le CIS recommande au moins 15 minutes. Un délai trop court permet à un attaquant de relancer ses tentatives de force brute rapidement après la réinitialisation du compteur.

Impact métier : Un compteur qui se réinitialise trop rapidement annule l'efficacité du seuil de verrouillage, permettant des attaques par force brute lentes mais continues.

AUDIT :

- Console `secpol.msc` > Stratégies de compte > Stratégie de verrouillage du compte
- Via PowerShell :

```
net accounts | findstr /i "fenêtre\|observation\|window"
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "ResetLockoutCount"
```

AUDIT :

- Valeur attendue : **15 minutes ou plus**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de verrouillage du compte > Réinitialiser le compteur de verrouillage du compte après` → **15 minutes**
2. Via PowerShell :

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

VALEUR PAR DÉFAUT :

Non défini

1.2.4 *Autoriser le verrouillage du compte Administrateur* — Critique

MITRE ATT&CK : T1110.001 (Brute Force: Password Guessing)

DESCRIPTION :

Par défaut dans les versions antérieures de Windows, le compte Administrateur intégré (RID 500) était exempt de la politique de verrouillage, ce qui en faisait une cible privilégiée pour les attaques par force brute. Windows Server 2025 introduit la possibilité de soumettre ce compte au verrouillage. Le CIS recommande d'activer ce paramètre pour éliminer cette exception dangereuse. Note : ce paramètre ne s'applique qu'aux connexions réseau ; le compte Administrateur peut toujours se connecter en mode de récupération.

Impact métier : Sans verrouillage du compte Administrateur, un attaquant peut effectuer des tentatives de force brute illimitées sur le compte le plus privilégié du système.

AUDIT :

- Console `secpol.msc` > Stratégies de compte > Stratégie de verrouillage du compte
- Via PowerShell :

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas SECURITYPOLICY
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "AllowAdministratorLockout"
# Windows Server 2025 spécifique
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SAM" -Name "AllowAdministratorLockout" -ErrorAction SilentlyContinue
```

AUDIT :

- Valeur attendue : **Activé (1)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de verrouillage du compte > Autoriser le verrouillage du compte Administrateur` → **Activé**
2. Via registre :

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

VALEUR PAR DÉFAUT :

Activé (nouveau défaut dans Windows Server 2025)

1.3 — Politique Kerberos (référence domaine)

1.3.1 *Application des restrictions d'ouverture de session utilisateur* — Moyen

MITRE ATT&CK : T1558 (Steal or Forge Kerberos Tickets)

DESCRIPTION :

Ce paramètre détermine si le Centre de Distribution de Clés (KDC) valide chaque demande de ticket de session en vérifiant la politique de droits de l'utilisateur sur l'ordinateur cible. Cette validation supplémentaire, bien qu'elle engendre un léger surcoût de performance, garantit que les utilisateurs ne peuvent pas obtenir de tickets de service pour des machines auxquelles ils n'ont pas le droit d'accéder. C'est un mécanisme de défense en profondeur contre l'abus de tickets Kerberos.

Impact métier : Sans cette restriction, un utilisateur pourrait obtenir un ticket de service pour un serveur auquel ses droits d'accès ont été révoqués récemment.

AUDIT :

- Via PowerShell (sur un contrôleur de domaine ou depuis le serveur membre) :

```
# Depuis le serveur membre, interroger la politique du domaine
Get-ADDefaultDomainPasswordPolicy | Select-Object -ExpandProperty ComplexityEnabled
# Via gpresult pour voir les paramètres Kerberos appliqués
gpresult /r /scope:computer | findstr /i "kerberos"
```

AUDIT :

- Valeur attendue : **Activé**

REMÉDIATION :

1. Via GPO (Default Domain Policy) : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie Kerberos > Appliquer les restrictions pour l'ouverture de session utilisateur` → **Activé**

VALEUR PAR DÉFAUT :

Activé

1.3.2 *Durée de vie maximale du ticket de service* Moyen

MITRE ATT&CK : T1558.003 (Steal or Forge Kerberos Tickets: Kerberoasting)

DESCRIPTION :

Ce paramètre définit la durée maximale (en minutes) pendant laquelle un ticket de service Kerberos (TGS) reste valide. Le CIS recommande une valeur de 600 minutes (10 heures). Des tickets à longue durée de vie augmentent la fenêtre d'exploitation pour les attaques de type Kerberoasting. La réduction de cette durée limite le temps pendant lequel un ticket volé peut être utilisé, mais une valeur trop basse peut entraîner des interruptions de service dues aux renouvellements fréquents.

Impact métier : Des tickets de service à longue durée de vie permettent à un attaquant d'utiliser un ticket compromis pendant une période prolongée sans avoir besoin de se réauthentifier.

```
# Depuis le serveur membre, vérifier via gpresult
gpresult /r /scope:computer 2>$null | Select-String -Pattern "Kerberos"
# Ou interroger le domaine
([ADSI]"LDAP://$(([ADSI]'LDAP://RootDSE').defaultNamingContext)").maxServiceTicketAge
```

AUDIT :

- Valeur attendue : **600 minutes ou moins**

REMÉDIATION :

1. Via GPO (Default Domain Policy) : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie Kerberos > Durée de vie maximale du ticket de service` → **600 minutes**

VALEUR PAR DÉFAUT :

600 minutes

1.3.3 *Durée de vie maximale du ticket utilisateur* Moyen

MITRE ATT&CK : T1558.001 (Steal or Forge Kerberos Tickets: Golden Ticket)

DESCRIPTION :

Ce paramètre définit la durée maximale (en heures) du Ticket d'Octroi de Tickets (TGT) Kerberos. Le CIS recommande une valeur de 10 heures. Le TGT est le ticket maître utilisé pour obtenir des tickets de service. Un TGT compromis (via un Golden Ticket par exemple) donne un accès total au domaine. Réduire la durée de vie du TGT limite la fenêtre d'exploitation en cas de compromission de la clé du compte KRBTGT.

Impact métier : Un TGT à longue durée de vie augmente la fenêtre temporelle pendant laquelle un attaquant peut exploiter un ticket volé ou forgé.

```
# Vérification via klist sur le serveur membre
klist
# Vérification de la politique de domaine
gpresult /h C:\ANC-Audit\gpresult.html /f
```

AUDIT :

- Valeur attendue : **10 heures ou moins**

REMÉDIATION :

1. Via GPO (Default Domain Policy) : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie Kerberos > Durée de vie maximale du ticket utilisateur` → **10 heures**

VALEUR PAR DÉFAUT :

10 heures

1.3.4 *Durée de vie maximale pour le renouvellement du ticket utilisateur* Moyen

MITRE ATT&CK : T1558.001 (Steal or Forge Kerberos Tickets: Golden Ticket)

DESCRIPTION :

Ce paramètre détermine la période (en jours) pendant laquelle un TGT peut être renouvelé. Le CIS recommande 7 jours. Passé ce délai, l'utilisateur doit se réauthentifier complètement. Ce mécanisme de renouvellement permet aux sessions longues de continuer sans réauthentification, mais une fenêtre de renouvellement trop longue augmente le risque d'utilisation prolongée de tickets compromis.

Impact métier : Une fenêtre de renouvellement excessive permet le maintien d'un accès non autorisé pendant une période prolongée sans nécessiter de nouvelle authentification.

```
gpresult /r /scope:computer | Select-String -Pattern "renewal"
```

AUDIT :

- Valeur attendue : **7 jours ou moins**

REMÉDIATION :

1. Via GPO (Default Domain Policy) : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie Kerberos > Durée de vie maximale pour le renouvellement du ticket utilisateur` → **7 jours**

VALEUR PAR DÉFAUT :

7 jours

1.3.5 *Tolérance maximale pour la synchronisation de l'horloge* Moyen

MITRE ATT&CK : T1558 (Steal or Forge Kerberos Tickets)

DESCRIPTION :

L'authentification Kerberos repose sur la synchronisation horaire entre le client et le serveur. Ce paramètre définit la tolérance maximale (en minutes) pour la dérive de l'horloge. Le CIS recommande 5 minutes. Une tolérance trop grande ouvre la porte aux attaques par rejeu de tickets (replay attacks). Une tolérance trop faible peut causer des échecs d'authentification si le serveur NTP n'est pas correctement configuré.

Impact métier : Une dérive horaire excessive peut causer des échecs d'authentification Kerberos. Une tolérance trop permissive permet les attaques par rejeu.

```
# Vérifier la synchronisation horaire
w32tm /query /status
w32tm /query /configuration
# Vérifier le décalage horaire avec le DC
w32tm /stripchart /computer:DC01 /samples:3 /dataonly
```

AUDIT :

- Valeur attendue : **5 minutes ou moins**

REMÉDIATION :

1. Via GPO (Default Domain Policy) : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie Kerberos > Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur` → **5 minutes**
2. Configurer le service NTP :

```
w32tm /config /manualpeerlist:"ntp.pool.org" /syncfromflags:MANUAL /reliable:YES /update
Restart-Service w32time
w32tm /resync
```

VALEUR PAR DÉFAUT :

5 minutes

1.4 — Gestion des comptes locaux et LAPS

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

MITRE ATT&CK : T1078.003 (Valid Accounts: Local Accounts)

DESCRIPTION :

Windows LAPS (Local Administrator Password Solution), natif dans Windows Server 2025, gère automatiquement les mots de passe des comptes administrateur locaux en les faisant tourner régulièrement et en les stockant de manière sécurisée dans Active Directory ou Azure AD. Sans LAPS, les mots de passe administrateur locaux sont souvent identiques sur tous les serveurs, ce qui facilite le mouvement latéral via Pass-the-Hash. Windows Server 2025 intègre LAPS nativement (remplaçant le Legacy LAPS) avec support du stockage dans Azure AD et du chiffrement des mots de passe.

Impact métier : Sans LAPS, la compromission d'un seul mot de passe administrateur local donne accès à tous les serveurs utilisant le même mot de passe, permettant un mouvement latéral généralisé.

```
# Vérifier si Windows LAPS est configuré
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\LAPS\Config" -ErrorAction SilentlyContinue
# Vérifier la politique LAPS via GPO
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Policies\LAPS" -ErrorAction SilentlyContinue
# Vérifier le statut LAPS du compte géré
Get-LapsAADPassword -DeviceIds (Get-ComputerInfo).CsName -ErrorAction SilentlyContinue
Get-LapsDiagnostics -ErrorAction SilentlyContinue
# Vérifier l'état via le module LAPS
Get-Command -Module LAPS -ErrorAction SilentlyContinue
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Policies\LAPS`
- Valeur attendue : **LAPS configuré et actif, rotation ≤ 30 jours**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Système > LAPS`
2. Activer « Configurer la sauvegarde du mot de passe » → Active Directory ou Azure AD
3. Configurer « Paramètres du mot de passe » → Complexité élevée, longueur 20+, âge 30 jours
4. Via PowerShell :

```
# Mettre à jour le schéma AD pour LAPS (sur un DC)
Update-LapsADSchema
# Configurer les permissions
Set-LapsADComputerSelfPermission -Identity "OU=Servers,DC=domain,DC=com"
```

VALEUR PAR DÉFAUT :

Non configuré — **NON CONFORME**

1.4.2 *Renommer le compte administrateur local* — Élevé

MITRE ATT&CK : T1078.003 (Valid Accounts: Local Accounts)

DESCRIPTION :

Le compte Administrateur intégré (RID 500) est une cible connue pour les attaques automatisées. Le renommer ne constitue pas une mesure de sécurité forte (le SID reste identifiable), mais cela ajoute une couche d'obscurité qui bloque les scripts d'attaque basiques et les scanners automatisés qui ciblent le nom « Administrator » ou « Administrateur ». Cette mesure est recommandée par le CIS, l'ANSSI et le DISA STIG comme défense en profondeur.

Impact métier : Les attaques automatisées ciblant le compte « Administrator » par nom sont bloquées, réduisant le bruit dans les journaux de sécurité.

```
# Vérifier le nom actuel du compte RID 500
Get-LocalUser | Where-Object { $_.SID -like "*-500" } | Select-Object Name, SID, Enabled
# Via WMI
Get-WmiObject Win32_UserAccount | Where-Object { $_.SID -match "-500$" } | Select-Object Name
```

AUDIT :

- Valeur attendue : **Nom différent de « Administrator » et « Administrateur »**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Comptes : Renommer le compte Administrateur` → nom personnalisé (ex: `ANC_Admin_Local`)
2. Via PowerShell :

```
Rename-LocalUser -Name "Administrator" -NewName "ANC_Admin_Local"
```

VALEUR PAR DÉFAUT :

Administrator / Administrateur

1.4.3 *Renommer le compte Invité* — Moyen

MITRE ATT&CK : T1078.003 (Valid Accounts: Local Accounts)

DESCRIPTION :

Le compte Invité intégré, bien qu'il soit désactivé par défaut, devrait être renommé pour ajouter une couche supplémentaire de protection. Ce renommage empêche les outils d'attaque automatisés de cibler ce compte par son nom par défaut. Combiné avec la désactivation du compte (contrôle 1.4.4), cela élimine un vecteur d'attaque potentiel.

Impact métier : Risque faible mais mesure de défense en profondeur recommandée par le CIS pour limiter la surface d'attaque.

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

AUDIT :

- Valeur attendue : **Nom différent de « Guest » et « Invité »**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Comptes : Renommer le compte Invité` → nom personnalisé
2. Via PowerShell :

```
Rename-LocalUser -Name "Guest" -NewName "ANC_Invite_Disabled"
```

VALEUR PAR DÉFAUT :

Guest / Invité

1.4.4 *Désactiver le compte Invité* — Élevé

MITRE ATT&CK : T1078.003 (Valid Accounts: Local Accounts)

DESCRIPTION :

Le compte Invité permet un accès anonyme au système sans authentification. Sa désactivation est essentielle pour empêcher tout accès non autorisé. Bien que désactivé par défaut dans Windows Server 2025, cette vérification est cruciale car des scripts ou des applications peuvent le réactiver. Le compte Invité ne doit jamais être utilisé dans un environnement de production.

Impact métier : Un compte Invité actif permet un accès non authentifié au système, pouvant servir de point d'entrée pour une compromission.

```
Get-LocalUser -Name "Guest" -ErrorAction SilentlyContinue | Select-Object Name, Enabled
# Ou par SID
Get-LocalUser | Where-Object { $_.SID -like "*-501" } | Select-Object Name, Enabled
```

AUDIT :

- Valeur attendue : **Désactivé (Enabled = False)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Comptes : État du compte Invité` → **Désactivé**
2. Via PowerShell :

```
Disable-LocalUser -Name "Guest"
```

VALEUR PAR DÉFAUT :

Désactivé

1.4.5 *Désactiver le compte Administrateur local intégré* Élevé

MITRE ATT&CK : T1078.003 (Valid Accounts: Local Accounts)

DESCRIPTION :

Le compte Administrateur intégré (RID 500) devrait être désactivé lorsque LAPS est déployé ou lorsqu'un autre compte administrateur est disponible. Ce compte possède des propriétés spéciales (non verrouillable par défaut dans les anciennes versions, SID prévisible) qui en font une cible de choix. En cas d'utilisation de LAPS, le compte peut rester activé mais doit être géré exclusivement via LAPS.

Impact métier : Un compte Administrateur local activé sans gestion LAPS représente un risque de compromission par force brute et de mouvement latéral.

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

AUDIT :

- Valeur attendue : **Désactivé (sauf si géré par LAPS)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Comptes : État du compte Administrateur` → **Désactivé**
2. Via PowerShell :

```
Disable-LocalUser -SID (Get-LocalUser | Where-Object { $_.SID -like "*-500" }).SID
```

VALEUR PAR DÉFAUT :

Activé (avec mot de passe généré aléatoirement lors de l'installation)

1.4.6 *Utilisation de comptes de service gérés de groupe (gMSA)* Élevé

MITRE ATT&CK : T1078.002 (Valid Accounts: Domain Accounts)

DESCRIPTION :

Les comptes de service gérés de groupe (Group Managed Service Accounts - gMSA) offrent une gestion automatique des mots de passe pour les comptes de service avec une rotation tous les 30 jours et des mots de passe de 240 caractères générés aléatoirement. Cette fonctionnalité élimine le risque lié aux mots de passe de comptes de service statiques qui ne sont jamais changés et sont souvent stockés en clair dans des scripts ou des fichiers de configuration.

Impact métier : Les comptes de service avec des mots de passe statiques sont des cibles privilégiées pour les attaques Kerberoasting et le mouvement latéral.

```
# Lister les comptes de service sur le serveur
Get-WmiObject Win32_Service | Where-Object { $_.StartName -ne "LocalSystem" -and $_.StartName -ne "NT AUTHORITY\LocalService" -and
# Vérifier si des gMSA sont utilisés
Get-ADServiceAccount -Filter * -ErrorAction SilentlyContinue | Select-Object Name, Enabled, PasswordLastSet
# Vérifier les services utilisant des comptes de domaine (non-gMSA)
Get-WmiObject Win32_Service | Where-Object { $_.StartName -match "\\" -and $_.StartName -notmatch "\$" } | Select-Object Name, Star
```

AUDIT :

- Valeur attendue : **Tous les comptes de service domaine utilisent gMSA ou ont des justifications documentées**

REMÉDIATION :

1. Créer un gMSA :

```
New-ADServiceAccount -Name "gMSA_ServiceName" -DNSHostName "server.domain.com" -PrincipalsAllowedToRetrieveManagedPassword "Server$
Install-ADServiceAccount -Identity "gMSA_ServiceName"
# Configurer le service pour utiliser le gMSA
Set-Service -Name "ServiceName" -ServiceAccountName "domain\gMSA_ServiceName$"
```

VALEUR PAR DÉFAUT :

Non configuré — comptes de service manuels

1.4.7 *Restreindre l'utilisation de mots de passe vides pour les comptes locaux* Critique

MITRE ATT&CK : T1078.003 (Valid Accounts: Local Accounts)

DESCRIPTION :

Ce paramètre, lorsqu'il est activé, empêche les comptes locaux avec des mots de passe vides de se connecter via le réseau (RDP, SMB, WinRM). Les connexions console restent possibles. Cette restriction est essentielle pour empêcher l'exploitation de comptes locaux créés sans mot de passe, ce qui est particulièrement risqué dans les environnements où des comptes de test ou temporaires peuvent exister.

Impact métier : Un compte avec un mot de passe vide accessible depuis le réseau constitue une porte d'entrée triviale pour tout attaquant sur le réseau.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LimitBlankPasswordUse"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Comptes : Restreindre l'utilisation de mots de passe vides par le compte local à l'ouverture de session console` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LimitBlankPasswordUse" -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :

Activé

1.4.8 *Bloquer les comptes Microsoft pour l'authentification* Élevé

MITRE ATT&CK : T1078.004 (Valid Accounts: Cloud Accounts)

DESCRIPTION :

Ce paramètre empêche les utilisateurs de se connecter au serveur avec un compte Microsoft (compte personnel @outlook.com, @live.com, etc.). Dans un environnement d'entreprise, seuls les comptes de domaine Active Directory ou Azure AD doivent être utilisés pour l'authentification. L'autorisation des comptes Microsoft sur un serveur de production crée un canal d'authentification non contrôlé par les politiques de sécurité de l'entreprise.

Impact métier : L'utilisation de comptes Microsoft sur un serveur d'entreprise contourne les politiques de sécurité du domaine, l'audit centralisé et le contrôle d'accès.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "NoConnectedUser" -ErrorAction Silen
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\NoConnectedUser`
- Valeur attendue : **3 (Les utilisateurs ne peuvent pas ajouter ni se connecter avec des comptes Microsoft)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Comptes : Bloquer les comptes Microsoft` → **Les utilisateurs ne peuvent pas ajouter ni se connecter avec des comptes Microsoft**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "NoConnectedUser" -Value 3 -Type DWo
```

VALEUR PAR DÉFAUT :

Non défini

Section 2 — STRATÉGIES LOCALES (Local Policies)

2.1 — Attribution des droits utilisateur (User Rights Assignment)

2.1.1 *Accéder à cet ordinateur depuis le réseau* — Élevé

MITRE ATT&CK : T1021 (Remote Services)

DESCRIPTION :

Ce droit détermine quels utilisateurs et groupes peuvent se connecter au serveur via le réseau (SMB, RPC, etc.). Pour un serveur membre, le CIS recommande de limiter ce droit aux groupes Administrateurs et Utilisateurs authentifiés. Tout compte ou groupe supplémentaire augmente la surface d'attaque réseau. L'attribution de ce droit au groupe « Tout le monde » est particulièrement dangereuse car elle permet des connexions anonymes.

Impact métier : Un accès réseau trop permissif permet aux attaquants de tenter des connexions SMB, d'énumérer les partages et de lancer des attaques de mouvement latéral.

```
# Vérifier via secedit
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeNetworkLogonRight"
# Via ntrights (Resource Kit)
# Via PowerShell avancé
$sid = New-Object System.Security.Principal.SecurityIdentifier("S-1-5-32-544")
whoami /priv
```

AUDIT :

- Valeur attendue : **Administrateurs, Utilisateurs authentifiés** uniquement

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Accéder à cet ordinateur depuis le réseau` → **Administrateurs, Utilisateurs authentifiés**
2. Via secedit : `SeNetworkLogonRight = *S-1-5-32-544,*S-1-5-11`

VALEUR PAR DÉFAUT :

Administrateurs, Opérateurs de sauvegarde, Utilisateurs, Tout le monde

2.1.2 *Agir en tant que partie du système d'exploitation* — Critique

MITRE ATT&CK : T1134 (Access Token Manipulation)

DESCRIPTION :

Ce droit permet à un processus d'usurper l'identité de n'importe quel utilisateur sans authentification, obtenant ainsi un accès aux ressources locales auxquelles cet utilisateur a accès. Ce privilège est extrêmement dangereux et ne doit être attribué à aucun utilisateur ou groupe. Seul le système d'exploitation lui-même (compte LocalSystem) devrait avoir ce droit. Un processus disposant de ce privilège peut créer des jetons d'accès avec n'importe quel SID et n'importe quels privilèges.

Impact métier : L'attribution de ce droit à un compte utilisateur ou de service équivaut à donner un accès système complet, permettant une escalade de privilèges totale.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeTcbPrivilege"
```

AUDIT :

- Valeur attendue : **Personne (aucun compte)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Agir en tant que partie du système d'exploitation` → **(vide)**

VALEUR PAR DÉFAUT :

Personne

2.1.3 *Permettre l'ouverture de session locale* — Élevé

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Ce droit détermine qui peut se connecter directement au serveur (console physique ou virtuelle). Le CIS recommande de limiter ce droit au groupe Administrateurs uniquement sur un serveur membre. Permettre l'ouverture de session locale à des utilisateurs non-administrateurs augmente le risque d'escalade de privilèges locale et d'accès non autorisé aux ressources du serveur.

Impact métier : Des utilisateurs non autorisés avec un accès console peuvent exploiter des vulnérabilités locales pour élever leurs privilèges ou accéder à des données sensibles stockées sur le serveur.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeInteractiveLogonRight"
```

AUDIT :

- Valeur attendue : **Administrateurs** uniquement

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Permettre l'ouverture de session locale` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs, Opérateurs de sauvegarde, Utilisateurs

2.1.4 *Autoriser l'ouverture de session par les services Bureau à distance* Critique

MITRE ATT&CK : T1021.001 (Remote Services: Remote Desktop Protocol)

DESCRIPTION :

Ce droit contrôle quels utilisateurs peuvent ouvrir une session interactive via les Services Bureau à distance (RDP). Le CIS recommande de limiter ce droit aux groupes Administrateurs et Utilisateurs du Bureau à distance. L'ajout de groupes supplémentaires élargit la surface d'attaque RDP. Ce paramètre fonctionne en conjonction avec les paramètres de sécurité NLA et le chiffrement RDP.

Impact métier : Un accès RDP trop permissif expose le serveur aux attaques par force brute RDP et à l'exploitation de vulnérabilités du protocole RDP.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeRemoteInteractiveLogonRight"
# Vérifier aussi le groupe local
Get-LocalGroupMember -Group "Utilisateurs du Bureau à distance" -ErrorAction SilentlyContinue
Get-LocalGroupMember -Group "Remote Desktop Users" -ErrorAction SilentlyContinue
```

AUDIT :

- Valeur attendue : **Administrateurs, Utilisateurs du Bureau à distance**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Autoriser l'ouverture de session par les services Bureau à distance` → **Administrateurs, Utilisateurs du Bureau à distance**

VALEUR PAR DÉFAUT :

Administrateurs, Utilisateurs du Bureau à distance

2.1.5 *Sauvegarder les fichiers et les répertoires* Moyen

MITRE ATT&CK : T1003.003 (OS Credential Dumping: NTDS)

DESCRIPTION :

Ce droit permet à un utilisateur de contourner les permissions NTFS pour effectuer des sauvegardes. Un attaquant disposant de ce privilège peut sauvegarder (et donc lire) n'importe quel fichier du système, y compris la base SAM, les fichiers SYSTEM et NTDS.dit. Le CIS recommande de limiter ce droit aux Administrateurs uniquement sur un serveur membre.

Impact métier : Un utilisateur avec ce droit peut extraire des données sensibles protégées par NTFS, incluant les bases de données de mots de passe.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeBackupPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs** uniquement

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Sauvegarder les fichiers et les répertoires` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs, Opérateurs de sauvegarde

2.1.6 *Créer un objet-jeton* Critique

MITRE ATT&CK : T1134.002 (Access Token Manipulation: Create Process with Token)

DESCRIPTION :

Ce droit permet à un processus de créer des jetons d'accès Windows. Un jeton d'accès contient l'identité de sécurité d'un utilisateur et ses privilèges. La possibilité de créer des jetons arbitraires permet une usurpation d'identité complète. Ce droit ne doit être attribué à aucun utilisateur — seul le processus LSASS (Local Security Authority) utilise ce privilège dans le fonctionnement normal.

Impact métier : La création de jetons arbitraires permet une escalade de privilèges complète et l'usurpation de n'importe quelle identité.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeCreateTokenPrivilege"
```

AUDIT :

- Valeur attendue : **Personne (aucun compte)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Créer un objet-jeton` → **(vide)**

VALEUR PAR DÉFAUT :

Personne

2.1.7 *Créer des objets globaux* Moyen

MITRE ATT&CK : T1055 (Process Injection)

DESCRIPTION :

Ce droit détermine si un utilisateur peut créer des objets globaux accessibles à toutes les sessions Terminal Services ou Bureau à distance. Les objets globaux incluent les sections de mémoire partagée, les mutex et les sémaphores. Ce droit doit être limité aux Administrateurs, SERVICE et SERVICE LOCAL pour prévenir l'injection de code malveillant dans les sessions d'autres utilisateurs.

Impact métier : La création d'objets globaux malveillants peut permettre l'interception de données inter-sessions ou l'injection de code dans les processus d'autres utilisateurs.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeCreateGlobalPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs, SERVICE, SERVICE LOCAL, SERVICE RÉSEAU**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Créer des objets globaux` → **Administrateurs, SERVICE, SERVICE LOCAL, SERVICE RÉSEAU**

VALEUR PAR DÉFAUT :

Administrateurs, SERVICE, SERVICE LOCAL, SERVICE RÉSEAU

2.1.8 *Créer des objets partagés permanents* Moyen

MITRE ATT&CK : T1055 (Process Injection)

DESCRIPTION :

Ce droit permet la création d'objets de répertoire dans le gestionnaire d'objets Windows. Ces objets partagés permanents persistent dans le noyau et peuvent être utilisés pour étendre l'espace de noms des objets. Ce droit n'est normalement nécessaire que pour les pilotes en mode noyau et ne doit être attribué à aucun utilisateur.

Impact métier : L'abus de ce droit peut permettre l'injection de code persistant au niveau du noyau.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeCreatePermanentPrivilege"
```

AUDIT :

- Valeur attendue : **Personne (aucun compte)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Créer des objets partagés permanents` → **(vide)**

VALEUR PAR DÉFAUT :

Personne

2.1.9 *Créer des liens symboliques* Moyen

MITRE ATT&CK : T1547 (Boot or Logon Autostart Execution)

DESCRIPTION :

Les liens symboliques NTFS permettent de rediriger transparemment l'accès à un fichier ou répertoire vers un autre emplacement. Un utilisateur malveillant avec ce droit pourrait créer des liens symboliques pour piéger des applications privilégiées et leur faire accéder ou modifier des fichiers non prévus (attaque de type symlink race). Le CIS recommande de limiter ce droit aux Administrateurs et aux comptes Hyper-V si applicable.

Impact métier : Les liens symboliques malveillants peuvent être utilisés pour l'escalade de privilèges en exploitant des applications qui suivent les liens sans vérification.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeCreateSymbolicLinkPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs** (et NT VIRTUAL MACHINE\Virtual Machines si Hyper-V installé)

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Créer des liens symboliques` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs

2.1.10 *Déboguer les programmes* Critique

MITRE ATT&CK : T1003.001 (OS Credential Dumping: LSASS Memory)

DESCRIPTION :

Ce droit permet à un utilisateur d'attacher un débogueur à n'importe quel processus, y compris les processus système comme LSASS. C'est le droit le plus communément exploité par les outils d'extraction de mots de passe comme Mimikatz, qui utilise SeDebugPrivilege pour lire la mémoire du processus LSASS et extraire les identifiants en clair ou hachés. Le CIS recommande de limiter strictement ce droit aux Administrateurs sur un serveur membre, voire de le supprimer entièrement si le débogage n'est pas nécessaire.

Impact métier : Tout utilisateur avec le droit SeDebugPrivilege peut extraire les mots de passe de la mémoire LSASS et compromettre l'ensemble du domaine Active Directory.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeDebugPrivilege"
# Vérifier les utilisateurs connectés ayant ce privilège
whoami /priv | findstr "SeDebugPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs** (idéalement personne si pas de besoin de débogage)

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Déboguer les programmes` → **Administrateurs** (ou vide)

VALEUR PAR DÉFAUT :

Administrateurs

2.1.11 *Refuser l'accès à cet ordinateur depuis le réseau* Critique

MITRE ATT&CK : T1021 (Remote Services)

DESCRIPTION :

Ce paramètre définit les comptes qui ne peuvent PAS accéder au serveur via le réseau, même s'ils disposent du droit « Accéder à cet ordinateur depuis le réseau ». Le CIS recommande d'inclure au minimum le groupe Invités et le compte Administrateur local dans cette liste de refus. Cela empêche l'utilisation du compte administrateur local pour le mouvement latéral via SMB et bloque tout accès réseau via le compte Invité.

Impact métier : Sans ce refus explicite, le compte administrateur local peut être utilisé pour le mouvement latéral Pass-the-Hash entre serveurs.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeDenyNetworkLogonRight"
```

AUDIT :

- Valeur attendue : **Invités, Administrateur local (compte RID 500)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Refuser l'accès à cet ordinateur depuis le réseau` → **Invités, Administrateur local**

VALEUR PAR DÉFAUT :

Invité

2.1.12 *Refuser l'ouverture de session en tant que tâche* Moyen

MITRE ATT&CK : T1053 (Scheduled Task/Job)

DESCRIPTION :

Ce paramètre empêche les comptes spécifiés d'être utilisés pour exécuter des tâches planifiées. Le CIS recommande d'inclure le groupe Invités dans cette liste. Cela empêche la création de tâches planifiées avec le compte Invité, qui pourraient être utilisées pour la persistance ou l'exécution de code malveillant.

Impact métier : L'exécution de tâches planifiées avec des comptes non autorisés peut servir de mécanisme de persistance pour un attaquant.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeDenyBatchLogonRight"
```

AUDIT :

- Valeur attendue : **Invités**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Refuser l'ouverture de session en tant que tâche` → **Invités**

VALEUR PAR DÉFAUT :

Non défini

2.1.13 *Refuser l'ouverture de session en tant que service* — Moyen

MITRE ATT&CK : T1543.003 (Create or Modify System Process: Windows Service)

DESCRIPTION :

Ce paramètre empêche les comptes spécifiés d'être utilisés comme identité pour des services Windows. Le CIS recommande d'inclure le groupe Invités. Cela empêche la création de services malveillants s'exécutant sous le compte Invité, une technique d'escalade de privilèges et de persistance.

Impact métier : Un service s'exécutant sous un compte compromis peut fournir un accès persistant et privilégié au système.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeDenyServiceLogonRight"
```

AUDIT :

- Valeur attendue : **Invités**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Refuser l'ouverture de session en tant que service` → **Invités**

VALEUR PAR DÉFAUT :

Non défini

2.1.14 *Refuser l'ouverture de session locale* — Élevé

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Ce paramètre empêche les comptes spécifiés de se connecter directement au serveur via la console. Le CIS recommande d'inclure le groupe Invités dans cette liste de refus. La connexion locale donne un accès direct au matériel et aux périphériques du serveur, ce qui est un risque si des comptes non autorisés peuvent l'utiliser.

Impact métier : Une connexion locale non autorisée donne un accès physique aux ressources du serveur, permettant potentiellement le vol de données ou la manipulation du système.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeDenyInteractiveLogonRight"
```

AUDIT :

- Valeur attendue : **Invités**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Refuser l'ouverture de session locale` → **Invités**

VALEUR PAR DÉFAUT :

Non défini

2.1.15 *Refuser l'ouverture de session par les services Bureau à distance* — Critique

MITRE ATT&CK : T1021.001 (Remote Services: Remote Desktop Protocol)

DESCRIPTION :

Ce paramètre détermine quels utilisateurs ne peuvent pas ouvrir de session RDP sur le serveur. Le CIS recommande d'inclure au minimum le groupe Invités et le compte Administrateur local (RID 500). Refuser l'accès RDP au compte administrateur local force l'utilisation de comptes nominatifs pour les connexions RDP, améliorant la traçabilité et empêchant l'exploitation du compte administrateur local via RDP.

Impact métier : L'accès RDP avec le compte administrateur local est un vecteur principal de mouvement latéral et ne permet pas l'attribution nominative des actions.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeDenyRemoteInteractiveLogonRight"
```

AUDIT :

- Valeur attendue : **Invités, Administrateur local**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Refuser l'ouverture de session par les services Bureau à distance` → **Invités, Administrateur local**

VALEUR PAR DÉFAUT :

Non défini

2.1.16 *Autoriser l'approbation des ordinateurs et des comptes utilisateurs pour la délégation* — Critique

MITRE ATT&CK : T1134.001 (Access Token Manipulation: Token Impersonation/Theft)

DESCRIPTION :

La délégation Kerberos permet à un service d'usurper l'identité d'un utilisateur pour accéder à d'autres ressources réseau en son nom. Ce droit contrôle qui peut configurer la délégation sur les objets AD. Sur un serveur membre, ce droit ne doit être attribué à personne — la délégation est configurée au niveau du domaine par les administrateurs de domaine. Une délégation non contrôlée (unconstrained delegation) est un risque majeur car elle permet de capturer le TGT de tout utilisateur s'authentifiant sur le serveur.

Impact métier : La délégation non contrôlée permet le vol de tickets Kerberos et l'accès à n'importe quelle ressource du domaine au nom de l'utilisateur compromis.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeEnableDelegationPrivilege"
# Vérifier les objets AD avec délégation non contrainte
Get-ADComputer -Filter {TrustedForDelegation -eq $true} -ErrorAction SilentlyContinue | Select-Object Name
```

AUDIT :

- Valeur attendue : **Personne (aucun compte)** sur un serveur membre

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Autoriser l'approbation des ordinateurs et des comptes utilisateurs pour la délégation` → **(vide)**

VALEUR PAR DÉFAUT :

Administrateurs (à corriger)

2.1.17 *Forcer l'arrêt à partir d'un système distant* — Moyen

MITRE ATT&CK : T1529 (System Shutdown/Reboot)

DESCRIPTION :

Ce droit détermine qui peut arrêter ou redémarrer le serveur à distance. Le CIS recommande de limiter ce droit au groupe Administrateurs uniquement. L'attribution de ce droit à des utilisateurs non autorisés permet un déni de service en arrêtant le serveur à distance.

Impact métier : Un arrêt non autorisé du serveur entraîne une interruption de service et potentiellement une perte de données.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeRemoteShutdownPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Forcer l'arrêt à partir d'un système distant` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs, Opérateurs de serveur

2.1.18 *Générer des audits de sécurité* — Moyen

MITRE ATT&CK : T1562.002 (Impair Defenses: Disable Windows Event Logging)

DESCRIPTION :

Ce droit détermine quels comptes peuvent générer des entrées dans le journal de sécurité. Le CIS recommande de limiter ce droit à SERVICE LOCAL et SERVICE RÉSEAU. Un utilisateur malveillant avec ce droit pourrait inonder le journal de sécurité avec de fausses entrées, masquant ainsi les véritables événements de sécurité ou causant l'écrasement d'événements importants.

Impact métier : La capacité de générer des audits de sécurité arbitraires peut être utilisée pour masquer des activités malveillantes dans un flot de faux événements.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeAuditPrivilege"
```

AUDIT :

- Valeur attendue : **SERVICE LOCAL, SERVICE RÉSEAU**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Générer des audits de sécurité` → **SERVICE LOCAL, SERVICE RÉSEAU**

VALEUR PAR DÉFAUT :

SERVICE LOCAL, SERVICE RÉSEAU

2.1.19 *Emprunter l'identité d'un client après authentification* Élevé

MITRE ATT&CK : T1134 (Access Token Manipulation)

DESCRIPTION :

Ce droit permet à un processus de service d'emprunter l'identité d'un utilisateur authentifié qui s'y connecte. Cette capacité est nécessaire pour les services réseau (IIS, SQL Server) mais doit être strictement contrôlée. Le CIS recommande de limiter ce droit aux Administrateurs, SERVICE LOCAL, SERVICE RÉSEAU et SERVICE.

Impact métier : Un service compromis disposant de ce droit peut usurper l'identité de tout utilisateur qui s'y authentifie, permettant l'accès aux ressources de cet utilisateur.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeImpersonatePrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs, SERVICE LOCAL, SERVICE RÉSEAU, SERVICE**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Emprunter l'identité d'un client après authentification` → **Administrateurs, SERVICE LOCAL, SERVICE RÉSEAU, SERVICE**

VALEUR PAR DÉFAUT :

Administrateurs, SERVICE LOCAL, SERVICE RÉSEAU, SERVICE

2.1.20 *Augmenter la priorité de planification* Moyen

MITRE ATT&CK : T1489 (Service Stop)

DESCRIPTION :

Ce droit permet à un utilisateur d'augmenter la priorité de base d'un processus. Un utilisateur malveillant avec ce droit pourrait augmenter la priorité d'un processus au maximum, causant un déni de service en monopolisant les ressources CPU. Le CIS recommande de limiter ce droit au groupe Administrateurs et à Window Manager\Window Manager Group.

Impact métier : L'abus de la priorité de planification peut causer un déni de service local en rendant le serveur inutilisable.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeIncreaseBasePriorityPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs, Window Manager\Window Manager Group**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Augmenter la priorité de planification` → **Administrateurs, Window Manager\Window Manager Group**

VALEUR PAR DÉFAUT :

Administrateurs, Window Manager\Window Manager Group

2.1.21 *Charger et décharger les pilotes de périphériques* Critique

MITRE ATT&CK : T1068 (Exploitation for Privilege Escalation)

DESCRIPTION :

Ce droit permet à un utilisateur de charger des pilotes de périphériques en mode noyau. Les pilotes mode noyau s'exécutent avec les privilèges les plus élevés du système et peuvent modifier n'importe quelle partie de la mémoire du noyau. Un pilote malveillant peut installer un rootkit, désactiver les protections de sécurité ou extraire des données sensibles. Ce droit doit être strictement limité aux Administrateurs.

Impact métier : Le chargement d'un pilote noyau malveillant permet un contrôle total et indétectable du système.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeLoadDriverPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Charger et décharger les pilotes de périphériques` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs

2.1.22 *Gérer le journal d'audit et de sécurité* Élevé

MITRE ATT&CK : T1070.001 (Indicator Removal: Clear Windows Event Logs)

DESCRIPTION :

Ce droit détermine qui peut configurer l'audit d'accès aux objets et qui peut consulter et effacer le journal de sécurité. Un attaquant avec ce droit peut effacer les traces de son activité dans le journal de sécurité. Le CIS recommande de limiter ce droit au groupe Administrateurs uniquement, tout en s'assurant que les journaux sont également envoyés à un SIEM centralisé pour prévenir la suppression locale.

Impact métier : La capacité d'effacer les journaux de sécurité permet à un attaquant de masquer ses traces, rendant l'investigation forensique impossible.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeSecurityPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Gérer le journal d'audit et de sécurité` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs

2.1.23 *Modifier les valeurs de l'environnement du microprogramme* Moyen

MITRE ATT&CK : T1542 (Pre-OS Boot)

DESCRIPTION :

Ce droit permet la modification des variables d'environnement UEFI/BIOS. Un attaquant avec ce droit pourrait modifier les variables de firmware pour contourner Secure Boot, installer un bootkit ou rendre le système non amorçable. Le CIS recommande de limiter ce droit au groupe Administrateurs.

Impact métier : La modification du firmware peut compromettre l'intégrité du processus de démarrage et rendre les protections de sécurité inefficaces.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeSystemEnvironmentPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Modifier les valeurs de l'environnement du microprogramme` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs

2.1.24 *Effectuer des tâches de maintenance de volume* Moyen

MITRE ATT&CK : T1006 (Direct Volume Access)

DESCRIPTION :

Ce droit permet d'effectuer des opérations de maintenance sur les volumes (défragmentation, vérification de disque, etc.). Un utilisateur avec ce droit peut accéder directement aux données brutes du disque, contournant les permissions NTFS, et potentiellement lire des fichiers supprimés ou des données sensibles. Le CIS recommande de limiter ce droit aux Administrateurs.

Impact métier : L'accès direct au volume permet le contournement des permissions NTFS et l'accès aux données supprimées.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeManageVolumePrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Effectuer des tâches de maintenance de volume` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs

2.1.25 *Restaurer les fichiers et les répertoires* Moyen

MITRE ATT&CK : T1574 (Hijack Execution Flow)

DESCRIPTION :

Ce droit permet de restaurer des fichiers et répertoires en contournant les permissions NTFS, les listes de contrôle d'accès (ACL) et les audits. Un utilisateur avec ce droit peut écraser n'importe quel fichier du système, y compris des exécutables système ou des fichiers de configuration critiques. Le CIS recommande de limiter ce droit aux Administrateurs uniquement.

Impact métier : La restauration non autorisée de fichiers peut permettre le remplacement de binaires système par des versions malveillantes, constituant un vecteur d'escalade de privilèges.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeRestorePrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Restaurer les fichiers et les répertoires` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs, Opérateurs de sauvegarde

2.1.26 *Arrêter le système* Moyen

MITRE ATT&CK : T1529 (System Shutdown/Reboot)

DESCRIPTION :

Ce droit détermine qui peut arrêter le système localement. Le CIS recommande de limiter ce droit au groupe Administrateurs. L'arrêt non autorisé d'un serveur de production constitue un déni de service direct.

Impact métier : Un arrêt non autorisé provoque une interruption de service affectant les utilisateurs et les applications dépendantes.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeShutdownPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Arrêter le système` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs, Opérateurs de sauvegarde

2.1.27 *Prendre possession de fichiers ou d'autres objets* Critique

MITRE ATT&CK : T1222 (File and Directory Permissions Modification)

DESCRIPTION :

Ce droit permet à un utilisateur de prendre possession de n'importe quel objet sécurisable du système (fichiers, dossiers, clés de registre, processus, threads). Après avoir pris possession d'un objet, l'utilisateur peut modifier ses permissions pour s'accorder un accès complet. Ce droit contourne toutes les protections de contrôle d'accès NTFS et ne doit être accordé qu'aux Administrateurs.

Impact métier : L'appropriation d'objets système critiques permet le contournement total des contrôles d'accès et l'accès à toutes les données du système.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeTakeOwnershipPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Prendre possession de fichiers ou d'autres objets` → **Administrateurs**

VALEUR PAR DÉFAUT :

Administrateurs

2.1.28 *Ajuster les quotas de mémoire pour un processus* Moyen

MITRE ATT&CK : T1489 (Service Stop)

DESCRIPTION :

Ce droit permet de modifier la quantité de mémoire disponible pour un processus. Un utilisateur malveillant pourrait utiliser ce droit pour réduire les quotas de mémoire des processus critiques, causant leur arrêt ou un déni de service. Le CIS recommande de limiter ce droit aux Administrateurs, SERVICE LOCAL et SERVICE RÉSEAU.

Impact métier : La manipulation des quotas de mémoire peut causer l'arrêt de services critiques et un déni de service.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeIncreaseQuotaPrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs, SERVICE LOCAL, SERVICE RÉSEAU**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Ajuster les quotas de mémoire pour un processus` → **Administrateurs, SERVICE LOCAL, SERVICE RÉSEAU**

VALEUR PAR DÉFAUT :

Administrateurs, SERVICE LOCAL, SERVICE RÉSEAU

2.1.29 *Modifier l'heure système* Moyen

MITRE ATT&CK : T1070.006 (Indicator Removal: Timestomp)

DESCRIPTION :

Ce droit permet de modifier l'horloge interne du système. La modification de l'heure peut affecter l'authentification Kerberos (qui dépend de la synchronisation horaire), corrompre les horodatages des journaux de sécurité et compromettre les investigations forensiques. Le CIS recommande de limiter ce droit aux Administrateurs et SERVICE LOCAL.

Impact métier : La manipulation de l'heure système compromet la fiabilité des journaux, peut causer des échecs d'authentification Kerberos et rend les investigations forensiques non fiables.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeSystemtimePrivilege"
```

AUDIT :

- Valeur attendue : **Administrateurs, SERVICE LOCAL**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Modifier l'heure système` → **Administrateurs, SERVICE LOCAL**

VALEUR PAR DÉFAUT :

Administrateurs, SERVICE LOCAL

2.1.30 *Remplacer un jeton de niveau processus* Moyen

MITRE ATT&CK : T1134 (Access Token Manipulation)

DESCRIPTION :

Ce droit permet à un processus de remplacer le jeton d'accès par défaut associé à un processus enfant. Ce droit est utilisé par les services qui doivent lancer des processus en tant qu'autres utilisateurs. Le CIS recommande de limiter ce droit à SERVICE LOCAL et SERVICE RÉSEAU.

Impact métier : L'abus de ce droit peut permettre l'exécution de processus sous des identités différentes, facilitant l'escalade de privilèges.

```
secedit /export /cfg C:\ANC-Audit\secpol.cfg /areas USER_RIGHTS
Select-String -Path C:\ANC-Audit\secpol.cfg -Pattern "SeAssignPrimaryTokenPrivilege"
```

AUDIT :

- Valeur attendue : **SERVICE LOCAL, SERVICE RÉSEAU**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Remplacer un jeton de niveau processus` → **SERVICE LOCAL, SERVICE RÉSEAU**

VALEUR PAR DÉFAUT :

SERVICE LOCAL, SERVICE RÉSEAU

2.2 — Options de sécurité (Security Options)

2.2.1 *Audit : Forcer les paramètres de sous-catégorie de stratégie d'audit* Élevé

MITRE ATT&CK : T1562.002 (Impair Defenses: Disable Windows Event Logging)

DESCRIPTION :

Ce paramètre force Windows à utiliser les sous-catégories de stratégie d'audit (Advanced Audit Policy) plutôt que les catégories de base (Basic Audit Policy). Les sous-catégories offrent un contrôle beaucoup plus granulaire sur les événements journalisés. Sans ce paramètre, les stratégies d'audit de base peuvent écraser les stratégies avancées, réduisant la visibilité sur les événements de sécurité critiques.

Impact métier : Sans stratégie d'audit avancée, la détection des intrusions et la conformité réglementaire sont compromises par manque de granularité dans la journalisation.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "SCENoApplyLegacyAuditPolicy"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Audit : Forcer les paramètres de sous-catégorie de stratégie d'audit (Windows Vista ou version ultérieure) à se substituer aux paramètres de catégorie de stratégie d'audit` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "SCENoApplyLegacyAuditPolicy" -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :

Non défini

2.2.2 *Audit : Arrêter le système immédiatement si les audits de sécurité ne peuvent pas être journalisés* Moyen

MITRE ATT&CK : T1562.002 (Impair Defenses: Disable Windows Event Logging)

DESCRIPTION :

Ce paramètre arrête le système lorsque le journal de sécurité est plein et ne peut pas enregistrer de nouveaux événements. Bien que cette mesure semble extrême, elle garantit que les événements de sécurité ne sont jamais perdus silencieusement. Dans la plupart des environnements, ce paramètre est laissé désactivé car un arrêt non planifié est plus disruptif que la perte potentielle d'événements. La recommandation CIS est de le désactiver mais d'assurer que les journaux sont dimensionnés correctement et archivés.

Impact métier : L'activation peut causer des arrêts non planifiés. La désactivation peut entraîner la perte d'événements d'audit critiques.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "CrashOnAuditFail"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\CrashOnAuditFail`
- Valeur attendue : **0 (Désactivé)** — mais assurer la collecte centralisée des logs

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Audit : Arrêter le système immédiatement si les audits de sécurité ne peuvent pas être journalisés` → **Désactivé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "CrashOnAuditFail" -Value 0 -Type DWord
```

VALEUR PAR DÉFAUT :

Désactivé

2.2.3 *Périphériques : Autorisation de formatage et d'éjection des médias amovibles* Moyen

MITRE ATT&CK : T1052 (Exfiltration Over Physical Medium)

DESCRIPTION :

Ce paramètre contrôle qui peut formater et éjecter des médias amovibles NTFS. Le CIS recommande de limiter cette capacité aux Administrateurs et Utilisateurs interactifs. Limiter l'accès aux médias amovibles réduit le risque d'exfiltration de données et d'introduction de malware via des clés USB ou des disques externes.

Impact métier : L'accès non contrôlé aux médias amovibles facilite l'exfiltration de données sensibles et l'introduction de malware.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name "AllocateDASD"
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD`
- Valeur attendue : **0 (Administrateurs)** ou **2 (Administrateurs et Utilisateurs interactifs)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Périphériques : Autorisation de formatage et d'éjection des médias amovibles` → **Administrateurs**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name "AllocateDASD" -Value "0" -Type String
```

VALEUR PAR DÉFAUT :

Non défini

2.2.4 *Périphériques : Empêcher les utilisateurs d'installer des pilotes d'imprimante* — Moyen

MITRE ATT&CK : T1547.012 (Boot or Logon Autostart Execution: Print Processors)

DESCRIPTION :

Ce paramètre empêche les utilisateurs non-administrateurs d'installer des pilotes d'imprimante sur le serveur. Les pilotes d'imprimante s'exécutent en mode noyau et peuvent être exploités pour l'escalade de privilèges (comme l'a démontré la vulnérabilité PrintNightmare - CVE-2021-34527). Le CIS recommande d'activer ce paramètre pour empêcher l'installation non autorisée de pilotes d'imprimante.

Impact métier : L'installation non contrôlée de pilotes d'imprimante est un vecteur d'attaque connu pour l'escalade de privilèges et l'exécution de code en mode noyau.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers" -Name "AddPrinterDriv
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers`
- Valeur attendue : **1 (Activé — seuls les administrateurs peuvent installer)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Périphériques : Empêcher les utilisateurs d'installer des pilotes d'imprimante` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers" -Name "AddPrinterDriv
```

VALEUR PAR DÉFAUT :

Désactivé

2.2.5 *Membre de domaine : Chiffrer ou signer numériquement les données de canal sécurisé (toujours)* — Critique

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Le canal sécurisé (secure channel) est la connexion authentifiée entre un serveur membre et son contrôleur de domaine. Ce paramètre garantit que toutes les communications de canal sécurisé sont chiffrées ou signées numériquement. Sans cette protection, un attaquant en position de man-in-the-middle peut intercepter ou modifier les communications d'authentification entre le serveur et le DC, y compris les changements de mot de passe de compte machine.

Impact métier : L'interception du canal sécurisé permet la modification des politiques de sécurité et le vol d'identifiants d'authentification entre le serveur et le contrôleur de domaine.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "RequireSignOrSeal"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Membre de domaine : Chiffrer ou signer numériquement les données de canal sécurisé (toujours)` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "RequireSignOrSeal" -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :

Activé

2.2.6 *Membre de domaine : Chiffrer numériquement les données de canal sécurisé (si possible)* — Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Ce paramètre active le chiffrement des données de canal sécurisé lorsque le contrôleur de domaine le prend en charge. En combinaison avec le contrôle 2.2.5, ce paramètre assure un niveau maximal de protection des communications avec le DC. Le chiffrement est préféré à la simple signature car il protège la confidentialité en plus de l'intégrité.

Impact métier : Sans chiffrement du canal sécurisé, les données d'authentification transitent en clair sur le réseau interne.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "SealSecureChannel"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Membre de domaine : Chiffrer numériquement les données de canal sécurisé (si possible)` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "SealSecureChannel" -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :

Activé

2.2.7 *Membre de domaine : Signer numériquement les données de canal sécurisé (si possible)* Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Ce paramètre assure que toutes les données de canal sécurisé sont signées numériquement lorsque le DC le prend en charge, protégeant l'intégrité des communications même si le chiffrement n'est pas disponible.

Impact métier : Sans signature, les données de canal sécurisé peuvent être modifiées en transit par un attaquant en position d'interception.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "SignSecureChannel"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Membre de domaine : Signer numériquement les données de canal sécurisé (si possible)` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "SignSecureChannel" -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :

Activé

2.2.8 *Membre de domaine : Désactiver les modifications de mot de passe du compte ordinateur* Élevé

MITRE ATT&CK : T1098 (Account Manipulation)

DESCRIPTION :

Ce paramètre, lorsqu'il est activé, empêche le serveur membre de changer automatiquement son mot de passe de compte machine dans Active Directory. Le CIS recommande de le laisser désactivé (autoriser les changements). Le mot de passe du compte machine est utilisé pour l'authentification du canal sécurisé. Un mot de passe qui ne change jamais est vulnérable si le secret est compromis.

Impact métier : Un mot de passe de compte machine statique peut être compromis et utilisé pour usurper l'identité du serveur dans le domaine.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "DisablePasswordChange"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange`
- Valeur attendue : **0 (Désactivé — autoriser les changements)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Membre de domaine : Désactiver les modifications de mot de passe du compte ordinateur` → **Désactivé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "DisablePasswordChange" -Value 0 -Type D
```

VALEUR PAR DÉFAUT :

Désactivé

2.2.9 *Membre de domaine : Âge maximal du mot de passe du compte ordinateur* Moyen

MITRE ATT&CK : T1098 (Account Manipulation)

DESCRIPTION :

Ce paramètre définit l'âge maximal (en jours) du mot de passe du compte machine avant sa rotation automatique. Le CIS recommande une valeur entre 1 et 30 jours. Par défaut, le mot de passe change tous les 30 jours. Réduire cette valeur renforce la sécurité du canal sécurisé mais peut poser des problèmes si le serveur est isolé du domaine pendant une longue période.

Impact métier : Un mot de passe de compte machine périmé peut être utilisé pour des attaques Silver Ticket.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "MaximumPasswordAge"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge`
- Valeur attendue : **30 jours ou moins**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Membre de domaine : Âge maximal du mot de passe du compte ordinateur` → **30 jours**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "MaximumPasswordAge" -Value 30 -Type DWo
```

VALEUR PAR DÉFAUT :

30 jours

2.2.10 *Membre de domaine : Nécessite une clé de session forte (Windows 2000 ou ultérieur)* Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Ce paramètre exige l'utilisation d'un chiffrement fort (128 bits) pour les données du canal sécurisé. Sans cette exigence, le système peut négocier un chiffrement plus faible (56 ou 40 bits) qui peut être craqué. Dans un environnement Windows Server 2025, tous les DC prennent en charge les clés 128 bits.

Impact métier : L'utilisation de clés de chiffrement faibles pour le canal sécurisé permet le déchiffrement des communications par un attaquant.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "RequireStrongKey"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Membre de domaine : Nécessite une clé de session forte` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" -Name "RequireStrongKey" -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :

Activé

2.2.11 *Ouverture de session interactive : Ne pas afficher le dernier nom d'utilisateur connecté* Élevé

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Ce paramètre empêche l'affichage du nom du dernier utilisateur connecté sur l'écran de connexion Windows. L'affichage du dernier nom d'utilisateur révèle des noms de compte valides à quiconque a accès à l'écran de connexion, facilitant les attaques par force brute ou ingénierie sociale. L'ANSSI recommande systématiquement la désactivation de cette fonctionnalité sur les serveurs.

Impact métier : L'exposition des noms d'utilisateur facilite les attaques ciblées par force brute et pulvérisation de mots de passe.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName`
- Valeur attendue : **1 (Activé — ne pas afficher)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Ouverture de session interactive : Ne pas afficher le dernier nom d'utilisateur connecté` → **Activé**
2. Via registre :

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

VALEUR PAR DÉFAUT :

Désactivé

2.2.12 *Ouverture de session interactive : Ne pas demander la combinaison CTRL+ALT+SUPPR* Moyen

MITRE ATT&CK : T1056.002 (Input Capture: GUI Input Capture)

DESCRIPTION :

La séquence CTRL+ALT+SUPPR (Secure Attention Sequence - SAS) garantit que l'écran de connexion Windows est authentique et non une imitation créée par un malware pour capturer les identifiants. Le CIS recommande de maintenir cette exigence activée (paramètre = Désactivé) pour empêcher les attaques par faux écran de connexion. Sur un serveur, cette protection est importante même si le risque est moindre qu'en environnement poste de travail.

Impact métier : Sans la SAS, un malware peut afficher un faux écran de connexion pour capturer les identifiants administrateur.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD`
- Valeur attendue : **0 (Désactivé — CTRL+ALT+SUPPR requis)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Ouverture de session interactive : Ne pas demander la combinaison CTRL+ALT+SUPPR` → **Désactivé**
2. Via registre :

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

VALEUR PAR DÉFAUT :

Non défini (CTRL+ALT+SUPPR requis par défaut sur les serveurs)

2.2.13 *Ouverture de session interactive : Limite d'inactivité de l'ordinateur* Élevé

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Ce paramètre définit le temps d'inactivité (en secondes) après lequel la session utilisateur est automatiquement verrouillée. Le CIS recommande une valeur de 900 secondes (15 minutes) ou moins. Cette mesure protège contre l'accès non autorisé à une session laissée ouverte par un administrateur. Sur un serveur, les sessions administratives non verrouillées sont un risque critique car elles offrent un accès complet au système.

Impact métier : Une session administrateur non verrouillée et sans surveillance offre un accès complet au système à quiconque peut accéder physiquement ou via RDP au serveur.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\InactivityTimeoutSecs`
- Valeur attendue : **900 secondes ou moins (mais > 0)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Ouverture de session interactive : Limite d'inactivité de l'ordinateur` → **900**
2. Via registre :

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

VALEUR PAR DÉFAUT :

Non défini (pas de verrouillage automatique)

2.2.14 *Ouverture de session interactive : Texte du message pour les utilisateurs* Moyen

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Ce paramètre affiche un message d'avertissement légal avant l'écran de connexion. Ce message est une exigence légale dans de nombreuses juridictions pour pouvoir poursuivre les accès non autorisés. Il informe les utilisateurs que le système est réservé aux personnes autorisées et que les activités sont surveillées. L'ANSSI et le RGPD recommandent l'affichage d'une bannière de connexion.

Impact métier : Sans bannière légale, la poursuite judiciaire des accès non autorisés peut être compromise dans certaines juridictions.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText`
- Valeur attendue : **Texte non vide contenant l'avertissement d'accès réservé**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Ouverture de session interactive : Contenu du message pour les utilisateurs essayant de se connecter`
2. Texte recommandé :

```
AVERTISSEMENT : Ce système est la propriété de [Organisation]. L'accès est strictement réservé aux personnes autorisées. Toute util
```

VALEUR PAR DÉFAUT :

Vide (non configuré)

2.2.15 *Ouverture de session interactive : Titre du message pour les utilisateurs* Moyen

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Ce paramètre définit le titre de la boîte de dialogue de la bannière de connexion. Il complète le texte du message (contrôle 2.2.14) et est nécessaire pour que la bannière s'affiche correctement.

Impact métier : Complémentaire au contrôle 2.2.14 pour la validité légale de la bannière de connexion.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption`
- Valeur attendue : **Texte non vide (ex: "AVERTISSEMENT — ACCÈS RÉSERVÉ")**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Ouverture de session interactive : Titre du message pour les utilisateurs essayant de se connecter` → **"AVERTISSEMENT — ACCÈS RÉSERVÉ"**

VALEUR PAR DÉFAUT :

Vide (non configuré)

2.2.16 *Ouverture de session interactive : Comportement de retrait de carte à puce* — Moyen

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Ce paramètre détermine l'action effectuée lorsqu'une carte à puce est retirée. Le CIS recommande de configurer le verrouillage de la station de travail ou la déconnexion. Si des cartes à puce sont utilisées pour l'authentification sur le serveur, le retrait doit verrouiller la session pour empêcher l'accès non autorisé.

Impact métier : Sans verrouillage automatique au retrait de la carte à puce, une session authentifiée reste ouverte et accessible.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name "ScRemoveOption"
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption`
- Valeur attendue : **1 (Verrouiller la station)** ou **2 (Forcer la fermeture de session)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Ouverture de session interactive : Comportement de retrait de carte à puce` → **Verrouiller la station de travail**

VALEUR PAR DÉFAUT :

Aucune action

2.2.17 *Client réseau Microsoft : Communications signées numériquement (toujours)* — Critique

MITRE ATT&CK : T1557.001 (Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay)

DESCRIPTION :

Ce paramètre exige la signature SMB côté client pour toutes les communications SMB. La signature SMB empêche les attaques de relais SMB (SMB Relay) en garantissant l'authenticité et l'intégrité de chaque paquet SMB. Sans signature SMB obligatoire, un attaquant peut intercepter et relayer les authentifications SMB pour accéder à des ressources protégées (NTLM Relay attack). Windows Server 2025 améliore les performances de la signature SMB grâce à l'accélération matérielle AES.

Impact métier : Sans signature SMB, le serveur est vulnérable aux attaques de relais SMB qui permettent un mouvement latéral et un accès non autorisé aux partages réseau.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" -Name "RequireSecuritySignature"
# Ou via PowerShell natif
Get-SmbClientConfiguration | Select-Object RequireSecuritySignature
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Client réseau Microsoft : Communications signées numériquement (toujours)` → **Activé**
2. Via PowerShell :

```
Set-SmbClientConfiguration -RequireSecuritySignature $true -Force
```

VALEUR PAR DÉFAUT :

Activé (Windows Server 2025 — changement par rapport aux versions précédentes)

2.2.18 *Client réseau Microsoft : Envoyer un mot de passe non chiffré aux serveurs SMB tiers* — Critique

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Ce paramètre, lorsqu'il est activé, autorise le redirecteur SMB à envoyer des mots de passe en clair à des serveurs SMB non-Microsoft qui ne prennent pas en charge le chiffrement des mots de passe. Ce paramètre doit être absolument désactivé pour empêcher la transmission de mots de passe en clair sur le réseau, même vers des serveurs tiers (NAS, appliances, serveurs Linux avec Samba).

Impact métier : L'envoi de mots de passe en clair sur le réseau permet leur interception triviale par sniffing réseau.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" -Name "EnablePlainTextPassword"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword`
- Valeur attendue : **0 (Désactivé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Client réseau Microsoft : Envoyer un mot de passe non chiffré aux serveurs SMB tiers` → **Désactivé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" -Name "EnablePlainTextPassword" -Valu
```

VALEUR PAR DÉFAUT :

Désactivé

2.2.19 *Serveur réseau Microsoft : Communications signées numériquement (toujours)* Critique

MITRE ATT&CK : T1557.001 (Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay)

DESCRIPTION :

Ce paramètre exige la signature SMB côté serveur pour toutes les communications entrantes. La combinaison de la signature SMB obligatoire côté client (2.2.17) ET côté serveur (2.2.19) est nécessaire pour une protection complète contre les attaques de relais SMB. Dans Windows Server 2025, la signature SMB est activée par défaut, ce qui représente un changement de sécurité majeur par rapport aux versions précédentes.

Impact métier : Sans signature SMB côté serveur, les connexions entrantes ne sont pas authentifiées, permettant les attaques de relais et l'usurpation d'identité réseau.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters" -Name "RequireSecuritySignature"
Get-SmbServerConfiguration | Select-Object RequireSecuritySignature
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Serveur réseau Microsoft : Communications signées numériquement (toujours)` → **Activé**
2. Via PowerShell :

```
Set-SmbServerConfiguration -RequireSecuritySignature $true -Force
```

VALEUR PAR DÉFAUT :

Activé (Windows Server 2025)

2.2.20 *Serveur réseau Microsoft : Déconnecter les clients à l'expiration des horaires d'ouverture de session* Moyen

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Ce paramètre déconnecte les sessions SMB des utilisateurs dont les heures de connexion ont expiré. Sans ce paramètre, un utilisateur pourrait maintenir une session SMB active au-delà de ses heures autorisées. Le CIS recommande d'activer ce paramètre pour appliquer les restrictions horaires de connexion.

Impact métier : Le non-respect des heures de connexion autorisées augmente le risque d'utilisation non autorisée en dehors des heures de travail.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters" -Name "EnableForcedLogoff"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogoff`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Serveur réseau Microsoft : Déconnecter les clients à l'expiration des horaires d'ouverture de session` → **Activé**

VALEUR PAR DÉFAUT :

Activé

2.2.21 *Accès réseau : Ne pas autoriser l'énumération anonyme des comptes SAM* Critique

MITRE ATT&CK : T1087.001 (Account Discovery: Local Account)

DESCRIPTION :

Ce paramètre empêche les connexions anonymes d'énumérer les comptes stockés dans la base SAM (Security Account Manager). L'énumération anonyme des comptes fournit à un attaquant une liste de noms d'utilisateurs valides, facilitant les attaques par force brute et pulvérisation de mots de passe. Ce contrôle est fondamental pour limiter la reconnaissance réseau.

Impact métier : L'énumération anonyme des comptes fournit une liste de cibles pour les attaques par force brute et ingénierie sociale.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RestrictAnonymousSAM"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Accès réseau : Ne pas autoriser l'énumération anonyme des comptes SAM` → **Activé**
2. Via registre :

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

VALEUR PAR DÉFAUT :

Activé

2.2.22 *Accès réseau : Ne pas autoriser l'énumération anonyme des comptes et partages SAM* Critique

MITRE ATT&CK : T1135 (Network Share Discovery)

DESCRIPTION :

Ce paramètre étend la protection du contrôle 2.2.21 en empêchant également l'énumération anonyme des partages réseau. Un attaquant qui peut énumérer anonymement les partages réseau peut identifier des cibles pour l'exfiltration de données ou le mouvement latéral. Ce paramètre doit être activé en complément de la restriction d'énumération des comptes SAM.

Impact métier : L'énumération anonyme des partages révèle la structure réseau et les données potentiellement accessibles.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RestrictAnonymous"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Accès réseau : Ne pas autoriser l'énumération anonyme des comptes et partages SAM` → **Activé**
2. Via registre :

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

VALEUR PAR DÉFAUT :

Désactivé

2.2.23 *Accès réseau : Ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'authentification réseau* Élevé

MITRE ATT&CK : T1555 (Credentials from Password Stores)

DESCRIPTION :

Ce paramètre empêche le Gestionnaire d'informations d'identification (Credential Manager) de stocker les mots de passe et identifiants utilisés pour l'authentification de domaine. Les identifiants stockés dans le Credential Manager peuvent être extraits par des outils comme Mimikatz via la commande `dpapi::cred`. L'activation de ce paramètre force la saisie manuelle des identifiants à chaque connexion réseau.

Impact métier : Les identifiants stockés dans le Credential Manager sont extractibles par des outils d'attaque, fournissant des mots de passe en clair.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "DisableDomainCreds"
```

AUDIT :

- Registre : `HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\DisableDomainCreds`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Accès réseau : Ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'authentification réseau` → **Activé**

VALEUR PAR DÉFAUT :

Désactivé

2.2.24 *Accès réseau : Laisser les autorisations Tout le monde s'appliquer aux utilisateurs anonymes* Critique

MITRE ATT&CK : T1087.001 (Account Discovery: Local Account)

DESCRIPTION :

Lorsque ce paramètre est activé, les utilisateurs anonymes reçoivent les mêmes permissions que le groupe « Tout le monde », leur donnant un accès potentiel à toutes les ressources partagées. Le CIS recommande de désactiver ce paramètre pour s'assurer que les connexions anonymes n'héritent pas automatiquement des permissions du groupe Tout le monde.

Impact métier : Les connexions anonymes avec les permissions « Tout le monde » peuvent accéder à des ressources partagées non explicitement protégées.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "EveryoneIncludesAnonymous"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous`
- Valeur attendue : **0 (Désactivé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Accès réseau : Laisser les autorisations Tout le monde s'appliquer aux utilisateurs anonymes` → **Désactivé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "EveryoneIncludesAnonymous" -Value 0 -Type DWord
```

VALEUR PAR DÉFAUT :

Désactivé

2.2.25 *Accès réseau : Restreindre l'accès anonyme aux canaux nommés et aux partages* — Élevé

MITRE ATT&CK : T1021.002 (Remote Services: SMB/Windows Admin Shares)

DESCRIPTION :

Ce paramètre restreint l'accès anonyme aux canaux nommés (named pipes) et aux partages réseau qui sont explicitement listés dans les paramètres correspondants. L'activation de ce paramètre ferme les canaux de communication anonymes qui peuvent être exploités pour la reconnaissance réseau et le mouvement latéral.

Impact métier : L'accès anonyme aux canaux nommés et partages permet la reconnaissance et potentiellement l'accès à des données sensibles.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters" -Name "RestrictNullSessAccess"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Accès réseau : Restreindre l'accès anonyme aux canaux nommés et aux partages` → **Activé**

VALEUR PAR DÉFAUT :

Activé

2.2.26 *Accès réseau : Restreindre les clients autorisés à effectuer des appels distants vers SAM* — Critique

MITRE ATT&CK : T1087.001 (Account Discovery: Local Account)

DESCRIPTION :

Ce paramètre contrôle quels clients peuvent effectuer des appels RPC distants vers le SAM (Security Account Manager). Par défaut dans Windows Server 2025, ce paramètre est configuré pour n'autoriser que les Administrateurs. Ce contrôle est critique pour empêcher l'énumération des comptes à distance, qui est une étape clé dans la chaîne d'attaque.

Impact métier : L'énumération distante des comptes SAM fournit à un attaquant une liste complète de comptes locaux pour les attaques par force brute.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RestrictRemoteSAM" -ErrorAction SilentlyContinue
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RestrictRemoteSAM`
- Valeur attendue : **O:BAG:BAD:(A;;RC;;;BA)** (Seuls les Administrateurs)

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Accès réseau : Restreindre les clients autorisés à effectuer des appels distants vers SAM` → **Administrateurs : Autorisation à distance = Autoriser**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RestrictRemoteSAM" -Value "O:BAG:BAD:(A;;RC;;;BA)" -Type
```

VALEUR PAR DÉFAUT :

O:BAG:BAD:(A;;RC;;;BA) (Windows Server 2025)

2.2.27 *Sécurité réseau : Autoriser le système local à utiliser l'identité de l'ordinateur pour NTLM* — Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Ce paramètre autorise les services utilisant le compte LocalSystem à utiliser l'identité de l'ordinateur (compte machine) lors de l'authentification NTLM plutôt qu'une session nulle. Cela renforce la sécurité des communications réseau des services système en évitant les sessions nulles qui peuvent être interceptées ou relayées.

Impact métier : Les sessions nulles NTLM sont vulnérables aux attaques de relais et d'interception.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "UseMachineId"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\UseMachineId`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Autoriser le système local à utiliser l'identité de l'ordinateur pour NTLM` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "UseMachineId" -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :

Activé

2.2.28 *Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos* Critique

MITRE ATT&CK : T1558 (Steal or Forge Kerberos Tickets)

DESCRIPTION :

Ce paramètre définit les algorithmes de chiffrement que Kerberos peut utiliser. Le CIS recommande d'autoriser uniquement AES128_HMAC_SHA1 et AES256_HMAC_SHA1 (et éventuellement les futurs algorithmes). Les types de chiffrement RC4_HMAC_MD5, DES_CBC_CRC et DES_CBC_MD5 sont vulnérables et doivent être désactivés. RC4 est particulièrement ciblé par les attaques Kerberoasting car les tickets chiffrés en RC4 sont beaucoup plus rapides à cracker.

Impact métier : L'utilisation de chiffrement faible (RC4, DES) pour Kerberos facilite le craquage des tickets de service (Kerberoasting) et des TGT (Golden Ticket).

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters" -Name "SupportedEncryp
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\SupportedEncryptionTypes`
- Valeur attendue : **24 (AES128 + AES256)** ou **2147483640 (Future encryption types + AES128 + AES256)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos` → **AES128_HMAC_SHA1, AES256_HMAC_SHA1, Types de chiffrement futurs**
2. Via registre :

```
New-Item -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters" -Name "SupportedEncryp
```

VALEUR PAR DÉFAUT :

Non défini (tous les types autorisés)

2.2.29 *Sécurité réseau : Ne pas stocker la valeur de hachage de LAN Manager au prochain changement de mot de passe* Critique

MITRE ATT&CK : T1003.004 (OS Credential Dumping: LSA Secrets)

DESCRIPTION :

Le hachage LAN Manager (LM hash) est un format de hachage de mot de passe extrêmement faible, limité à 14 caractères et sans distinction majuscules/minuscules, divisé en deux blocs de 7 caractères chacun. Un hash LM peut être craqué en quelques secondes avec du matériel moderne. Ce paramètre empêche Windows de stocker le hash LM lors du prochain changement de mot de passe. L'activation de ce paramètre est absolument critique pour la sécurité des identifiants.

Impact métier : Les hashs LM stockés peuvent être craqués quasi-instantanément, compromettant tous les mots de passe du système.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "NoLMHash"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\NoLMHash`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Ne pas stocker la valeur de hachage de LAN Manager au prochain changement de mot de passe` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "NoLMHash" -Value 1 -Type DWord
```

VALEUR PAR DÉFAUT :

Activé

2.2.30 *Sécurité réseau : Niveau d'authentification LAN Manager* Critique

MITRE ATT&CK : T1550.002 (Use Alternate Authentication Material: Pass the Hash)

DESCRIPTION :

Ce paramètre détermine le protocole d'authentification réseau utilisé. Le CIS recommande le niveau le plus élevé : « Envoyer uniquement la réponse NTLMv2. Refuser LM et NTLM ». Les protocoles LM et NTLMv1 sont cryptographiquement faibles et vulnérables aux attaques par dictionnaire, table arc-en-ciel et relais. NTLMv2 offre une protection significativement meilleure avec des challenges de 128 bits et un HMAC-MD5.

Impact métier : L'acceptation de LM ou NTLMv1 expose les identifiants à un craquage rapide et aux attaques de relais d'authentification.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\LmCompatibilityLevel`
- Valeur attendue : **5 (Envoyer uniquement NTLMv2, Refuser LM et NTLM)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Niveau d'authentification LAN Manager` → **Envoyer uniquement la réponse NTLMv2. Refuser LM et NTLM**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel" -Value 5 -Type DWord
```

VALEUR PAR DÉFAUT :

3 (Envoyer uniquement NTLMv2)

2.2.31 *Sécurité réseau : Conditions requises pour la signature client LDAP* Critique

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Ce paramètre détermine le niveau de signature LDAP que le client exige lors des communications avec les serveurs LDAP. Le CIS recommande le niveau « Exiger la signature ». Sans signature LDAP, les communications entre le serveur membre et les contrôleurs de domaine peuvent être interceptées et modifiées (LDAP injection, modification de requêtes AD). L'attaque LDAP Relay est un vecteur courant pour l'escalade de privilèges dans Active Directory.

Impact métier : Les communications LDAP non signées permettent l'interception et la modification des requêtes Active Directory, y compris les modifications d'appartenance aux groupes privilégiés.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LDAP" -Name "LDAPClientIntegrity"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\LDAP\LDAPClientIntegrity`
- Valeur attendue : **1 (Négocier la signature)** ou **2 (Exiger la signature)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Conditions requises pour la signature client LDAP` → **Exiger la signature**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LDAP" -Name "LDAPClientIntegrity" -Value 2 -Type DWord
```

VALEUR PAR DÉFAUT :

1 (Négocier la signature)

2.2.32 *Sécurité réseau : Sécurité de session minimale pour les clients NTLM SSP* Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Ce paramètre définit les exigences minimales de sécurité pour les sessions NTLM côté client. Le CIS recommande d'exiger le chiffrement 128 bits et la sécurité de session NTLMv2. Cela empêche la négociation à la baisse vers des algorithmes de chiffrement faibles lors de l'établissement de sessions NTLM.

Impact métier : L'utilisation de sessions NTLM avec un chiffrement faible (56 bits ou 40 bits) permet le déchiffrement des communications par force brute.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" -Name "NtlmMinClientSec"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\NtlmMinClientSec`
- Valeur attendue : **537395200 (Exiger NTLMv2 et chiffrement 128 bits)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Sécurité de session minimale pour les clients basés sur NTLM SSP (y compris RPC sécurisé)` → **Exiger la sécurité de session NTLMv2, Exiger le chiffrement 128 bits**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" -Name "NtlmMinClientSec" -Value 537395200 -Type DWord
```

VALEUR PAR DÉFAUT :

536870912 (128 bits uniquement)

2.2.33 *Sécurité réseau : Sécurité de session minimale pour les serveurs NTLM SSP* Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Pendant symétrique côté serveur du contrôle 2.2.32. Ce paramètre définit les exigences minimales de sécurité pour les sessions NTLM côté serveur. Le CIS recommande les mêmes exigences : chiffrement 128 bits et NTLMv2.

Impact métier : Des exigences de sécurité de session insuffisantes permettent aux clients malveillants de négocier un chiffrement faible.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" -Name "NtlmMinServerSec"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\NtlmMinServerSec`
- Valeur attendue : **537395200 (Exiger NTLMv2 et chiffrement 128 bits)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Sécurité de session minimale pour les serveurs basés sur NTLM SSP` → **Exiger la sécurité de session NTLMv2, Exiger le chiffrement 128 bits**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" -Name "NtlmMinServerSec" -Value 537395200 -Type DWord
```

VALEUR PAR DÉFAUT :

536870912

2.2.34 *Contrôle de compte d'utilisateur : Comportement de l'invite d'élévation pour les administrateurs* Critique

MITRE ATT&CK : T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)

DESCRIPTION :

Ce paramètre contrôle le comportement de l'invite d'élévation UAC pour les administrateurs en mode Admin Approval. Le CIS recommande « Demander le consentement sur le bureau sécurisé » pour les serveurs membres. Le bureau sécurisé empêche les malwares de simuler une fenêtre UAC ou de cliquer automatiquement sur le bouton « Oui ». L'option « Élever sans demander » est à proscrire absolument car elle désactive la protection UAC.

Impact métier : Sans invite d'élévation sur le bureau sécurisé, les malwares peuvent s'auto-élever sans intervention de l'utilisateur.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin`
- Valeur attendue : **2 (Demander le consentement sur le bureau sécurisé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : Comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur` → **Demander le consentement sur le bureau sécurisé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "ConsentPromptBehaviorAdmin" -Value
```

VALEUR PAR DÉFAUT :

5 (Demander le consentement pour les binaires non-Windows)

2.2.35 *Contrôle de compte d'utilisateur : Comportement de l'invite d'élévation pour les utilisateurs standard* Élevé

MITRE ATT&CK : T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)

DESCRIPTION :

Ce paramètre contrôle le comportement de l'invite d'élévation pour les utilisateurs standard. Le CIS recommande « Refuser automatiquement les demandes d'élévation ». Cela empêche les utilisateurs standard de tenter d'exécuter des applications avec des privilèges élevés, forçant l'utilisation d'un compte administrateur explicite pour toute tâche nécessitant des privilèges.

Impact métier : L'autorisation d'élévation pour les utilisateurs standard crée un vecteur d'ingénierie sociale où un utilisateur peut être amené à élever un programme malveillant.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser`
- Valeur attendue : **0 (Refuser automatiquement)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : Comportement de l'invite d'élévation pour les utilisateurs standard` → **Refuser automatiquement les demandes d'élévation**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "ConsentPromptBehaviorUser" -Value 0
```

VALEUR PAR DÉFAUT :

3 (Demander des informations d'identification sur le bureau sécurisé)

2.2.36 *Contrôle de compte d'utilisateur : Détecter les installations d'applications et demander l'élévation* Moyen

MITRE ATT&CK : T1204.002 (User Execution: Malicious File)

DESCRIPTION :

Ce paramètre permet à Windows de détecter automatiquement les programmes d'installation et de demander l'élévation de privilèges. L'activation de ce paramètre sur un serveur garantit qu'aucune installation logicielle ne peut s'effectuer silencieusement sans la validation explicite d'un administrateur.

Impact métier : L'installation silencieuse de logiciels sans élévation UAC peut permettre l'installation de malware ou de logiciels non autorisés.

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

AUDIT :

- Registre : `HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableInstallerDetection`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : Détecter les installations d'applications et demander l'élévation` → **Activé**

VALEUR PAR DÉFAUT :

Activé

2.2.37 *Contrôle de compte d'utilisateur : Exécuter tous les administrateurs en mode d'approbation Administrateur* Critique

MITRE ATT&CK : T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)

DESCRIPTION :

Ce paramètre active le mode Admin Approval pour tous les comptes administrateurs, y compris le compte Administrateur intégré (RID 500). C'est le paramètre principal qui active UAC. Lorsque ce paramètre est désactivé, UAC est complètement désactivé et tous les processus des administrateurs s'exécutent avec des privilèges complets, éliminant la protection contre l'auto-élévation des malwares.

Impact métier : La désactivation d'UAC supprime la dernière ligne de défense contre l'élévation de privilèges par les malwares.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : Exécuter tous les administrateurs en mode d'approbation Administrateur` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value 1 -Type DWord
```

REMÉDIATION :

⚠️ **Un redémarrage est nécessaire après modification.**

VALEUR PAR DÉFAUT :

Activé

2.2.38 *Contrôle de compte d'utilisateur : Passer au bureau sécurisé lors de la demande d'élévation* Élevé

MITRE ATT&CK : T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)

DESCRIPTION :

Le bureau sécurisé est un bureau Windows séparé et isolé où s'affiche l'invite UAC. Aucune autre application ne peut interagir avec le bureau sécurisé, empêchant les malwares de simuler les clics sur l'invite UAC ou de capturer les identifiants saisis. Le CIS recommande d'activer ce paramètre pour garantir que les invites d'élévation sont affichées dans un environnement sécurisé.

Impact métier : Sans le bureau sécurisé, les malwares peuvent interagir programmatiquement avec l'invite UAC pour s'auto-élever.

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

AUDIT :

- Registre : `HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : Passer au bureau sécurisé lors de la demande d'élévation` → **Activé**

VALEUR PAR DÉFAUT :

Activé

2.2.39 *Contrôle de compte d'utilisateur : Virtualiser les échecs d'écriture de fichiers et de registre* Moyen

MITRE ATT&CK : T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)

DESCRIPTION :

Ce paramètre redirige les échecs d'écriture d'applications héritées (qui tentent d'écrire dans des emplacements protégés comme Program Files ou HKLM) vers des emplacements virtualisés par utilisateur. Le CIS recommande d'activer ce paramètre pour maintenir la compatibilité des applications héritées tout en préservant la sécurité du système.

Impact métier : La désactivation peut causer des dysfonctionnements d'applications héritées ou, si désactivée, permettre à des applications d'écrire dans des emplacements protégés.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableVirtualization`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : Virtualiser les échecs d'écriture de fichiers et de registre dans des emplacements définis par utilisateur` → **Activé**

VALEUR PAR DÉFAUT :

Activé

2.2.40 *Contrôle de compte d'utilisateur : Élever uniquement les applications UIAccess installées dans des emplacements sécurisés* Moyen

MITRE ATT&CK : T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)

DESCRIPTION :

Ce paramètre restreint l'utilisation du drapeau UIAccess aux applications installées dans des emplacements sécurisés (\Program Files\, \Windows\system32\). UIAccess permet à une application d'envoyer des entrées à des fenêtres d'applications élevées. Limiter ce droit aux emplacements sécurisés empêche les malwares d'exploiter UIAccess depuis un emplacement non protégé.

Impact métier : Des applications UIAccess malveillantes depuis des emplacements non sécurisés peuvent interagir avec les processus élevés.

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

AUDIT :

- Registre : `HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableSecureUIAPaths`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : Élever uniquement les applications UIAccess installées dans des emplacements sécurisés` → **Activé**

VALEUR PAR DÉFAUT :

Activé

2.2.41 *Cryptographie système : Utiliser des algorithmes conformes FIPS pour le chiffrement, le hachage et la signature* Moyen

MITRE ATT&CK : T1600 (Weaken Encryption)

DESCRIPTION :

Ce paramètre force l'utilisation d'algorithmes cryptographiques conformes à la norme FIPS 140. Lorsqu'il est activé, seuls les algorithmes validés FIPS sont utilisés (AES, SHA-256+, RSA 2048+). Note : l'activation de ce paramètre peut causer des problèmes de compatibilité avec certaines applications qui utilisent des algorithmes non-FIPS. Le CIS ne recommande pas systématiquement son activation mais le préconise pour les environnements à haute sécurité.

Impact métier : L'utilisation d'algorithmes non conformes FIPS peut ne pas satisfaire les exigences réglementaires de certains secteurs (défense, santé, finances).

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy" -Name "Enabled"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled`
- Valeur attendue : **Selon l'exigence de l'environnement**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Cryptographie système : Utiliser des algorithmes conformes FIPS` → **Activé (si requis)**

VALEUR PAR DÉFAUT :

Désactivé

2.2.42 *Arrêt : Permettre l'arrêt du système sans ouvrir de session* Moyen

MITRE ATT&CK : T1529 (System Shutdown/Reboot)

DESCRIPTION :

Ce paramètre contrôle si l'option d'arrêt est disponible sur l'écran de connexion Windows sans nécessiter d'authentification. Le CIS recommande de désactiver ce paramètre sur les serveurs pour empêcher un arrêt non autorisé par quiconque a un accès physique ou RDP au serveur sans disposer d'identifiants valides.

Impact métier : L'arrêt non autorisé d'un serveur de production cause une interruption de service immédiate.

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

AUDIT :

- Registre : `HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon`
- Valeur attendue : **0 (Désactivé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Arrêt : Permettre l'arrêt du système sans ouvrir de session` → **Désactivé**

VALEUR PAR DÉFAUT :

Activé (à corriger)

Section 3 — JOURNALISATION ET AUDIT (Event Log & Audit Policy)

3.1 — Stratégie d'audit avancée (Advanced Audit Policy Configuration)

3.1.1 *Auditer la validation des informations d'identification* — Critique

MITRE ATT&CK : T1110 (Brute Force)

DESCRIPTION :

Ce paramètre d'audit enregistre chaque tentative de validation d'informations d'identification sur le serveur. Pour un serveur membre, cela inclut les authentifications NTLM locales. Les événements générés (4774, 4775, 4776) sont essentiels pour détecter les attaques par force brute, la pulvérisation de mots de passe et les tentatives d'authentification avec des identifiants compromis. L'activation des succès ET des échecs est recommandée.

Impact métier : Sans cet audit, il est impossible de détecter les tentatives d'authentification malveillantes ou les comptes compromis.

```
auditpol /get /subcategory:"Validation des informations d'identification"
# Ou en anglais
auditpol /get /subcategory:"Credential Validation"
```

AUDIT :

- Valeur attendue : **Succès et Échec**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Configuration avancée de la stratégie d'audit > Stratégies d'audit > Ouverture de session de compte > Auditer la validation des informations d'identification` → **Succès et Échec**
2. Via commande :

```
auditpol /set /subcategory:"Credential Validation" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.2 *Auditer le service d'authentification Kerberos* — Élevé

MITRE ATT&CK : T1558 (Steal or Forge Kerberos Tickets)

DESCRIPTION :

Ce paramètre audite les demandes de tickets d'authentification Kerberos (TGT). Sur un serveur membre, les événements Kerberos fournissent des informations sur les authentifications entrantes depuis le domaine. L'audit des échecs permet de détecter les tentatives d'utilisation de tickets invalides ou forgés (Golden Ticket, Silver Ticket).

Impact métier : La détection d'utilisation de tickets Kerberos forgés est impossible sans cet audit.

```
auditpol /get /subcategory:"Kerberos Authentication Service"
```

AUDIT :

- Valeur attendue : **Succès et Échec**

REMÉDIATION :

1. Via GPO : `Configuration avancée de la stratégie d'audit > Ouverture de session de compte > Auditer le service d'authentification Kerberos` → **Succès et Échec**
2. Via commande :

```
auditpol /set /subcategory:"Kerberos Authentication Service" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.3 *Auditer la gestion des comptes d'ordinateur* — Moyen

MITRE ATT&CK : T1136 (Create Account)

DESCRIPTION :

Cet audit enregistre les modifications apportées aux comptes d'ordinateur dans Active Directory (création, suppression, modification). Ces événements sont importants pour détecter l'ajout non autorisé de machines au domaine, qui pourraient être utilisées comme pivots par un attaquant.

Impact métier : L'ajout non autorisé de machines au domaine peut créer des portes dérobées pour le mouvement latéral.

```
auditpol /get /subcategory:"Computer Account Management"
```

AUDIT :

- Valeur attendue : **Succès**

REMÉDIATION :

1. Via GPO : `Configuration avancée de la stratégie d'audit > Gestion du compte > Auditer la gestion des comptes d'ordinateur` → **Succès**
2. Via commande :

```
auditpol /set /subcategory:"Computer Account Management" /success:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.4 *Auditer la gestion des groupes de sécurité* Critique

MITRE ATT&CK : T1098 (Account Manipulation)

DESCRIPTION :

Cet audit enregistre toute modification des groupes de sécurité (ajout/suppression de membres, création/suppression de groupes). Les événements 4728, 4729, 4732, 4733, 4756, 4757 sont essentiels pour détecter l'ajout non autorisé de comptes à des groupes privilégiés (Administrateurs, Opérateurs de sauvegarde, etc.). C'est l'un des audits les plus critiques pour la détection des escalades de privilèges.

Impact métier : L'ajout non détecté d'un compte compromis à un groupe privilégié donne un accès administrateur persistant.

```
auditpol /get /subcategory:"Security Group Management"
```

AUDIT :

- Valeur attendue : **Succès**

REMÉDIATION :

1. Via GPO : `Configuration avancée de la stratégie d'audit > Gestion du compte > Auditer la gestion des groupes de sécurité` → **Succès**
2. Via commande :

```
auditpol /set /subcategory:"Security Group Management" /success:enable
```

VALEUR PAR DÉFAUT :

Succès

3.1.5 *Auditer la gestion des comptes d'utilisateur* Critique

MITRE ATT&CK : T1136.001 (Create Account: Local Account)

DESCRIPTION :

Cet audit enregistre les modifications des comptes utilisateurs : création, suppression, activation, désactivation, modification de mot de passe, changement de droits. Les événements 4720, 4722, 4723, 4724, 4725, 4726, 4738 sont fondamentaux pour la détection de la création de comptes backdoor et de la modification non autorisée de comptes existants.

Impact métier : La création non détectée de comptes backdoor ou la modification de comptes existants permet un accès persistant au système.

```
auditpol /get /subcategory:"User Account Management"
```

AUDIT :

- Valeur attendue : **Succès et Échec**

REMÉDIATION :

1. Via GPO : `Configuration avancée de la stratégie d'audit > Gestion du compte > Auditer la gestion des comptes d'utilisateur` → **Succès et Échec**
2. Via commande :

```
auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :

Succès

3.1.6 *Auditer l'activité DPAPI* Moyen

MITRE ATT&CK : T1555 (Credentials from Password Stores)

DESCRIPTION :

DPAPI (Data Protection API) est utilisé par Windows pour protéger les données sensibles stockées localement (mots de passe dans le Credential Manager, clés Wi-Fi, etc.). L'audit DPAPI enregistre les tentatives d'accès aux données protégées par DPAPI, ce qui peut révéler des tentatives d'extraction d'identifiants par des outils comme Mimikatz (dpapi::cred).

Impact métier : L'extraction non détectée de données DPAPI fournit des mots de passe en clair et des clés de chiffrement.

```
auditpol /get /subcategory:"DPAPI Activity"
```

AUDIT :

- Valeur attendue : **Succès et Échec**

```
auditpol /set /subcategory:"DPAPI Activity" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.7 *Auditer la création de processus* Critique

MITRE ATT&CK : T1059 (Command and Scripting Interpreter)

DESCRIPTION :

L'audit de la création de processus (événement 4688) est l'un des audits les plus importants pour la détection des menaces. Combiné avec l'enregistrement de la ligne de commande (contrôle complémentaire), cet audit permet de tracer chaque exécution de programme sur le système. C'est la base de la détection comportementale : exécution de PowerShell encodé, utilisation de LOLBins (Living Off the Land Binaries), téléchargement de charges utiles, mouvement latéral.

Impact métier : Sans l'audit de création de processus, il est impossible de reconstituer la chronologie d'une attaque ou de détecter l'exécution de code malveillant.

```
auditpol /get /subcategory:"Process Creation"
# Vérifier aussi l'enregistrement de la ligne de commande
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit" -Name "ProcessCreationIncludeCmdLine
```

AUDIT :

- Valeur attendue : **Succès** + ligne de commande activée

REMÉDIATION :

1. Via GPO : `Configuration avancée de la stratégie d'audit > Suivi détaillé > Auditer la création de processus` → **Succès**
2. Activer l'enregistrement de la ligne de commande :

   GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Système > Audit de création de processus > Inclure la ligne de commande dans les événements de création de processus` → **Activé**

   1. Via registre :

```
New-Item -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit" -Name "ProcessCreationIncludeCmdLine
auditpol /set /subcategory:"Process Creation" /success:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.8 *Auditer le verrouillage du compte* Élevé

MITRE ATT&CK : T1110.003 (Brute Force: Password Spraying)

DESCRIPTION :

Cet audit enregistre les verrouillages de comptes (événement 4740). La corrélation des verrouillages de comptes avec les tentatives de connexion échouées permet de détecter les attaques par force brute et pulvérisation de mots de passe en cours. Des verrouillages multiples et simultanés sont un indicateur fort d'attaque.

Impact métier : Les verrouillages de comptes non surveillés masquent des attaques actives par force brute.

```
auditpol /get /subcategory:"Account Lockout"
```

AUDIT :

- Valeur attendue : **Échec**

```
auditpol /set /subcategory:"Account Lockout" /failure:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.9 *Auditer l'appartenance à un groupe* Élevé

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Cet audit enregistre les groupes auxquels appartient un utilisateur lors de sa connexion (événement 4627). Cette information est critique pour le forensique car elle documente les privilèges exacts d'un utilisateur au moment de sa connexion. Si un groupe a été modifié entre deux connexions, cet audit permet de le détecter.

Impact métier : La connaissance exacte des groupes d'un utilisateur au moment de la connexion est essentielle pour l'investigation d'incidents.

```
auditpol /get /subcategory:"Group Membership"
```

AUDIT :

- Valeur attendue : **Succès**

```
auditpol /set /subcategory:"Group Membership" /success:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.10 *Auditer la fermeture de session* Moyen

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

L'audit de fermeture de session (événement 4634, 4647) permet de calculer la durée des sessions utilisateur et de corréler les activités avec des fenêtres temporelles précises. Cette information est importante pour l'investigation forensique et la détection de sessions suspectes.

Impact métier : Sans la corrélation connexion/déconnexion, il est impossible de déterminer la durée des sessions et d'identifier les sessions anormalement longues.

```
auditpol /get /subcategory:"Logoff"
```

AUDIT :

- Valeur attendue : **Succès**

```
auditpol /set /subcategory:"Logoff" /success:enable
```

VALEUR PAR DÉFAUT :

Succès

3.1.11 *Auditer l'ouverture de session* Critique

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

L'audit d'ouverture de session (événements 4624, 4625) est fondamental pour la sécurité. L'événement 4624 enregistre les connexions réussies avec le type de connexion (interactive, réseau, batch, service, RDP). L'événement 4625 enregistre les échecs avec la raison. Ces événements sont la première source d'information pour détecter les accès non autorisés, le mouvement latéral et les attaques par force brute.

Impact métier : Sans audit d'ouverture de session, aucune détection d'accès non autorisé n'est possible.

```
auditpol /get /subcategory:"Logon"
```

AUDIT :

- Valeur attendue : **Succès et Échec**

```
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :

Succès

3.1.12 *Auditer d'autres événements d'ouverture/fermeture de session* Moyen

MITRE ATT&CK : T1563 (Remote Service Session Hijacking)

DESCRIPTION :

Cette sous-catégorie capture des événements d'ouverture de session supplémentaires comme les connexions/déconnexions de sessions Terminal Services, le verrouillage/déverrouillage de stations et la reconnexion réseau. L'événement 4779 (déconnexion RDP) et 4778 (reconnexion RDP) sont particulièrement importants pour suivre les sessions Bureau à distance.

Impact métier : Le suivi des sessions RDP est crucial pour détecter le détournement de sessions.

```
auditpol /get /subcategory:"Other Logon/Logoff Events"
```

AUDIT :

- Valeur attendue : **Succès et Échec**

```
auditpol /set /subcategory:"Other Logon/Logoff Events" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.13 *Auditer l'ouverture de session spéciale* Élevé

MITRE ATT&CK : T1078.002 (Valid Accounts: Domain Accounts)

DESCRIPTION :

L'ouverture de session spéciale (événement 4672) se produit lorsqu'un utilisateur avec des privilèges administratifs se connecte. Cet événement documente exactement quels privilèges « sensibles » sont attribués au jeton de l'utilisateur. La surveillance de cet événement permet de détecter les connexions avec des privilèges élevés et d'identifier les comptes qui se connectent avec des droits inhabituels.

Impact métier : La détection de connexions avec des privilèges élevés inattendus est un indicateur précoce de compromission de comptes.

```
auditpol /get /subcategory:"Special Logon"
```

AUDIT :

- Valeur attendue : **Succès**

```
auditpol /set /subcategory:"Special Logon" /success:enable
```

VALEUR PAR DÉFAUT :

Succès

3.1.14 *Auditer les modifications de la stratégie d'audit* — Critique

MITRE ATT&CK : T1562.002 (Impair Defenses: Disable Windows Event Logging)

DESCRIPTION :

Cet audit (événement 4719) enregistre toute modification de la stratégie d'audit elle-même. C'est un audit « méta » qui protège les autres audits : si un attaquant tente de désactiver la journalisation pour masquer ses activités, cette tentative sera elle-même enregistrée. La surveillance de l'événement 4719 dans un SIEM est un contrôle de sécurité critique.

Impact métier : Un attaquant qui peut modifier silencieusement la stratégie d'audit peut opérer sans laisser de traces.

```
auditpol /get /subcategory:"Audit Policy Change"
```

AUDIT :

- Valeur attendue : **Succès**

```
auditpol /set /subcategory:"Audit Policy Change" /success:enable
```

VALEUR PAR DÉFAUT :

Succès

3.1.15 *Auditer les modifications de la stratégie d'authentification* — Élevé

MITRE ATT&CK : T1556 (Modify Authentication Process)

DESCRIPTION :

Cet audit enregistre les modifications de la stratégie d'authentification (événement 4706, 4707, 4713, 4716, 4717). Cela inclut la modification des relations d'approbation, la politique Kerberos et les mécanismes d'authentification. Un attaquant modifiant la stratégie d'authentification peut créer des portes dérobées persistantes dans le processus d'authentification.

Impact métier : La modification non détectée de la stratégie d'authentification peut créer des accès persistants invisibles.

```
auditpol /get /subcategory:"Authentication Policy Change"
```

AUDIT :

- Valeur attendue : **Succès**

```
auditpol /set /subcategory:"Authentication Policy Change" /success:enable
```

VALEUR PAR DÉFAUT :

Succès

3.1.16 *Auditer l'utilisation de privilèges sensibles* — Critique

MITRE ATT&CK : T1134 (Access Token Manipulation)

DESCRIPTION :

Cet audit enregistre l'utilisation de privilèges sensibles (SeDebugPrivilege, SeTakeOwnershipPrivilege, SeBackupPrivilege, etc.). Les événements 4673, 4674 documentent quand ces privilèges sont activés et utilisés. L'utilisation de SeDebugPrivilege est un indicateur fort d'extraction de mots de passe (Mimikatz). L'utilisation de SeTakeOwnershipPrivilege peut indiquer une tentative d'accès non autorisé.

Impact métier : L'utilisation non surveillée de privilèges sensibles masque les activités d'escalade de privilèges et d'extraction de données.

```
auditpol /get /subcategory:"Sensitive Privilege Use"
```

AUDIT :

- Valeur attendue : **Succès et Échec**

```
auditpol /set /subcategory:"Sensitive Privilege Use" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.17 *Auditer l'intégrité du système et le pilote IPsec* — Élevé

MITRE ATT&CK : T1562 (Impair Defenses)

DESCRIPTION :

L'audit d'intégrité du système enregistre les événements liés à l'intégrité du sous-système de sécurité Windows (événements 4612, 4615, 4616, 4618, 4621, 4622). Ces événements signalent les échecs de validation d'intégrité, les modifications de l'heure système et les anomalies du sous-système d'audit. L'audit du pilote IPsec (événements 4960-4969) est important pour le suivi de la sécurité réseau.

Impact métier : Les atteintes à l'intégrité du système de sécurité Windows signalent une compromission potentielle du noyau ou des mécanismes de protection.

```
auditpol /get /subcategory:"System Integrity"
auditpol /get /subcategory:"IPsec Driver"
```

AUDIT :

- Valeur attendue : **Succès et Échec** pour les deux

```
auditpol /set /subcategory:"System Integrity" /success:enable /failure:enable
auditpol /set /subcategory:"IPsec Driver" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :

Succès, Échec (System Integrity)

3.1.18 *Auditer d'autres événements système* Moyen

MITRE ATT&CK : T1562 (Impair Defenses)

DESCRIPTION :

Cette catégorie audite les événements liés au démarrage et à l'arrêt du pare-feu Windows, au chargement de paquets d'authentification et aux notifications d'enregistrement de processus du sous-système de sécurité. L'événement 5024 (démarrage du pare-feu) et 5025 (arrêt du pare-feu) sont importants pour détecter la désactivation du pare-feu par un attaquant.

Impact métier : La désactivation non détectée du pare-feu expose le serveur à des attaques réseau directes.

```
auditpol /get /subcategory:"Other System Events"
```

AUDIT :

- Valeur attendue : **Succès et Échec**

```
auditpol /set /subcategory:"Other System Events" /success:enable /failure:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.19 *Auditer l'extension du système de sécurité* Élevé

MITRE ATT&CK : T1556 (Modify Authentication Process)

DESCRIPTION :

Cet audit enregistre le chargement de paquets d'authentification, de fournisseurs de sécurité, de paquets de notification et de filtres de sécurité dans le sous-système LSA. L'événement 4610 (chargement de paquet d'authentification) est crucial pour détecter les SSP (Security Support Provider) malveillants qui peuvent capturer les mots de passe en clair, technique utilisée par Mimikatz via misc::memssp.

Impact métier : Le chargement d'un SSP malveillant dans LSA permet la capture de tous les mots de passe en clair.

```
auditpol /get /subcategory:"Security System Extension"
```

AUDIT :

- Valeur attendue : **Succès**

```
auditpol /set /subcategory:"Security System Extension" /success:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.1.20 *Auditer l'accès au système de fichiers et aux objets du registre* Élevé

MITRE ATT&CK : T1083 (File and Directory Discovery)

DESCRIPTION :

L'audit d'accès aux objets du système de fichiers et du registre enregistre les tentatives d'accès aux fichiers, dossiers et clés de registre protégés par des ACL avec des entrées d'audit (SACL). Cet audit est particulièrement important pour surveiller l'accès aux fichiers sensibles (SAM, NTDS.dit, certificats, clés privées) et aux clés de registre critiques (HKLM\SAM, HKLM\SECURITY).

Impact métier : L'accès non surveillé aux fichiers et registres sensibles masque les tentatives d'extraction de données critiques.

```
auditpol /get /subcategory:"File System"
auditpol /get /subcategory:"Registry"
```

AUDIT :

- Valeur attendue : **Échec** au minimum

```
auditpol /set /subcategory:"File System" /failure:enable
auditpol /set /subcategory:"Registry" /failure:enable
```

VALEUR PAR DÉFAUT :

Non configuré

3.2 — Configuration des journaux d'événements

3.2.1 *Taille maximale du journal de sécurité* Critique

MITRE ATT&CK : T1070.001 (Indicator Removal: Clear Windows Event Logs)

DESCRIPTION :

La taille du journal de sécurité détermine le volume d'événements qui peut être conservé avant l'écrasement ou l'arrêt de l'enregistrement. Le CIS recommande un minimum de 196 608 Ko (192 Mo). Pour un serveur avec un audit avancé actif, une taille de 1 Go ou plus est recommandée pour éviter la perte d'événements entre les cycles de collecte SIEM.

Impact métier : Un journal de sécurité sous-dimensionné perd les événements les plus anciens, potentiellement les premières traces d'une compromission.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Security" -Name "MaxSize"
# Ou
Get-WinEvent -ListLog Security | Select-Object MaximumSizeInBytes
# Convertir en Ko
(Get-WinEvent -ListLog Security).MaximumSizeInBytes / 1KB
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security\MaxSize`
- Valeur attendue : **196608 Ko minimum (recommandé : 1048576 Ko = 1 Go)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Service Journal des événements > Sécurité > Taille maximale du fichier journal (Ko)` → **1048576**
2. Via PowerShell :

```
wevtutil sl Security /ms:1073741824
```

VALEUR PAR DÉFAUT :

20480 Ko (20 Mo) — **INSUFFISANT**

3.2.2 *Taille maximale du journal système* Élevé

MITRE ATT&CK : T1070.001 (Indicator Removal: Clear Windows Event Logs)

DESCRIPTION :

Le journal système contient les événements générés par le système d'exploitation (services, pilotes, erreurs matérielles). Le CIS recommande un minimum de 32 768 Ko (32 Mo). Ce journal est important pour diagnostiquer les problèmes système et les modifications de configuration.

Impact métier : La perte d'événements système empêche le diagnostic des problèmes et la corrélation avec les événements de sécurité.

```
(Get-WinEvent -ListLog System).MaximumSizeInBytes / 1KB
```

AUDIT :

- Valeur attendue : **32768 Ko minimum**

```
wevtutil sl System /ms:33554432
```

VALEUR PAR DÉFAUT :

20480 Ko (20 Mo)

3.2.3 *Taille maximale du journal d'application* Moyen

MITRE ATT&CK : T1070.001 (Indicator Removal: Clear Windows Event Logs)

DESCRIPTION :

Le journal d'application contient les événements générés par les applications et les services. Le CIS recommande un minimum de 32 768 Ko. Les événements applicatifs peuvent contenir des informations de sécurité importantes (erreurs d'authentification, exceptions de sécurité, violations de politique).

Impact métier : La perte d'événements applicatifs peut masquer des indicateurs de compromission au niveau des applications.

```
(Get-WinEvent -ListLog Application).MaximumSizeInBytes / 1KB
```

AUDIT :

- Valeur attendue : **32768 Ko minimum**

```
wevtutil sl Application /ms:33554432
```

VALEUR PAR DÉFAUT :

20480 Ko (20 Mo)

3.2.4 *Méthode de rétention du journal de sécurité* Élevé

MITRE ATT&CK : T1070.001 (Indicator Removal: Clear Windows Event Logs)

DESCRIPTION :

Ce paramètre détermine le comportement lorsque le journal de sécurité atteint sa taille maximale. Les options sont : écraser les événements les plus anciens, archiver le journal avant écrasement, ou ne pas écraser (arrêter la journalisation). La meilleure pratique est de configurer l'écrasement des événements avec une rétention suffisante et une collecte SIEM en temps réel pour garantir qu'aucun événement n'est perdu.

Impact métier : L'arrêt de la journalisation ou l'écrasement sans collecte centralisée entraîne la perte d'événements critiques.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\EventLog\Security" -Name "Retention"
Get-WinEvent -ListLog Security | Select-Object LogMode
```

AUDIT :

- Valeur attendue : **Écraser les événements anciens (LogMode = Circular)** avec collecte SIEM active

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Service Journal des événements > Sécurité > Méthode de rétention du journal de sécurité` → **Écraser les événements selon les besoins**
2. Assurer une collecte SIEM en temps réel pour la rétention à long terme

VALEUR PAR DÉFAUT :

Écraser les événements selon les besoins

3.2.5 *Activer le journal PowerShell/Operational* Critique

MITRE ATT&CK : T1059.001 (Command and Scripting Interpreter: PowerShell)

DESCRIPTION :

Le journal Microsoft-Windows-PowerShell/Operational doit être activé et dimensionné correctement pour capturer les événements PowerShell détaillés. Ce journal complète le Script Block Logging (Section 10) en enregistrant les événements de pipeline, les erreurs et les informations de session PowerShell.

Impact métier : PowerShell est le vecteur d'attaque #1 sur Windows. Sans journalisation, les activités malveillantes PowerShell sont invisibles.

```
Get-WinEvent -ListLog "Microsoft-Windows-PowerShell/Operational" | Select-Object IsEnabled, MaximumSizeInBytes, LogMode
```

AUDIT :

- Valeur attendue : **Activé, taille ≥ 100 Mo**

```
wevtutil sl "Microsoft-Windows-PowerShell/Operational" /e:true /ms:104857600
```

VALEUR PAR DÉFAUT :

Activé, 15 Mo

Section 4 — PARE-FEU WINDOWS DEFENDER (Windows Defender Firewall)

4.1 — Profil Domaine

4.1.1 *Pare-feu activé sur le profil Domaine* — Critique

MITRE ATT&CK : T1562.004 (Impair Defenses: Disable or Modify System Firewall)

DESCRIPTION :

Le pare-feu Windows Defender doit être activé sur le profil Domaine, qui s'applique lorsque le serveur est connecté à son domaine Active Directory. La désactivation du pare-feu expose le serveur à toutes les connexions réseau entrantes non sollicitées, y compris les tentatives d'exploitation de vulnérabilités, le mouvement latéral et la propagation de malware. Windows Server 2025 améliore les performances du pare-feu avec WFP (Windows Filtering Platform) optimisé.

Impact métier : Un pare-feu désactivé expose directement tous les services du serveur aux attaques réseau, y compris les exploits distants et la propagation de ransomware.

```
Get-NetFirewallProfile -Name Domain | Select-Object Enabled
netsh advfirewall show domainprofile state
```

AUDIT :

- Valeur attendue : **Activé (True/ON)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows Defender avec fonctions avancées de sécurité > Propriétés > Profil du domaine > État du pare-feu` → **Activé**
2. Via PowerShell :

```
Set-NetFirewallProfile -Name Domain -Enabled True
```

VALEUR PAR DÉFAUT :

Activé

4.1.2 *Action par défaut pour les connexions entrantes — Profil Domaine* — Critique

MITRE ATT&CK : T1190 (Exploit Public-Facing Application)

DESCRIPTION :

L'action par défaut pour les connexions entrantes détermine le comportement du pare-feu lorsqu'aucune règle ne correspond à une connexion entrante. Le CIS recommande de bloquer toutes les connexions entrantes par défaut et de n'autoriser que les connexions explicitement autorisées par des règles. C'est le principe du « deny by default » (refus par défaut), fondamental en sécurité réseau.

Impact métier : Une politique « autoriser par défaut » permet toute connexion entrante non explicitement bloquée, exposant les services non protégés par des règles.

```
Get-NetFirewallProfile -Name Domain | Select-Object DefaultInboundAction
```

AUDIT :

- Valeur attendue : **Block (Bloquer)**

REMÉDIATION :

1. Via GPO : Profil du domaine > Connexions entrantes → **Bloquer**
2. Via PowerShell :

```
Set-NetFirewallProfile -Name Domain -DefaultInboundAction Block
```

VALEUR PAR DÉFAUT :

Block

4.1.3 *Action par défaut pour les connexions sortantes — Profil Domaine* — Moyen

MITRE ATT&CK : T1048 (Exfiltration Over Alternative Protocol)

DESCRIPTION :

L'action par défaut pour les connexions sortantes contrôle les connexions initiées depuis le serveur vers l'extérieur. Le CIS recommande d'autoriser par défaut les connexions sortantes (moins restrictif que l'entrant). Pour un durcissement avancé (ANSSI niveau renforcé), bloquer par défaut les connexions sortantes et n'autoriser que les flux nécessaires (whitelist sortant) offre une protection supérieure contre l'exfiltration et les callbacks C2.

Impact métier : L'absence de filtrage sortant permet l'exfiltration de données et les communications avec des serveurs de commande et contrôle (C2).

```
Get-NetFirewallProfile -Name Domain | Select-Object DefaultOutboundAction
```

AUDIT :

- Valeur attendue : **Allow (Autoriser)** — CIS standard / **Block** — ANSSI renforcé

```
Set-NetFirewallProfile -Name Domain -DefaultOutboundAction Allow
# Pour le mode renforcé ANSSI :
# Set-NetFirewallProfile -Name Domain -DefaultOutboundAction Block
```

VALEUR PAR DÉFAUT :

Allow

4.1.4 *Journalisation du pare-feu — Profil Domaine* Élevé

MITRE ATT&CK : T1562.004 (Impair Defenses: Disable or Modify System Firewall)

DESCRIPTION :

La journalisation du pare-feu enregistre les connexions autorisées et/ou bloquées. Le CIS recommande d'activer la journalisation des paquets abandonnés (bloqués) avec une taille de fichier d'au moins 16 384 Ko. Cette journalisation est essentielle pour détecter les tentatives d'accès bloquées, identifier les attaquants qui scannent les ports et diagnostiquer les problèmes de connectivité.

Impact métier : Sans journalisation du pare-feu, il est impossible de détecter les tentatives de connexion bloquées et les scans de ports.

```
Get-NetFirewallProfile -Name Domain | Select-Object LogBlocked, LogAllowed, LogFileName, LogMaxSizeKilobytes
netsh advfirewall show domainprofile logging
```

AUDIT :

- Valeur attendue : **LogBlocked = True, LogMaxSizeKilobytes ≥ 16384**

```
Set-NetFirewallProfile -Name Domain -LogBlocked True -LogAllowed True -LogMaxSizeKilobytes 16384 -LogFileName "%SystemRoot%\System3
```

VALEUR PAR DÉFAUT :

LogBlocked = False, LogMaxSizeKilobytes = 4096

4.1.5 *Interdire les notifications de fusion de règles locales — Profil Domaine* Moyen

MITRE ATT&CK : T1562.004 (Impair Defenses: Disable or Modify System Firewall)

DESCRIPTION :

Ce paramètre contrôle si les règles de pare-feu locales sont fusionnées avec les règles de GPO. Le CIS recommande de ne pas autoriser la fusion pour empêcher les administrateurs locaux d'ajouter des règles qui contournent la politique de sécurité centralisée. Sans cette restriction, un administrateur local (ou un malware avec des privilèges administrateur) peut créer des règles autorisant du trafic non autorisé.

Impact métier : La fusion de règles locales permet le contournement de la politique de pare-feu centralisée.

```
Get-NetFirewallProfile -Name Domain | Select-Object AllowLocalFirewallRules, AllowLocalIPsecRules
```

AUDIT :

- Valeur attendue : **AllowLocalFirewallRules = False**

```
Set-NetFirewallProfile -Name Domain -AllowLocalFirewallRules False
```

VALEUR PAR DÉFAUT :

True (fusion autorisée)

4.2 — Profil Privé

4.2.1 *Pare-feu activé sur le profil Privé* Critique

MITRE ATT&CK : T1562.004 (Impair Defenses: Disable or Modify System Firewall)

DESCRIPTION :

Le profil Privé s'applique lorsque le serveur est connecté à un réseau identifié comme privé (mais pas un domaine). Ce profil doit être activé pour protéger le serveur dans tous les scénarios de connexion. Un serveur mal configuré pourrait se retrouver sur un profil Privé au lieu du profil Domaine (problème de détection réseau).

Impact métier : Un pare-feu désactivé sur le profil Privé expose le serveur si la détection du domaine échoue.

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

AUDIT :

- Valeur attendue : **Activé (True), DefaultInboundAction = Block**

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

VALEUR PAR DÉFAUT :

Activé

4.2.2 *Configuration complète du profil Privé* Élevé

MITRE ATT&CK : T1562.004 (Impair Defenses: Disable or Modify System Firewall)

DESCRIPTION :

L'ensemble des paramètres du profil Privé doivent être configurés de manière identique au profil Domaine : pare-feu activé, connexions entrantes bloquées par défaut, journalisation activée, et fusion des règles locales interdite. La cohérence entre les profils élimine les failles de configuration.

Impact métier : Une configuration incohérente entre les profils crée des failles exploitables en forçant le serveur sur un profil moins restrictif.

```
Get-NetFirewallProfile -Name Private | Format-List *
```

AUDIT :

- Valeur attendue : **Identique au profil Domaine (voir contrôles 4.1.1 à 4.1.5)**

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

VALEUR PAR DÉFAUT :

Activé avec valeurs par défaut

4.3 — Profil Public

4.3.1 *Pare-feu activé sur le profil Public* Critique

MITRE ATT&CK : T1562.004 (Impair Defenses: Disable or Modify System Firewall)

DESCRIPTION :

Le profil Public est le plus restrictif et s'applique lorsque le serveur est connecté à un réseau non reconnu. Ce profil DOIT être activé et configuré de manière très restrictive. Un serveur mal configuré peut se retrouver sur le profil Public lors d'un changement de réseau ou d'un problème de détection.

Impact métier : Le profil Public est la dernière ligne de défense réseau. Sa désactivation expose le serveur dans les scénarios de réseau non identifié.

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

AUDIT :

- Valeur attendue : **Activé (True), DefaultInboundAction = Block**

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

VALEUR PAR DÉFAUT :

Activé

4.3.2 *Configuration complète du profil Public* Critique

MITRE ATT&CK : T1562.004 (Impair Defenses: Disable or Modify System Firewall)

DESCRIPTION :

Le profil Public doit avoir la configuration la plus restrictive de tous les profils. Les paramètres de journalisation et de fusion de règles doivent être identiques ou plus stricts que le profil Domaine. La journalisation des paquets abandonnés est particulièrement importante sur ce profil.

Impact métier : Le profil Public mal configuré est le vecteur d'attaque le plus dangereux en cas de changement de réseau non détecté.

```
Get-NetFirewallProfile -Name Public | Format-List *
```

AUDIT :

- Valeur attendue : **Activé, Bloquer entrant, Journalisation des blocages, Pas de fusion locale**

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

VALEUR PAR DÉFAUT :

Activé avec valeurs par défaut

4.3.3 *Audit des règles de pare-feu existantes* Élevé

MITRE ATT&CK : T1562.004 (Impair Defenses: Disable or Modify System Firewall)

DESCRIPTION :

Au-delà de la configuration globale, il est essentiel d'auditer les règles de pare-feu individuelles pour s'assurer qu'aucune règle trop permissive n'expose le serveur. Les règles autorisant « Tous les programmes », « Tous les ports » ou « Toutes les adresses IP » doivent être identifiées et justifiées. Les règles désactivées mais présentes doivent également être examinées.

Impact métier : Des règles de pare-feu trop permissives annulent l'efficacité de la politique de pare-feu globale.

```
# Lister toutes les règles entrantes activées
Get-NetFirewallRule -Direction Inbound -Enabled True | Select-Object DisplayName, Profile, Action, Protocol | Format-Table -AutoSiz
# Identifier les règles trop permissives
Get-NetFirewallRule -Direction Inbound -Enabled True | Where-Object { $_.Action -eq "Allow" } | Get-NetFirewallPortFilter | Where-O
# Compter les règles par profil
Get-NetFirewallRule -Enabled True | Group-Object Profile | Select-Object Name, Count
```

AUDIT :

- Valeur attendue : **Aucune règle « Any/Any » non justifiée**

REMÉDIATION :

1. Examiner chaque règle autorisant « Any » sur les ports ou adresses
2. Restreindre les règles aux ports et adresses spécifiques nécessaires
3. Documenter et justifier chaque règle de pare-feu

VALEUR PAR DÉFAUT :

Plusieurs règles par défaut (RDP, partage de fichiers, etc.)

5.0 — SERVICES SYSTÈME (System Services)

5.1.1 *Désactiver le service Spouleur d'impression (Print Spooler)* — Critique

MITRE ATT&CK : T1547.012 (Boot or Logon Autostart Execution: Print Processors)

DESCRIPTION :

Le service Spouleur d'impression (Print Spooler) a été la source de nombreuses vulnérabilités critiques, dont PrintNightmare (CVE-2021-34527, CVE-2021-1675) qui permet l'exécution de code à distance avec des privilèges SYSTEM. Sur un serveur qui n'a pas besoin d'imprimer, ce service doit être désactivé. Même sur Windows Server 2025 avec les correctifs appliqués, la surface d'attaque du spouleur reste significative.

Impact métier : Le service Print Spooler est historiquement l'un des services les plus exploités pour l'exécution de code à distance et l'escalade de privilèges.

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

AUDIT :

- Valeur attendue : **StartType = Disabled, Status = Stopped**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Services système > Spouleur d'impression` → **Désactivé**
2. Via PowerShell :

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

VALEUR PAR DÉFAUT :

Automatique (démarré)

5.1.2 *Désactiver le service Assistance à distance (Remote Assistance)* — Élevé

MITRE ATT&CK : T1021.001 (Remote Services: Remote Desktop Protocol)

DESCRIPTION :

Le service d'Assistance à distance permet à un utilisateur externe de prendre le contrôle du bureau avec le consentement de l'utilisateur local. Sur un serveur de production, ce service n'est pas nécessaire et représente un vecteur d'attaque potentiel via l'ingénierie sociale.

Impact métier : L'assistance à distance peut être exploitée via l'ingénierie sociale pour obtenir un accès distant au serveur.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Remote Assistance" -Name "fAllowToGetHelp"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Remote Assistance\fAllowToGetHelp`
- Valeur attendue : **0 (Désactivé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Système > Assistance à distance > Configurer la demande d'assistance à distance` → **Désactivé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Remote Assistance" -Name "fAllowToGetHelp" -Value 0 -Type DWord
```

VALEUR PAR DÉFAUT :

Désactivé sur Server Core, Activé sur Server avec Expérience utilisateur

5.1.3 *Désactiver le service WinRM (si non utilisé)* — Moyen

MITRE ATT&CK : T1021.006 (Remote Services: Windows Remote Management)

DESCRIPTION :

Le service Windows Remote Management (WinRM) permet l'administration distante via PowerShell Remoting et WS-Management. Si le serveur n'est pas géré via PowerShell Remoting, ce service devrait être désactivé pour réduire la surface d'attaque. Si WinRM est nécessaire, il doit être configuré avec HTTPS (port 5986) et authentification Kerberos uniquement.

Impact métier : WinRM mal configuré (HTTP, authentification basique) expose le serveur à l'interception d'identifiants et à l'exécution de commandes à distance non autorisée.

```
Get-Service -Name "WinRM" | Select-Object Name, Status, StartType
# Si WinRM est actif, vérifier sa configuration
winrm get winrm/config 2>$null
Get-WSManInstance -ResourceURI winrm/config/listener -Enumerate 2>$null | Select-Object Transport, Port, CertificateThumbprint
```

AUDIT :

- Valeur attendue : **Désactivé** ou **HTTPS uniquement avec certificat valide**

```
# Si non nécessaire :
Stop-Service -Name "WinRM" -Force
Set-Service -Name "WinRM" -StartupType Disabled
# Si nécessaire, configurer HTTPS :
winrm quickconfig -transport:https
```

VALEUR PAR DÉFAUT :

Démarrage manuel

5.1.4 *Désactiver le service de découverte SSDP (SSDP Discovery)* Moyen

MITRE ATT&CK : T1046 (Network Service Discovery)

DESCRIPTION :

Le service SSDP (Simple Service Discovery Protocol) est utilisé pour la découverte de périphériques UPnP. Ce service est inutile sur un serveur de production et augmente la surface d'attaque réseau en diffusant la présence du serveur sur le réseau et en acceptant des annonces de découverte potentiellement malveillantes.

Impact métier : Le service SSDP expose le serveur à la découverte réseau non autorisée et aux attaques UPnP.

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

AUDIT :

- Valeur attendue : **StartType = Disabled**

```
Stop-Service -Name "SSDPSRV" -Force -ErrorAction SilentlyContinue
Set-Service -Name "SSDPSRV" -StartupType Disabled
```

VALEUR PAR DÉFAUT :

Manuel

5.1.5 *Désactiver le service Hôte de périphérique UPnP* Moyen

MITRE ATT&CK : T1046 (Network Service Discovery)

DESCRIPTION :

Le service hôte de périphérique UPnP (Universal Plug and Play Device Host) permet l'hébergement de périphériques UPnP. Comme le service SSDP, il est inutile sur un serveur et augmente la surface d'attaque réseau.

Impact métier : UPnP peut être exploité pour ouvrir des ports sur le pare-feu ou rediriger le trafic réseau.

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

AUDIT :

- Valeur attendue : **StartType = Disabled**

```
Stop-Service -Name "upnphost" -Force -ErrorAction SilentlyContinue
Set-Service -Name "upnphost" -StartupType Disabled
```

VALEUR PAR DÉFAUT :

Manuel

5.1.6 *Désactiver le service Xbox et services de jeu* Moyen

MITRE ATT&CK : T1543.003 (Create or Modify System Process: Windows Service)

DESCRIPTION :

Les services Xbox et de jeu (Xbox Accessory Management, Xbox Game Monitoring, Xbox Live Auth Manager, Xbox Live Game Save, Xbox Live Networking) n'ont aucune raison d'être sur un serveur. Leur présence et activation indiquent soit une installation non standard soit une compromission.

Impact métier : Les services non nécessaires augmentent la surface d'attaque et consomment des ressources système.

```
Get-Service -Name "Xbox*" -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
```

AUDIT :

- Valeur attendue : **Désactivé ou inexistant**

```
Get-Service -Name "Xbox*" -ErrorAction SilentlyContinue | Stop-Service -Force -ErrorAction SilentlyContinue
Get-Service -Name "Xbox*" -ErrorAction SilentlyContinue | Set-Service -StartupType Disabled
```

VALEUR PAR DÉFAUT :

Absent sur Server Core, Manuel sur Server avec Expérience utilisateur

5.1.7 *Désactiver Bluetooth Support Service* Moyen

MITRE ATT&CK : T1011 (Exfiltration Over Other Network Medium)

DESCRIPTION :

Le service de support Bluetooth n'a pas sa place sur un serveur de production. Bluetooth est un vecteur d'attaque potentiel pour l'exfiltration de données et l'accès non autorisé à proximité. Ce service doit être désactivé systématiquement sur tous les serveurs.

Impact métier : Bluetooth peut être exploité pour l'exfiltration de données à courte portée et l'accès non autorisé.

```
Get-Service -Name "bthserv" -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
```

AUDIT :

- Valeur attendue : **Désactivé ou inexistant**

```
Stop-Service -Name "bthserv" -Force -ErrorAction SilentlyContinue
Set-Service -Name "bthserv" -StartupType Disabled -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :

Manuel

5.1.8 *Désactiver le service LxssManager (WSL)* Élevé

MITRE ATT&CK : T1059 (Command and Scripting Interpreter)

DESCRIPTION :

Le service LxssManager (Windows Subsystem for Linux) n'a pas sa place sur un serveur de production sauf cas d'usage spécifique documenté. WSL fournit un environnement Linux complet qui peut être utilisé pour exécuter des outils d'attaque Linux, contourner les protections Windows (AppLocker, WDAC) et accéder aux fichiers Windows depuis un contexte Linux.

Impact métier : WSL peut contourner les protections de sécurité Windows et fournir un environnement d'exécution non surveillé par les outils EDR Windows.

```
Get-Service -Name "LxssManager" -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
Get-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux -ErrorAction SilentlyContinue | Select-Object Sta
```

AUDIT :

- Valeur attendue : **Désactivé/inexistant, fonctionnalité non installée**

```
Stop-Service -Name "LxssManager" -Force -ErrorAction SilentlyContinue
Set-Service -Name "LxssManager" -StartupType Disabled -ErrorAction SilentlyContinue
Disable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux -NoRestart
```

VALEUR PAR DÉFAUT :

Non installé

5.1.9 *Désactiver les services IIS inutiles* Élevé

MITRE ATT&CK : T1190 (Exploit Public-Facing Application)

DESCRIPTION :

Si IIS est installé mais pas nécessaire, le service W3SVC (World Wide Web Publishing) et les services associés doivent être désactivés. Si IIS est nécessaire, vérifier les contrôles de la Section 15. Un serveur IIS non utilisé mais actif est une cible facile pour les attaques web.

Impact métier : Un serveur IIS non configuré et non maintenu est une cible facile pour les exploits web.

```
Get-Service -Name "W3SVC","WAS","IISADMIN" -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
Get-WindowsFeature Web-Server -ErrorAction SilentlyContinue | Select-Object Name, Installed
```

AUDIT :

- Valeur attendue : **Désactivé si le rôle IIS n'est pas requis**

```
# Désinstaller le rôle IIS si non nécessaire
Remove-WindowsFeature Web-Server -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :

Non installé (sauf si le rôle a été ajouté)

5.1.10 *Désactiver le service FTP (FTPSVC)* Critique

MITRE ATT&CK : T1048.003 (Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol)

DESCRIPTION :

Le protocole FTP transmet les identifiants et les données en clair sur le réseau. Le service FTP doit être désactivé et remplacé par des alternatives sécurisées (SFTP, FTPS, SCP). Si le service FTP est présent et actif, tous les identifiants transmis sont interceptables par sniffing réseau.

Impact métier : FTP transmet les identifiants en clair, permettant leur interception triviale par sniffing réseau.

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

AUDIT :

- Valeur attendue : **Inexistant ou Désactivé**

```
Stop-Service -Name "FTPSVC" -Force -ErrorAction SilentlyContinue
Set-Service -Name "FTPSVC" -StartupType Disabled -ErrorAction SilentlyContinue
# Désinstaller la fonctionnalité FTP
Remove-WindowsFeature Web-Ftp-Server -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :

Non installé

6.0 — REGISTRE ET PERMISSIONS (Registry & File System)

6.1.1 *Permissions sur la ruche de registre SAM* — Critique

MITRE ATT&CK : T1003.002 (OS Credential Dumping: Security Account Manager)

DESCRIPTION :

La ruche de registre SAM (Security Account Manager) contient les hashs des mots de passe des comptes locaux. Les permissions sur la clé `HKLM\SAM` doivent être strictement limitées au compte SYSTEM. Tout accès non autorisé à cette clé permet l'extraction des hashs de mots de passe locaux sans avoir besoin de droits administrateur élevés.

Impact métier : L'accès en lecture à la ruche SAM permet l'extraction de tous les hashs de mots de passe locaux.

```
# Vérifier les permissions sur HKLM:\SAM
$acl = Get-Acl "HKLM:\SAM"
$acl.Access | Format-Table IdentityReference, FileSystemRights, AccessControlType -AutoSize
# Vérifier le fichier SAM sur disque
icacls C:\Windows\System32\config\SAM
```

AUDIT :

- Valeur attendue : **Accès limité à SYSTEM et Administrateurs en lecture seule**

REMÉDIATION :

1. Restaurer les permissions par défaut via la commande :

```
secedit /configure /db secedit.sdb /cfg "%SystemRoot%\inf\defltbase.inf" /areas REGKEYS /overwrite
```

VALEUR PAR DÉFAUT :

SYSTEM : Contrôle total, Administrateurs : Lecture

6.1.2 *Permissions sur la ruche de registre SECURITY* — Critique

MITRE ATT&CK : T1003.004 (OS Credential Dumping: LSA Secrets)

DESCRIPTION :

La ruche SECURITY contient les secrets LSA (LSA Secrets), les informations de politique de sécurité et le cache d'identifiants de domaine (DCC2). L'accès à cette ruche permet l'extraction de mots de passe de comptes de service, du mot de passe du compte machine et des identifiants mis en cache. Les permissions doivent être limitées strictement à SYSTEM.

Impact métier : L'accès à la ruche SECURITY permet l'extraction de secrets LSA, incluant les mots de passe de comptes de service.

```
$acl = Get-Acl "HKLM:\SECURITY"
$acl.Access | Format-Table IdentityReference, FileSystemRights, AccessControlType -AutoSize
icacls C:\Windows\System32\config\SECURITY
```

AUDIT :

- Valeur attendue : **SYSTEM : Contrôle total uniquement**

```
secedit /configure /db secedit.sdb /cfg "%SystemRoot%\inf\defltbase.inf" /areas REGKEYS /overwrite
```

VALEUR PAR DÉFAUT :

SYSTEM : Contrôle total

6.1.3 *Protection du registre contre l'accès réseau distant* — Élevé

MITRE ATT&CK : T1012 (Query Registry)

DESCRIPTION :

Le service de registre distant (Remote Registry) permet la modification du registre Windows à distance. Ce service doit être désactivé sauf besoin spécifique documenté. Si le service est actif, les clés `winreg\AllowedExactPaths` et `winreg\AllowedPaths` définissent quels chemins de registre sont accessibles à distance.

Impact métier : L'accès distant au registre permet la modification non autorisée de la configuration de sécurité du serveur.

```
Get-Service -Name "RemoteRegistry" | Select-Object Name, Status, StartType
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedExactPaths" -Name "Machine" -ErrorAc
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths" -Name "Machine" -ErrorAction
```

AUDIT :

- Valeur attendue : **Service RemoteRegistry désactivé**

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

VALEUR PAR DÉFAUT :

Manuel (non démarré)

6.1.4 *Permissions sur les fichiers système critiques* — Élevé

MITRE ATT&CK : T1222.001 (File and Directory Permissions Modification: Windows File and Directory Permissions Modification)

DESCRIPTION :

Les permissions sur les répertoires système critiques (\Windows\System32, \Windows\SysWOW64, \Program Files) doivent empêcher la modification par des utilisateurs non-administrateurs. Un attaquant qui peut écrire dans ces répertoires peut remplacer des binaires système (DLL hijacking, binary planting) pour obtenir une exécution de code avec des privilèges élevés.

Impact métier : La modification de fichiers système permet l'injection de code avec les plus hauts privilèges.

```
# Vérifier les permissions sur les répertoires critiques
icacls C:\Windows\System32 | Select-Object -First 10
icacls "C:\Program Files" | Select-Object -First 10
# Rechercher les fichiers avec des permissions non standard
accesschk.exe -w -s -d "Users" C:\Windows\System32 2>$null | Select-Object -First 20
```

AUDIT :

- Valeur attendue : **Utilisateurs : Lecture et exécution uniquement, Administrateurs et SYSTEM : Contrôle total**

REMÉDIATION :

1. Restaurer les permissions par défaut :

```
secedit /configure /db secedit.sdb /cfg "%SystemRoot%\inf\defltbase.inf" /areas FILESTORE /overwrite
```

REMÉDIATION :

1. Utiliser SFC pour vérifier l'intégrité :

```
sfc /scannow
```

VALEUR PAR DÉFAUT :

Permissions Windows par défaut (NTFS)

6.1.5 *Désactiver l'enregistrement du nom NetBIOS* — Élevé

MITRE ATT&CK : T1557.001 (Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning)

DESCRIPTION :

NetBIOS over TCP/IP est un protocole hérité utilisé pour la résolution de noms dans les réseaux pré-AD. NetBIOS est vulnérable aux attaques de poisoning (NBNS Spoofing) où un attaquant répond aux requêtes de résolution de noms pour intercepter le trafic réseau. Sur un serveur Windows Server 2025 dans un domaine AD avec DNS fonctionnel, NetBIOS n'est pas nécessaire.

Impact métier : NetBIOS permet les attaques d'empoisonnement de noms qui redirigent le trafic réseau vers un attaquant.

```
# Vérifier la configuration NetBIOS sur chaque interface
Get-WmiObject Win32_NetworkAdapterConfiguration -Filter "IPEnabled=True" | Select-Object Description, TcpipNetbiosOptions
# 0 = Par défaut, 1 = Activé, 2 = Désactivé
# Ou via registre
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\*" -Name "NetbiosOptions" -ErrorAction
```

AUDIT :

- Valeur attendue : **2 (Désactivé) sur toutes les interfaces**

```
# Désactiver NetBIOS sur toutes les interfaces
Get-WmiObject Win32_NetworkAdapterConfiguration -Filter "IPEnabled=True" | ForEach-Object { $_.SetTcpipNetbios(2) }
```

VALEUR PAR DÉFAUT :

0 (Par défaut — activé par DHCP)

6.1.6 *Désactiver LLMNR (Link-Local Multicast Name Resolution)* — Critique

MITRE ATT&CK : T1557.001 (Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay)

DESCRIPTION :

LLMNR est un protocole de résolution de noms par multicast qui est exploité par les outils d'attaque comme Responder pour capturer des hashs d'authentification NTLM. Lorsqu'un serveur ne peut pas résoudre un nom via DNS, il envoie une requête LLMNR en multicast. Un attaquant sur le même réseau peut répondre et recevoir le hash NTLM du serveur. La désactivation de LLMNR est une mesure de sécurité fondamentale.

Impact métier : LLMNR permet la capture triviale de hashs NTLM par un attaquant sur le réseau local.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name "EnableMulticast" -ErrorAction SilentlyContin
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\EnableMulticast`
- Valeur attendue : **0 (Désactivé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Réseau > Client DNS > Désactiver la résolution de noms multidiffusion` → **Activé**
2. Via registre :

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name "EnableMulticast" -Value 0 -Type DWord
```

VALEUR PAR DÉFAUT :

Activé (1) — **NON CONFORME**

6.1.7 *Désactiver mDNS (Multicast DNS)* Élevé

MITRE ATT&CK : T1557.001 (Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning)

DESCRIPTION :

mDNS (Multicast DNS) est un autre protocole de résolution de noms par multicast, similaire à LLMNR mais utilisant le port 5353/UDP. Windows Server 2025 supporte mDNS, et comme LLMNR, il peut être exploité pour la capture de hashs NTLM. La désactivation de mDNS est recommandée sur les serveurs en environnement d'entreprise.

Impact métier : mDNS présente les mêmes risques que LLMNR pour la capture de hashs NTLM.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters" -Name "EnableMDNS" -ErrorAction SilentlyContin
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\EnableMDNS`
- Valeur attendue : **0 (Désactivé)**

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters" -Name "EnableMDNS" -Value 0 -Type DWord
```

VALEUR PAR DÉFAUT :

Activé (1)

Section 7 — SÉCURITÉ RÉSEAU (Network Security)

7.1 — SMB Signing & Encryption

7.1.1 *Signature SMB requise côté serveur* — Critique

MITRE ATT&CK : T1557.001 (Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay)

DESCRIPTION :

La signature SMB côté serveur garantit que chaque paquet SMB entrant est authentifié et intègre. Dans Windows Server 2025, la signature SMB est activée par défaut — un changement majeur par rapport aux versions précédentes. Cette mesure est la défense principale contre les attaques de relais SMB (NTLM Relay). Les performances sont optimisées grâce à l'accélération matérielle AES-CMAC dans Windows Server 2025.

Impact métier : Sans signature SMB, le serveur est vulnérable aux attaques de relais SMB qui permettent l'exécution de code à distance.

```
Get-SmbServerConfiguration | Select-Object RequireSecuritySignature, EnableSecuritySignature
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters" -Name "RequireSecuritySignature"
```

AUDIT :

- Valeur attendue : **RequireSecuritySignature = True**

```
Set-SmbServerConfiguration -RequireSecuritySignature $true -Force
```

VALEUR PAR DÉFAUT :

True (Windows Server 2025 — nouveau défaut)

7.1.2 *Chiffrement SMB activé* — Élevé

MITRE ATT&CK : T1040 (Network Sniffing)

DESCRIPTION :

Le chiffrement SMB (SMB 3.0+) chiffre l'intégralité du trafic SMB en transit, protégeant la confidentialité des données au-delà de la simple signature. Windows Server 2025 prend en charge le chiffrement AES-256-GCM pour SMB, offrant une protection renforcée. L'activation du chiffrement SMB est recommandée pour les partages contenant des données sensibles.

Impact métier : Sans chiffrement SMB, les données transférées via les partages réseau sont lisibles par sniffing.

```
Get-SmbServerConfiguration | Select-Object EncryptData, RejectUnencryptedAccess
# Vérifier le chiffrement par partage
Get-SmbShare | Select-Object Name, EncryptData
```

AUDIT :

- Valeur attendue : **EncryptData = True** (au minimum sur les partages sensibles)

```
# Chiffrement global
Set-SmbServerConfiguration -EncryptData $true -Force
# Ou par partage
Set-SmbShare -Name "ShareSensible" -EncryptData $true -Force
```

VALEUR PAR DÉFAUT :

False (désactivé par défaut)

7.1.3 *Désactiver SMBv1* — Critique

MITRE ATT&CK : T1210 (Exploitation of Remote Services)

DESCRIPTION :

SMBv1 est un protocole obsolète avec de nombreuses vulnérabilités critiques, notamment EternalBlue (MS17-010) utilisé par WannaCry et NotPetya. Windows Server 2025 ne devrait pas avoir SMBv1 installé, mais il est crucial de vérifier. SMBv1 ne supporte pas la signature obligatoire ni le chiffrement. Sa simple présence représente un risque critique.

Impact métier : SMBv1 est vulnérable à EternalBlue et à de nombreuses autres attaques. Son utilisation est le vecteur #1 de propagation de ransomware.

```
# Vérifier si SMBv1 est installé
Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -ErrorAction SilentlyContinue | Select-Object State
Get-SmbServerConfiguration | Select-Object EnableSMB1Protocol
# Vérifier via fonctionnalité Windows
Get-WindowsFeature FS-SMB1 -ErrorAction SilentlyContinue | Select-Object Name, Installed
```

AUDIT :

- Valeur attendue : **SMBv1 désinstallé et désactivé**

```
# Désactiver SMBv1
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
# Désinstaller la fonctionnalité
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart
Remove-WindowsFeature FS-SMB1 -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :

Non installé (Windows Server 2025)

7.1.4 *SMB over QUIC (Windows Server 2025)* — Moyen

MITRE ATT&CK : T1071 (Application Layer Protocol)

DESCRIPTION :

Windows Server 2025 introduit SMB over QUIC, permettant l'accès aux partages de fichiers via le protocole QUIC (UDP 443) avec chiffrement TLS 1.3 intégré. Si SMB over QUIC n'est pas utilisé, il doit être désactivé. Si utilisé, vérifier que l'authentification par certificat est correctement configurée et que seuls les clients autorisés peuvent se connecter.

Impact métier : SMB over QUIC mal configuré peut exposer les partages de fichiers sur Internet via UDP 443.

```
Get-SmbServerConfiguration | Select-Object EnableSMBQUIC -ErrorAction SilentlyContinue
# Vérifier les certificats SMB over QUIC
Get-SmbServerCertificateMapping -ErrorAction SilentlyContinue
```

AUDIT :

- Valeur attendue : **Désactivé sauf besoin explicite et documenté**

```
Set-SmbServerConfiguration -EnableSMBQUIC $false -Force
```

VALEUR PAR DÉFAUT :

Désactivé

7.2 — LDAP Signing & Channel Binding

7.2.1 *Signature LDAP côté client requise* — Critique

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

La signature LDAP côté client garantit l'intégrité des communications LDAP entre le serveur membre et les contrôleurs de domaine. Sans signature, un attaquant peut intercepter et modifier les requêtes LDAP (modification d'appartenance aux groupes, changement de mots de passe, extraction de données AD). Windows Server 2025 renforce les exigences de signature LDAP par défaut.

Impact métier : Les communications LDAP non signées permettent la modification non autorisée des objets Active Directory.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LDAP" -Name "LDAPClientIntegrity"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\LDAP\LDAPClientIntegrity`
- Valeur attendue : **2 (Exiger la signature)**

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LDAP" -Name "LDAPClientIntegrity" -Value 2 -Type DWord
```

VALEUR PAR DÉFAUT :

1 (Négocier)

7.2.2 *Channel Binding LDAP* — Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Le Channel Binding LDAP (EPA — Extended Protection for Authentication) lie l'authentification LDAP au canal TLS sous-jacent, empêchant les attaques de relais LDAP. Cette protection est complémentaire à la signature LDAP et doit être activée lorsque LDAPS (LDAP over TLS) est utilisé. Windows Server 2025 renforce le support du Channel Binding.

Impact métier : Sans Channel Binding, les communications LDAPS restent vulnérables aux attaques de relais LDAP.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name "LdapEnforceChannelBinding" -ErrorAction Sil
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\LdapEnforceChannelBinding`
- Valeur attendue : **2 (Toujours)** sur les DC, vérifier la compatibilité côté client

```
# Vérifier la compatibilité avant d'activer
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name "LdapEnforceChannelBinding" -Value 2 -Type D
```

VALEUR PAR DÉFAUT :

Non configuré

7.3 — Restrictions NTLM

7.3.1 *Niveau d'authentification LAN Manager* — Critique

MITRE ATT&CK : T1550.002 (Use Alternate Authentication Material: Pass the Hash)

DESCRIPTION :

Ce paramètre (détaillé en 2.2.30) est rappelé ici pour son importance critique dans la sécurité réseau. Le niveau 5 « Envoyer uniquement NTLMv2, refuser LM et NTLM » est le seul niveau acceptable pour un serveur Windows Server 2025. Les niveaux inférieurs permettent l'utilisation de protocoles d'authentification cryptographiquement faibles (LM, NTLMv1) qui sont craquables en temps réel.

Impact métier : L'acceptation de LM ou NTLMv1 permet le craquage instantané des identifiants d'authentification.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel"
```

AUDIT :

- Valeur attendue : **5**

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel" -Value 5 -Type DWord
```

VALEUR PAR DÉFAUT :

3

7.3.2 *Audit et restriction du trafic NTLM* — Élevé

MITRE ATT&CK : T1550.002 (Use Alternate Authentication Material: Pass the Hash)

DESCRIPTION :

Au-delà du niveau d'authentification LAN Manager, Windows Server 2025 offre des contrôles granulaires pour auditer et restreindre le trafic NTLM. L'audit NTLM permet d'identifier les applications et services qui utilisent encore NTLM, préalable nécessaire avant de passer au blocage complet. L'objectif final est de migrer entièrement vers Kerberos.

Impact métier : NTLM est intrinsèquement vulnérable aux attaques de relais. La réduction de l'utilisation de NTLM réduit la surface d'attaque.

```
# Auditer l'utilisation de NTLM
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" -Name "AuditReceivingNTLMTraffic" -ErrorAction SilentlyC
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" -Name "RestrictReceivingNTLMTraffic" -ErrorAction Silent
# Vérifier les événements d'audit NTLM
Get-WinEvent -LogName "Microsoft-Windows-NTLM/Operational" -MaxEvents 10 -ErrorAction SilentlyContinue
```

AUDIT :

- Valeur attendue : **Audit activé (AuditReceivingNTLMTraffic = 2)** dans un premier temps

REMÉDIATION :

1. Phase 1 — Audit :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" -Name "AuditReceivingNTLMTraffic" -Value 2 -Type DWord
```

REMÉDIATION :

1. Phase 2 — Blocage (après analyse) :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" -Name "RestrictReceivingNTLMTraffic" -Value 2 -Type DWor
```

VALEUR PAR DÉFAUT :

Non configuré

7.4 — Configuration TLS/SSL

7.4.1 *Désactiver SSL 2.0 et SSL 3.0* — Critique

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

SSL 2.0 et SSL 3.0 sont des protocoles de chiffrement obsolètes avec des vulnérabilités connues (POODLE, DROWN). Ils doivent être désactivés côté serveur ET côté client. Windows Server 2025 devrait avoir ces protocoles désactivés par défaut, mais la vérification est nécessaire car des applications tierces peuvent les réactiver.

Impact métier : SSL 2.0/3.0 sont cryptographiquement brisés et permettent le déchiffrement des communications réseau.

```
# Vérifier SSL 2.0
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" -Name "Enabled"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client" -Name "Enabled"
# Vérifier SSL 3.0
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" -Name "Enabled"
```

AUDIT :

- Valeur attendue : **Enabled = 0 (Désactivé)** pour SSL 2.0 et SSL 3.0

```
# Désactiver SSL 2.0
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" -Force
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" -Name "Enabled"
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client" -Force
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client" -Name "Enabled"
# Désactiver SSL 3.0
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" -Force
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" -Name "Enabled"
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client" -Force
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client" -Name "Enabled"
```

VALEUR PAR DÉFAUT :

Désactivé dans Windows Server 2025

7.4.2 *Désactiver TLS 1.0 et TLS 1.1*

Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

TLS 1.0 et 1.1 sont considérés comme obsolètes par l'IETF (RFC 8996), l'ANSSI, le NIST et les principaux navigateurs. Bien qu'ils soient plus sûrs que SSL, ils présentent des faiblesses cryptographiques (BEAST, Lucky 13) et ne supportent pas les suites de chiffrement modernes. Seuls TLS 1.2 et TLS 1.3 doivent être autorisés.

Impact métier : L'utilisation de TLS 1.0/1.1 expose les communications à des vulnérabilités cryptographiques connues et enfreint les exigences PCI DSS.

```
# Vérifier TLS 1.0
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Name "Enabled"
# Vérifier TLS 1.1
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Name "Enabled"
```

AUDIT :

- Valeur attendue : **Enabled = 0 pour TLS 1.0 et TLS 1.1**

```
# Désactiver TLS 1.0
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Force
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Name "Enabled"
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Name "Disabled
# Désactiver TLS 1.1
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Force
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Name "Enabled"
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Name "Disabled
```

VALEUR PAR DÉFAUT :

TLS 1.0 et 1.1 désactivés par défaut dans Windows Server 2025

7.4.3 *Activer et configurer TLS 1.3*

Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

TLS 1.3 est la version la plus récente et la plus sécurisée du protocole TLS. Windows Server 2025 offre un support natif complet de TLS 1.3. Ce protocole élimine les suites de chiffrement faibles, réduit la latence (handshake en 1-RTT), et offre une confidentialité persistante (Forward Secrecy) par défaut. L'activation de TLS 1.3 est fortement recommandée.

Impact métier : TLS 1.3 offre la meilleure protection cryptographique disponible et améliore les performances réseau.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Server" -Name "Enabled"
# Vérifier les suites de chiffrement TLS 1.3
Get-TlsCipherSuite | Where-Object { $_.Name -match "TLS_AES" -or $_.Name -match "TLS_CHACHA" } | Select-Object Name
```

AUDIT :

- Valeur attendue : **TLS 1.3 activé avec les suites AES-256-GCM et AES-128-GCM**

```
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Server" -Force
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Server" -Name "Enabled"
```

VALEUR PAR DÉFAUT :

Activé dans Windows Server 2025

7.4.4 *Configuration des suites de chiffrement TLS*

Élevé

MITRE ATT&CK : T1600 (Weaken Encryption)

DESCRIPTION :

La configuration des suites de chiffrement détermine les algorithmes utilisés pour les connexions TLS. Les suites faibles (RC4, DES, 3DES, NULL, export-grade) doivent être désactivées. Seules les suites avec échange de clés ECDHE/DHE (Forward Secrecy), chiffrement AES-GCM et hachage SHA-256+ doivent être autorisées.

Impact métier : Des suites de chiffrement faibles permettent le déchiffrement rétrospectif des communications interceptées.

```
Get-TlsCipherSuite | Select-Object Name, CipherSuite | Format-Table -AutoSize
# Vérifier les suites via registre
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002" -Name "Functions" -ErrorAction S
```

AUDIT :

- Valeur attendue : **Uniquement des suites AES-GCM avec ECDHE/DHE**

```
# Désactiver les suites faibles
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_AES_128_CBC_SHA" -ErrorAction SilentlyContinue
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_AES_256_CBC_SHA" -ErrorAction SilentlyContinue
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_3DES_EDE_CBC_SHA" -ErrorAction SilentlyContinue
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_RC4_128_SHA" -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :

Suites par défaut Windows Server 2025 (excluent déjà RC4 et DES)

7.5 — DNS Security

7.5.1 *Configurer DNS over HTTPS (DoH) ou DNS over TLS (DoT)* Moyen

MITRE ATT&CK : T1071.004 (Application Layer Protocol: DNS)

DESCRIPTION :

Windows Server 2025 supporte nativement DNS over HTTPS (DoH). Le chiffrement des requêtes DNS empêche l'espionnage et la manipulation des résolutions DNS en transit. Cependant, sur un serveur membre en domaine utilisant les DNS AD intégrés, DoH n'est pas toujours applicable. Évaluer selon l'architecture réseau.

Impact métier : Les requêtes DNS en clair révèlent les sites et services accédés par le serveur et sont vulnérables au détournement.

```
Get-DnsClientDohServerAddress -ErrorAction SilentlyContinue
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters" -Name "EnableAutoDoh" -ErrorAction SilentlyCon
```

AUDIT :

- Valeur attendue : **Configuré selon l'architecture réseau**

```
# Ajouter un serveur DoH
Add-DnsClientDohServerAddress -ServerAddress "1.1.1.1" -DohTemplate "https://cloudflare-dns.com/dns-query" -AllowFallbackToUdp $fal
```

VALEUR PAR DÉFAUT :

Non configuré

7.6 — Durcissement des protocoles réseau

7.6.1 *Désactiver IPv6 (si non utilisé)* Moyen

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Si IPv6 n'est pas utilisé dans l'infrastructure réseau, il devrait être désactivé sur le serveur pour réduire la surface d'attaque. IPv6 peut être exploité pour des attaques de type Router Advertisement (RA) Spoofing, DHCPv6 Poisoning et création de tunnels IPv6 clandestins. Note : Microsoft ne recommande pas de désactiver complètement IPv6 car certains composants Windows en dépendent.

Impact métier : IPv6 non géré peut être utilisé comme vecteur d'attaque non surveillé par les outils de sécurité réseau.

```
Get-NetAdapterBinding -ComponentID ms_tcpip6 | Select-Object Name, Enabled
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters" -Name "DisabledComponents" -ErrorAction Silently
```

AUDIT :

- Valeur attendue : **Désactivé si non utilisé (DisabledComponents = 0xFF)**

```
# Désactiver IPv6 (méthode recommandée par Microsoft)
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters" -Name "DisabledComponents" -Value 0xFF -Type DWo
# Ou par interface
Disable-NetAdapterBinding -Name "Ethernet" -ComponentID ms_tcpip6
```

VALEUR PAR DÉFAUT :

Activé

7.6.2 *Configurer IPSec pour les communications sensibles* Moyen

MITRE ATT&CK : T1040 (Network Sniffing)

DESCRIPTION :

IPSec (Internet Protocol Security) fournit le chiffrement et l'authentification au niveau réseau. Pour les communications sensibles (entre serveurs critiques, vers les contrôleurs de domaine), l'utilisation d'IPSec est recommandée comme couche de protection supplémentaire. Windows Server 2025 optimise les performances IPSec avec le support matériel étendu.

Impact métier : Les communications réseau non chiffrées entre serveurs critiques sont vulnérables à l'interception.

```
# Vérifier les règles de sécurité de connexion (IPSec)
Get-NetIPsecRule -ErrorAction SilentlyContinue | Select-Object DisplayName, Enabled, InboundSecurity, OutboundSecurity
# Vérifier les associations de sécurité actives
Get-NetIPsecMainModeSA -ErrorAction SilentlyContinue
```

AUDIT :

- Valeur attendue : **Configuré selon les besoins de l'architecture**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows avec fonctions avancées de sécurité > Règles de sécurité de connexion`
2. Créer des règles IPSec pour les flux critiques

VALEUR PAR DÉFAUT :

Non configuré

7.6.3 *Désactiver WPAD (Web Proxy Auto-Discovery)* Élevé

MITRE ATT&CK : T1557.001 (Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning)

DESCRIPTION :

WPAD permet la découverte automatique de serveurs proxy via DHCP ou DNS. Un attaquant peut exploiter WPAD pour rediriger le trafic HTTP/HTTPS du serveur via un proxy malveillant, permettant l'interception de données et d'identifiants. La désactivation de WPAD est recommandée sur les serveurs avec une configuration proxy manuelle ou sans proxy.

Impact métier : L'exploitation de WPAD permet l'interception de tout le trafic web du serveur via un proxy malveillant.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\WinHttpAutoProxySvc" -ErrorAction SilentlyContinue
Get-Service -Name "WinHttpAutoProxySvc" | Select-Object Name, Status, StartType
```

AUDIT :

- Valeur attendue : **Service désactivé ou proxy configuré manuellement**

```
Set-Service -Name "WinHttpAutoProxySvc" -StartupType Disabled
Stop-Service -Name "WinHttpAutoProxySvc" -Force -ErrorAction SilentlyContinue
```

VALEUR PAR DÉFAUT :

Manuel

8.0 — CREDENTIAL GUARD & PROTECTION DES IDENTIFIANTS

8.1.1 *Activer Credential Guard (Virtualization-Based Security)* — Critique

MITRE ATT&CK : T1003.001 (OS Credential Dumping: LSASS Memory)

DESCRIPTION :

Windows Credential Guard utilise la sécurité basée sur la virtualisation (VBS) pour isoler les secrets NTLM et les tickets Kerberos dans un conteneur sécurisé inaccessible depuis le système d'exploitation, même par un processus avec des privilèges SYSTEM. Cette technologie rend inefficaces les outils d'extraction d'identifiants comme Mimikatz. Windows Server 2025 améliore Credential Guard avec un support étendu et des performances optimisées.

Impact métier : Sans Credential Guard, un attaquant avec des droits admin peut extraire tous les mots de passe et tickets Kerberos de la mémoire LSASS.

```
# Vérifier l'état de VBS et Credential Guard
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard -ErrorAction SilentlyContinue | Select-O
# Vérifier via registre
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LsaCfgFlags" -ErrorAction SilentlyContinue
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" -Name "EnableVirtualizationBasedSecurity" -ErrorActi
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" -Name "LsaCfgFlags" -ErrorAction SilentlyContinue
# Vérifier via msinfo32
systeminfo | findstr /i "Credential Guard"
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\LsaCfgFlags`
- Valeur attendue : **1 (Activé avec verrouillage UEFI)** ou **2 (Activé sans verrouillage UEFI)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Système > Device Guard > Activer la sécurité basée sur la virtualisation` → **Activé**
2. Sécurité basée sur la virtualisation pour Credential Guard → **Activé avec verrouillage UEFI**
3. Via registre :

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" -Name "EnableVirtualizationBasedSecurity" -Value 1 -
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" -Name "LsaCfgFlags" -Value 1 -Type DWord
```

REMÉDIATION :

⚠️ **Prérequis : UEFI Secure Boot, TPM 2.0, Hyper-V activé**

VALEUR PAR DÉFAUT :

Non configuré

8.1.2 *Activer la protection LSA (LSA Protection / RunAsPPL)* — Critique

MITRE ATT&CK : T1003.001 (OS Credential Dumping: LSASS Memory)

DESCRIPTION :

La protection LSA (Local Security Authority) exécute le processus LSASS en tant que processus protégé (PPL — Protected Process Light). Un processus PPL ne peut être accédé en lecture ou écriture que par d'autres processus PPL signés par Microsoft. Cela empêche les outils d'extraction de mots de passe (Mimikatz, procdump) d'accéder à la mémoire LSASS, même avec des droits administrateur. Windows Server 2025 active cette protection par défaut.

Impact métier : Sans protection PPL, le processus LSASS peut être lu par n'importe quel processus avec SeDebugPrivilege, permettant l'extraction de tous les identifiants en mémoire.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RunAsPPL"
# Vérifier le statut actuel du processus LSASS
Get-Process lsass | Select-Object Name, Id, ProcessName
# Via événements
Get-WinEvent -LogName "Microsoft-Windows-Kernel-Boot/Operational" -FilterXPath "*[System[EventID=12]]" -MaxEvents 1 -ErrorAction Si
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL`
- Valeur attendue : **2 (Activé avec verrouillage UEFI)** dans Windows Server 2025

REMÉDIATION :

1. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RunAsPPL" -Value 2 -Type DWord
```

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Système > Autorité de sécurité locale > Configurer LSASS pour qu'il s'exécute en tant que processus protégé` → **Activé avec verrouillage UEFI**

   ⚠️ **Redémarrage nécessaire.**

VALEUR PAR DÉFAUT :

2 (Activé avec verrouillage UEFI) dans Windows Server 2025

8.1.3 *Désactiver WDigest Authentication* Critique

MITRE ATT&CK : T1003.001 (OS Credential Dumping: LSASS Memory)

DESCRIPTION :

WDigest est un protocole d'authentification hérité qui stocke les mots de passe en clair dans la mémoire LSASS pour supporter l'authentification Digest. Même si WDigest n'est pas utilisé, les mots de passe sont stockés en mémoire si le paramètre `UseLogonCredential` est activé. Mimikatz extrait facilement ces mots de passe en clair via la commande `sekurlsa::wdigest`. La désactivation de ce paramètre est absolument critique.

Impact métier : WDigest activé stocke les mots de passe EN CLAIR dans la mémoire LSASS, permettant leur extraction triviale.

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

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential`
- Valeur attendue : **0 (Désactivé)**

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" -Name "UseLogonCredential" -Value 0 -Type
```

VALEUR PAR DÉFAUT :

0 (Désactivé dans Windows Server 2025)

8.1.4 *Désactiver la mise en cache des identifiants de domaine* Élevé

MITRE ATT&CK : T1003.005 (OS Credential Dumping: Cached Domain Credentials)

DESCRIPTION :

Windows met en cache les identifiants de domaine (DCC2 — Domain Cached Credentials version 2) pour permettre la connexion lorsque le contrôleur de domaine n'est pas disponible. Le CIS recommande de limiter le nombre d'identifiants mis en cache à 4 ou moins (voire 0 si le DC est toujours accessible). Les identifiants mis en cache peuvent être extraits et craqués hors ligne.

Impact métier : Les identifiants mis en cache peuvent être extraits et craqués hors ligne, compromettant les comptes de domaine.

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

AUDIT :

- Registre : `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount`
- Valeur attendue : **4 ou moins** (0 si DC toujours accessible)

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Ouverture de session interactive : Nombre de connexions précédentes à mettre en cache` → **4**
2. Via registre :

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

VALEUR PAR DÉFAUT :

10

8.1.5 *Remote Credential Guard pour les connexions RDP* Élevé

MITRE ATT&CK : T1021.001 (Remote Services: Remote Desktop Protocol)

DESCRIPTION :

Remote Credential Guard protège les identifiants lors des connexions RDP en ne transmettant jamais les identifiants au serveur distant. Au lieu de cela, les requêtes d'authentification sont redirigées vers la machine locale. Cela empêche le vol d'identifiants sur un serveur compromis via RDP. Windows Server 2025 étend le support de Remote Credential Guard.

Impact métier : Sans Remote Credential Guard, les identifiants de l'administrateur sont envoyés au serveur distant et peuvent être volés si le serveur est compromis.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "DisableRestrictedAdmin" -ErrorAction SilentlyContinue
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation" -Name "RestrictedRemoteAdministration" -Er
```

AUDIT :

- Valeur attendue : **RestrictedRemoteAdministration = 1 ou 2 (Remote Credential Guard)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Système > Délégation des informations d'identification > Restreindre la délégation des informations d'identification aux serveurs distants` → **Exiger Remote Credential Guard**

VALEUR PAR DÉFAUT :

Non configuré

9.0 — CONTRÔLE DES APPLICATIONS (AppLocker / WDAC)

9.1.1 *Implémenter Windows Defender Application Control (WDAC)* Élevé

MITRE ATT&CK : T1204.002 (User Execution: Malicious File)

DESCRIPTION :

WDAC (Windows Defender Application Control) est le successeur recommandé d'AppLocker pour Windows Server 2025. WDAC fonctionne au niveau du noyau et ne peut pas être contourné par un administrateur local (contrairement à AppLocker). WDAC utilise des politiques de code intégrité (Code Integrity Policies) pour définir quelles applications sont autorisées à s'exécuter. Windows Server 2025 améliore WDAC avec le support des politiques signées et des mises à jour dynamiques.

Impact métier : Sans contrôle d'application, n'importe quel exécutable peut s'exécuter sur le serveur, y compris les ransomwares, les outils d'attaque et les cryptomineurs.

```
# Vérifier si WDAC est actif
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Select-Object CodeIntegrityPolicyEnfor
# Vérifier les politiques CI
Get-CIPolicy -FilePath "$env:windir\System32\CodeIntegrity\SiPolicy.p7b" -ErrorAction SilentlyContinue
citool --list-policies
```

AUDIT :

- Valeur attendue : **WDAC activé en mode enforce ou audit**

REMÉDIATION :

1. Créer une politique de base :

```
# Générer une politique basée sur l'état actuel du système (audit d'abord)
New-CIPolicy -FilePath C:\ANC-Audit\BasePolicy.xml -Level Publisher -Fallback Hash -UserPEs -Audit
# Convertir en binaire
ConvertFrom-CIPolicy -XmlFilePath C:\ANC-Audit\BasePolicy.xml -BinaryFilePath C:\ANC-Audit\SiPolicy.p7b
```

REMÉDIATION :

1. Déployer en mode audit d'abord, puis en mode enforce après validation

VALEUR PAR DÉFAUT :

Non configuré

9.1.2 *Configurer AppLocker (alternative à WDAC)* Élevé

MITRE ATT&CK : T1059 (Command and Scripting Interpreter)

DESCRIPTION :

Si WDAC n'est pas déployé, AppLocker offre une alternative de contrôle d'application basée sur des règles de stratégie de groupe. AppLocker peut contrôler l'exécution des fichiers .exe, .dll, .msi, .msp, les scripts (.ps1, .bat, .cmd, .vbs, .js) et les applications packagées. Contrairement à WDAC, AppLocker fonctionne au niveau utilisateur et peut être contourné par un administrateur local.

Impact métier : AppLocker fournit une couche de protection contre l'exécution de binaires non autorisés, bien que moins robuste que WDAC.

```
# Vérifier si le service AppIDSvc est démarré
Get-Service -Name AppIDSvc | Select-Object Name, Status, StartType
# Vérifier les règles AppLocker
Get-AppLockerPolicy -Effective | Select-Object -ExpandProperty RuleCollections
# Résumé par type
Get-AppLockerPolicy -Effective -Xml | Out-File C:\ANC-Audit\AppLockerPolicy.xml
```

AUDIT :

- Valeur attendue : **AppLocker configuré avec des règles pour Exe, Script, MSI, DLL**

REMÉDIATION :

1. Démarrer le service :

```
Set-Service -Name AppIDSvc -StartupType Automatic
Start-Service -Name AppIDSvc
```

REMÉDIATION :

1. Configurer via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de contrôle d'application > AppLocker`
2. Commencer en mode audit (Audit Only), puis passer en mode enforce

VALEUR PAR DÉFAUT :

Non configuré

9.1.3 *Bloquer l'exécution de scripts non signés* Élevé

MITRE ATT&CK : T1059.001 (Command and Scripting Interpreter: PowerShell)

DESCRIPTION :

Les règles AppLocker ou WDAC doivent bloquer l'exécution de scripts non signés dans les répertoires accessibles aux utilisateurs (profils utilisateurs, répertoires temporaires). Les attaquants déposent couramment des scripts malveillants dans ces emplacements. La restriction de l'exécution de scripts aux répertoires système protégés réduit significativement la surface d'attaque.

Impact métier : L'exécution non contrôlée de scripts est le vecteur principal de déploiement de malware et d'outils d'attaque.

```
# Vérifier la politique d'exécution PowerShell
Get-ExecutionPolicy -List
# Vérifier les règles AppLocker pour les scripts
Get-AppLockerPolicy -Effective | Select-Object -ExpandProperty RuleCollections | Where-Object { $_.RuleCollectionType -eq "Script"
```

AUDIT :

- Valeur attendue : **Exécution restreinte aux scripts signés ou depuis des répertoires approuvés**

REMÉDIATION :

1. Configurer la politique d'exécution PowerShell :

```
Set-ExecutionPolicy AllSigned -Scope LocalMachine
```

REMÉDIATION :

1. Créer des règles AppLocker de script :
2. Autoriser les scripts depuis \Windows\ et \Program Files\
3. Bloquer les scripts depuis les profils utilisateurs et les répertoires temporaires

VALEUR PAR DÉFAUT :

Non configuré (Exécution PowerShell = Restricted)

9.1.4 *Bloquer les LOLBins (Living Off the Land Binaries)* Élevé

MITRE ATT&CK : T1218 (System Binary Proxy Execution)

DESCRIPTION :

Les LOLBins (Living Off the Land Binaries) sont des binaires Windows légitimes utilisés par les attaquants pour exécuter du code malveillant tout en contournant les solutions de sécurité. Les LOLBins courants incluent : mshta.exe, regsvr32.exe, certutil.exe, bitsadmin.exe, msiexec.exe, wscript.exe, cscript.exe, rundll32.exe. Ces binaires doivent être bloqués ou surveillés via WDAC ou AppLocker.

Impact métier : Les LOLBins permettent l'exécution de code malveillant via des binaires signés par Microsoft, contournant les listes blanches basiques.

```
# Vérifier les règles de blocage des LOLBins dans AppLocker
Get-AppLockerPolicy -Effective | Select-Object -ExpandProperty RuleCollections | Where-Object { $_.RuleCollectionType -eq "Exe" }
# Vérifier l'utilisation récente des LOLBins
Get-WinEvent -LogName "Microsoft-Windows-AppLocker/EXE and DLL" -MaxEvents 50 -ErrorAction SilentlyContinue | Where-Object { $_.Mes
```

AUDIT :

- Valeur attendue : **LOLBins non nécessaires bloqués ou en mode audit**

REMÉDIATION :

1. Via AppLocker : Créer des règles de refus pour les LOLBins non nécessaires
2. Via WDAC : Ajouter des règles de blocage dans la politique CI
3. Références : https://lolbas-project.github.io/

VALEUR PAR DÉFAUT :

Non configuré

10.0 — POWERSHELL ET SCRIPTING

10.1.1 *Activer le Script Block Logging PowerShell* — Critique

MITRE ATT&CK : T1059.001 (Command and Scripting Interpreter: PowerShell)

DESCRIPTION :

Le Script Block Logging enregistre le contenu complet de chaque bloc de script PowerShell exécuté (événement 4104). C'est la mesure de détection la plus importante pour PowerShell car elle capture le code déobfusqué final, même si l'attaquant utilise l'encodage Base64, le chiffrement ou l'obfuscation. Le Script Block Logging capture l'intent final du code, rendant inefficaces les techniques d'évasion basées sur l'obfuscation.

Impact métier : Sans Script Block Logging, l'exécution de scripts PowerShell malveillants est invisible pour les équipes de sécurité et les outils SIEM.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Name "EnableScriptBlockLogging" -
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Name "EnableScriptBlockInvocation
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\EnableScriptBlockLogging`
- Valeur attendue : **1 (Activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows PowerShell > Activer la journalisation de blocs de scripts PowerShell` → **Activé**
2. Via registre :

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Name "EnableScriptBlockLogging" -
```

VALEUR PAR DÉFAUT :

Non configuré

10.1.2 *Activer le Module Logging PowerShell* — Élevé

MITRE ATT&CK : T1059.001 (Command and Scripting Interpreter: PowerShell)

DESCRIPTION :

Le Module Logging enregistre l'exécution de chaque commande PowerShell avec ses paramètres (événement 4103). Complémentaire au Script Block Logging, il fournit les informations d'entrée/sortie de chaque commande (pipeline). Pour une couverture maximale, activer le logging pour tous les modules (*).

Impact métier : Le Module Logging fournit un historique détaillé de chaque commande PowerShell exécutée, essentiel pour l'investigation forensique.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging" -Name "EnableModuleLogging" -ErrorActio
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames" -Name "*" -ErrorAction Sile
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\EnableModuleLogging`
- Valeur attendue : **1 (Activé), ModuleNames = * (tous les modules)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows PowerShell > Activer la journalisation des modules` → **Activé**, Modules = *
2. Via registre :

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging" -Name "EnableModuleLogging" -Value 1 -T
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames" -Name "*" -Value "*" -Type
```

VALEUR PAR DÉFAUT :

Non configuré

10.1.3 *Activer la transcription PowerShell* Élevé

MITRE ATT&CK : T1059.001 (Command and Scripting Interpreter: PowerShell)

DESCRIPTION :

La transcription PowerShell enregistre toutes les entrées et sorties de chaque session PowerShell dans des fichiers texte. C'est la méthode la plus complète pour capturer l'activité PowerShell, incluant les commandes interactives qui ne sont pas capturées par le Script Block Logging. Les fichiers de transcription doivent être stockés dans un répertoire protégé et collectés par le SIEM.

Impact métier : La transcription fournit l'enregistrement le plus complet de l'activité PowerShell, crucial pour l'investigation forensique.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" -Name "EnableTranscripting" -ErrorActio
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" -Name "OutputDirectory" -ErrorAction Si
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription\EnableTranscripting`
- Valeur attendue : **1 (Activé), OutputDirectory défini**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows PowerShell > Activer la transcription PowerShell` → **Activé**
2. Répertoire de sortie : `C:\PSTranscripts` (ou partage réseau sécurisé)
3. Inclure les en-têtes d'appel : **Activé**
4. Via registre :

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" -Name "EnableTranscripting" -Value 1 -T
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" -Name "OutputDirectory" -Value "C:\PSTr
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" -Name "EnableInvocationHeader" -Value 1
```

VALEUR PAR DÉFAUT :

Non configuré

10.1.4 *Configurer le mode de langage contraint (Constrained Language Mode)* Élevé

MITRE ATT&CK : T1059.001 (Command and Scripting Interpreter: PowerShell)

DESCRIPTION :

Le mode de langage contraint (CLM — Constrained Language Mode) limite les fonctionnalités PowerShell disponibles aux utilisateurs non administrateurs. En CLM, les appels .NET directs, les types COM, les expressions Add-Type et les scripts non signés sont bloqués. CLM est automatiquement activé lorsque WDAC ou AppLocker avec des règles de script est déployé. Ce mode réduit considérablement les capacités d'attaque PowerShell.

Impact métier : Sans CLM, PowerShell offre un accès complet aux API .NET et COM, permettant des attaques sophistiquées (chargement de shellcode, accès DPAPI, etc.).

```
$ExecutionContext.SessionState.LanguageMode
# Doit retourner "ConstrainedLanguage" pour les utilisateurs non-admin
```

AUDIT :

- Valeur attendue : **ConstrainedLanguage (pour les non-administrateurs)**

REMÉDIATION :

1. Déployer WDAC ou AppLocker avec des règles de script pour activer automatiquement CLM
2. Via variable d'environnement (moins sécurisé, contournable) :

```
[Environment]::SetEnvironmentVariable("__PSLockdownPolicy", "4", "Machine")
```

VALEUR PAR DÉFAUT :

FullLanguage (mode complet)

10.1.5 *Désactiver PowerShell v2* Critique

MITRE ATT&CK : T1059.001 (Command and Scripting Interpreter: PowerShell)

DESCRIPTION :

PowerShell v2 est une version héritée qui ne supporte AUCUNE des mesures de journalisation avancée (Script Block Logging, Module Logging, Transcription). Un attaquant peut explicitement lancer PowerShell v2 avec la commande `powershell -version 2` pour contourner toutes les mesures de journalisation. La désinstallation du moteur PowerShell v2 est absolument critique.

Impact métier : PowerShell v2 permet l'exécution de scripts malveillants sans aucune journalisation, rendant l'attaque complètement invisible.

```
Get-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root | Select-Object State
Get-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2 | Select-Object State
```

AUDIT :

- Valeur attendue : **State = Disabled (Désactivé)**

```
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root -NoRestart
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2 -NoRestart
```

VALEUR PAR DÉFAUT :

Installé (mais peut être désactivé via DISM)

10.1.6 *Configurer la politique d'exécution PowerShell* Moyen

MITRE ATT&CK : T1059.001 (Command and Scripting Interpreter: PowerShell)

DESCRIPTION :

La politique d'exécution PowerShell contrôle quels scripts peuvent être exécutés. Les niveaux sont : Restricted, AllSigned, RemoteSigned, Unrestricted, Bypass. Note : la politique d'exécution n'est PAS une mesure de sécurité robuste (elle est facilement contournable), mais elle fournit une couche de protection contre l'exécution accidentelle de scripts non fiables. Le CIS recommande AllSigned ou RemoteSigned.

Impact métier : La politique d'exécution offre une protection de base contre l'exécution accidentelle de scripts non fiables.

```
Get-ExecutionPolicy -List
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell" -Name "ExecutionPolicy" -ErrorAction S
```

AUDIT :

- Valeur attendue : **AllSigned ou RemoteSigned**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows PowerShell > Activer l'exécution de scripts` → **Autoriser les scripts signés uniquement**
2. Via PowerShell :

```
Set-ExecutionPolicy RemoteSigned -Scope LocalMachine -Force
```

VALEUR PAR DÉFAUT :

Restricted

Section 11 — BUREAU À DISTANCE (RDP / Remote Desktop)

11.0 — BUREAU À DISTANCE (RDP / Remote Desktop)

11.1.1 *Exiger l'authentification au niveau du réseau (NLA)* — Critique

MITRE ATT&CK : T1021.001 (Remote Services: Remote Desktop Protocol)

DESCRIPTION :

L'authentification au niveau du réseau (NLA — Network Level Authentication) exige que l'utilisateur s'authentifie AVANT l'établissement de la session RDP. Sans NLA, un attaquant peut établir une connexion RDP complète jusqu'à l'écran de connexion, consommant des ressources et exposant le serveur aux vulnérabilités pré-authentification (comme BlueKeep — CVE-2019-0708). NLA protège contre les attaques par force brute en validant les identifiants au niveau réseau.

Impact métier : Sans NLA, le serveur est exposé aux exploits RDP pré-authentification et aux attaques par déni de service RDP.

```
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 "SecurityLayer"
```

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication`
- Valeur attendue : **1 (NLA activé)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de la session Bureau à distance > Sécurité > Exiger l'authentification utilisateur pour les connexions distantes en utilisant l'authentification au niveau du réseau` → **Activé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name "UserAuthentication" -Val
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name "SecurityLayer" -Value 2
```

VALEUR PAR DÉFAUT :

Activé (Windows Server 2025)

11.1.2 *Configurer le niveau de chiffrement RDP* — Élevé

MITRE ATT&CK : T1040 (Network Sniffing)

DESCRIPTION :

Ce paramètre définit le niveau de chiffrement minimum pour les connexions RDP. Le CIS recommande le niveau « Élevé » (High) qui utilise le chiffrement RC4 128 bits ou AES. Avec NLA activé et TLS configuré, le chiffrement est négocié via TLS, mais ce paramètre sert de fallback et doit être configuré au niveau le plus élevé.

Impact métier : Un niveau de chiffrement faible permet l'interception et le déchiffrement des sessions RDP.

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

AUDIT :

- Registre : `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\MinEncryptionLevel`
- Valeur attendue : **3 (Élevé / High)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de la session Bureau à distance > Sécurité > Définir le niveau de chiffrement de la connexion client` → **Élevé**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name "MinEncryptionLevel" -Val
```

VALEUR PAR DÉFAUT :

Client Compatible

11.1.3 *Configurer le délai d'inactivité des sessions RDP* — Élevé

MITRE ATT&CK : T1563.002 (Remote Service Session Hijacking: RDP Hijacking)

DESCRIPTION :

Ce paramètre détermine le temps d'inactivité avant qu'une session RDP ne soit déconnectée automatiquement. Les sessions RDP inactives consomment des ressources et représentent un risque de sécurité car elles peuvent être détournées par un attaquant (RDP Session Hijacking via tscon.exe). Le CIS recommande un délai de 15 minutes maximum.

Impact métier : Les sessions RDP inactives sont des cibles pour le détournement de session et l'accès non autorisé.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name "MaxIdleTime" -ErrorAction SilentlyCo
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\MaxIdleTime`
- Valeur attendue : **900000 millisecondes (15 minutes)** ou moins

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de la session Bureau à distance > Limites de durée des sessions > Définir la limite de temps pour les sessions actives mais inactives des services Bureau à distance` → **15 minutes**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name "MaxIdleTime" -Value 900000 -Type DWo
```

VALEUR PAR DÉFAUT :

Non défini (pas de limite)

11.1.4 *Configurer le délai de déconnexion des sessions* — Moyen

MITRE ATT&CK : T1563.002 (Remote Service Session Hijacking: RDP Hijacking)

DESCRIPTION :

Ce paramètre détermine combien de temps une session RDP déconnectée reste sur le serveur avant d'être fermée. Les sessions déconnectées maintiennent les processus en cours et peuvent être reconnectées par un attaquant. Le CIS recommande un délai maximum d'une minute pour les sessions déconnectées.

Impact métier : Les sessions déconnectées maintiennent les processus actifs et les jetons d'authentification, pouvant être exploitées pour le détournement.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name "MaxDisconnectionTime" -ErrorAction S
```

AUDIT :

- Valeur attendue : **60000 millisecondes (1 minute)**

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name "MaxDisconnectionTime" -Value 60000 -
```

VALEUR PAR DÉFAUT :

Non défini

11.1.5 *Interdire la redirection du presse-papiers RDP* — Élevé

MITRE ATT&CK : T1115 (Clipboard Data)

DESCRIPTION :

La redirection du presse-papiers permet de copier-coller des données entre le client RDP et le serveur. Un attaquant ayant compromis le poste client peut utiliser cette fonctionnalité pour exfiltrer des données du serveur via le presse-papiers. De même, un serveur compromis peut accéder au presse-papiers du client.

Impact métier : La redirection du presse-papiers est un canal d'exfiltration de données entre le client et le serveur.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name "fDisableClip" -ErrorAction SilentlyC
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\fDisableClip`
- Valeur attendue : **1 (Activé — redirection désactivée)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de la session Bureau à distance > Redirection de périphériques et de ressources > Ne pas autoriser la redirection du Presse-papiers` → **Activé**

VALEUR PAR DÉFAUT :

Non défini (redirection autorisée)

11.1.6 *Interdire la redirection des lecteurs RDP* — Élevé

MITRE ATT&CK : T1039 (Data from Network Shared Drive)

DESCRIPTION :

La redirection des lecteurs permet d'accéder aux disques du client depuis la session RDP et vice versa. Cette fonctionnalité facilite le transfert de fichiers mais représente un risque significatif d'exfiltration de données et d'introduction de malware. Sur un serveur de production, cette redirection doit être désactivée.

Impact métier : La redirection des lecteurs crée un canal bidirectionnel pour le transfert de fichiers non contrôlé entre le client et le serveur.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name "fDisableCdm" -ErrorAction SilentlyCo
```

AUDIT :

- Registre : `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\fDisableCdm`
- Valeur attendue : **1 (Activé — redirection désactivée)**

REMÉDIATION :

1. Via GPO : `Composants Windows > Services Bureau à distance > Hôte de la session Bureau à distance > Redirection de périphériques et de ressources > Ne pas autoriser la redirection de lecteur` → **Activé**

VALEUR PAR DÉFAUT :

Non défini (redirection autorisée)

11.1.7 *Configurer le certificat TLS pour RDP* — Élevé

MITRE ATT&CK : T1557 (Adversary-in-the-Middle)

DESCRIPTION :

Par défaut, RDP utilise un certificat auto-signé pour le chiffrement TLS, ce qui ne protège pas contre les attaques MITM car les utilisateurs sont habitués à ignorer les avertissements de certificat. La configuration d'un certificat émis par une autorité de certification interne (PKI d'entreprise) permet de valider l'authenticité du serveur et de détecter les interceptions.

Impact métier : Un certificat auto-signé ne protège pas contre les attaques MITM sur RDP.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name "SSLCertificateSHA1Hash"
# Vérifier le certificat RDP
Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object { $_.EnhancedKeyUsageList -match "Remote Desktop" } | Select-Object Subjec
```

AUDIT :

- Valeur attendue : **Certificat émis par une CA interne, non auto-signé**

REMÉDIATION :

1. Installer un certificat émis par la PKI d'entreprise avec EKU « Remote Desktop Authentication »
2. Configurer via GPO : `Composants Windows > Services Bureau à distance > Hôte de la session Bureau à distance > Sécurité > Modèle de certificat d'authentification serveur`

VALEUR PAR DÉFAUT :

Certificat auto-signé

11.1.8 *Limiter le nombre de sessions RDP simultanées* — Moyen

MITRE ATT&CK : T1021.001 (Remote Services: Remote Desktop Protocol)

DESCRIPTION :

Limiter le nombre de sessions RDP simultanées réduit le risque de sessions non surveillées et force le partage de sessions, améliorant la traçabilité. Pour un serveur membre standard, le CIS recommande une limite d'une ou deux sessions simultanées.

Impact métier : Un nombre illimité de sessions RDP complique la surveillance et augmente le risque de sessions non détectées.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name "MaxInstanceCount" -ErrorAction Silen
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server" -Name "MaxConnectionAllowed" -ErrorAction SilentlyC
```

AUDIT :

- Valeur attendue : **2 sessions maximum**

REMÉDIATION :

1. Via GPO : `Composants Windows > Services Bureau à distance > Hôte de la session Bureau à distance > Connexions > Limiter le nombre de connexions` → **2**

VALEUR PAR DÉFAUT :

2 (pour le mode Administration à distance)

11.1.9 *Configurer le délai d'expiration du mot de passe RDP* Moyen

MITRE ATT&CK : T1021.001 (Remote Services: Remote Desktop Protocol)

DESCRIPTION :

Ce paramètre détermine si les mots de passe clients RDP enregistrés sont acceptés. Le CIS recommande de ne pas autoriser l'enregistrement des mots de passe pour les connexions RDP, forçant l'authentification à chaque connexion. Les mots de passe RDP enregistrés sont stockés dans le Credential Manager et peuvent être extraits.

Impact métier : Les mots de passe RDP enregistrés dans le Credential Manager sont extractibles par des outils d'attaque.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" -Name "DisablePasswordSaving" -ErrorAction
```

AUDIT :

- Valeur attendue : **1 (Désactiver l'enregistrement des mots de passe)**

REMÉDIATION :

1. Via GPO : `Composants Windows > Services Bureau à distance > Client Connexion Bureau à distance > Ne pas autoriser l'enregistrement de mot de passe` → **Activé**

VALEUR PAR DÉFAUT :

Non défini

12.0 — MISES À JOUR ET MAINTENANCE (Windows Update / WSUS)

12.1.1 *Vérifier que les mises à jour de sécurité sont à jour* — Critique

MITRE ATT&CK : T1190 (Exploit Public-Facing Application)

DESCRIPTION :

Les mises à jour de sécurité corrigent les vulnérabilités connues (CVE) qui sont activement exploitées par les attaquants. Un serveur non patché est la cible la plus facile et la plus courante. Le délai entre la publication d'un patch et son application doit être minimal (< 30 jours pour les correctifs critiques, < 72 heures pour les zero-day). Windows Server 2025 supporte les hotpatches qui permettent l'application de certains correctifs sans redémarrage.

Impact métier : Un serveur non patché est vulnérable à toutes les CVE publiées depuis le dernier patch, avec des exploits souvent disponibles publiquement.

```
# Date de la dernière mise à jour
Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 5 HotFixID, Description, InstalledOn
# Vérifier les mises à jour en attente
$session = New-Object -ComObject Microsoft.Update.Session
$searcher = $session.CreateUpdateSearcher()
$result = $searcher.Search("IsInstalled=0 and Type='Software'")
$result.Updates | Select-Object Title, MsrcSeverity
# Jours depuis le dernier patch
$lastPatch = (Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 1).InstalledOn
$daysSinceLastPatch = (New-TimeSpan -Start $lastPatch -End (Get-Date)).Days
Write-Host "Jours depuis le dernier patch : $daysSinceLastPatch"
```

AUDIT :

- Valeur attendue : **Moins de 30 jours depuis le dernier patch de sécurité**

REMÉDIATION :

1. Installer les mises à jour en attente :

```
# Via PowerShell (module PSWindowsUpdate)
Install-Module -Name PSWindowsUpdate -Force
Get-WindowsUpdate -AcceptAll -Install -AutoReboot
```

REMÉDIATION :

1. Planifier les mises à jour via WSUS ou Windows Update for Business

VALEUR PAR DÉFAUT :

Configuration dépendante de la politique de l'organisation

12.1.2 *Configurer Windows Update via WSUS ou WUfB* — Élevé

MITRE ATT&CK : T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain)

DESCRIPTION :

Pour les environnements d'entreprise, les mises à jour doivent être gérées via WSUS (Windows Server Update Services) ou Windows Update for Business (WUfB). Cela permet le contrôle et le test des mises à jour avant leur déploiement, la validation de l'intégrité des correctifs et la conformité à la politique de gestion des changements.

Impact métier : Les mises à jour non contrôlées peuvent introduire des problèmes de compatibilité. L'absence de gestion centralisée empêche le suivi de la conformité.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -ErrorAction SilentlyContinue | Select-Object WUSe
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -ErrorAction SilentlyContinue | Select-Object U
```

AUDIT :

- Valeur attendue : **WUServer configuré ou WUfB activé**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update > Spécifier l'emplacement intranet du service de mise à jour Microsoft`

VALEUR PAR DÉFAUT :

Windows Update direct (Microsoft)

12.1.3 *Configurer le redémarrage automatique après installation des mises à jour* Moyen

MITRE ATT&CK : T1190 (Exploit Public-Facing Application)

DESCRIPTION :

Certaines mises à jour nécessitent un redémarrage pour être pleinement appliquées. La configuration du redémarrage automatique en dehors des heures de production garantit que les correctifs sont effectivement appliqués. Windows Server 2025 introduit les hotpatches qui réduisent le besoin de redémarrage pour certains correctifs.

Impact métier : Les mises à jour non appliquées par manque de redémarrage laissent le serveur vulnérable malgré le téléchargement des correctifs.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "AUOptions" -ErrorAction SilentlyContinue
# Vérifier les redémarrages en attente
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\RebootRequired" -ErrorAction Sile
```

AUDIT :

- Valeur attendue : **Téléchargement automatique et installation planifiée (AUOptions = 4)**

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "AUOptions" -Value 4 -Type DWord
```

VALEUR PAR DÉFAUT :

3 (Téléchargement automatique, notification pour l'installation)

12.1.4 *Activer les hotpatches (Windows Server 2025)* Moyen

MITRE ATT&CK : T1190 (Exploit Public-Facing Application)

DESCRIPTION :

Windows Server 2025 introduit le hotpatching, une fonctionnalité qui permet d'appliquer certaines mises à jour de sécurité sans redémarrer le serveur. Le hotpatching modifie le code en mémoire du processus en cours d'exécution, éliminant le temps d'arrêt. Cette fonctionnalité est disponible pour les serveurs Azure Arc-enabled ou les VM Azure. L'activation du hotpatching réduit significativement le temps d'exposition aux vulnérabilités.

Impact métier : Le hotpatching permet l'application immédiate des correctifs de sécurité sans interruption de service.

```
# Vérifier si le hotpatching est supporté et configuré
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Update\TargetingInfo\Installed\*" -ErrorAction SilentlyC
# Vérifier Azure Arc
Get-Service -Name "himds" -ErrorAction SilentlyContinue | Select-Object Name, Status
```

AUDIT :

- Valeur attendue : **Activé si compatible avec l'infrastructure**

REMÉDIATION :

1. Enrôler le serveur dans Azure Arc
2. Activer le hotpatching via Azure Update Manager
3. Configurer la politique de hotpatch via Azure Policy

VALEUR PAR DÉFAUT :

Non configuré

13.0 — CHIFFREMENT ET PROTECTION DES DONNÉES

13.1.1 *Activer BitLocker sur le volume système*

Critique

MITRE ATT&CK : T1005 (Data from Local System)

DESCRIPTION :

BitLocker chiffre l'intégralité du volume de disque, protégeant les données contre l'accès physique non autorisé. Sans BitLocker, un attaquant ayant un accès physique au serveur peut extraire les disques, les monter sur un autre système et accéder à toutes les données, y compris les fichiers SAM, NTDS.dit, les certificats et les clés privées. Le protecteur TPM+PIN est recommandé pour empêcher le démarrage non autorisé.

Impact métier : Sans chiffrement de disque, toutes les données du serveur sont accessibles en cas d'accès physique ou de vol de disque.

```
# Vérifier l'état de BitLocker
Get-BitLockerVolume | Select-Object MountPoint, VolumeStatus, EncryptionMethod, KeyProtector, ProtectionStatus
# Vérifier le statut TPM
Get-Tpm | Select-Object TpmPresent, TpmReady, TpmEnabled, TpmActivated
```

AUDIT :

- Valeur attendue : **VolumeStatus = FullyEncrypted, ProtectionStatus = On, Protecteur = TPM + PIN**

REMÉDIATION :

1. Activer BitLocker via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteurs du système d'exploitation`
2. Via PowerShell :

```
Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 -TpmAndPinProtector -Pin (ConvertTo-SecureString "PIN_COMPLEXE" -AsPl
```

VALEUR PAR DÉFAUT :

Non configuré

13.1.2 *Configurer l'algorithme de chiffrement BitLocker*

Élevé

MITRE ATT&CK : T1600 (Weaken Encryption)

DESCRIPTION :

Windows Server 2025 supporte plusieurs algorithmes de chiffrement BitLocker. Le CIS recommande XTS-AES-256 pour les lecteurs fixes et AES-CBC-256 pour les lecteurs amovibles. XTS-AES est plus résistant aux attaques de manipulation de données et offre de meilleures performances.

Impact métier : Un algorithme de chiffrement faible réduit la protection effective de BitLocker.

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\FVE" -Name "EncryptionMethodWithXtsOs" -ErrorAction SilentlyContinue
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\FVE" -Name "EncryptionMethodWithXtsFdv" -ErrorAction SilentlyContinue
Get-BitLockerVolume | Select-Object MountPoint, EncryptionMethod
```

AUDIT :

- Valeur attendue : **XtsAes256 (7)**

REMÉDIATION :

1. Via GPO : `Chiffrement de lecteur BitLocker > Choisir la méthode de chiffrement et la puissance de chiffrement du lecteur` → **XTS-AES 256 bits**
2. Via registre :

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\FVE" -Name "EncryptionMethodWithXtsOs" -Value 7 -Type DWord
```

VALEUR PAR DÉFAUT :

XTS-AES 128 bits

13.1.3 *Sauvegarder les clés de récupération BitLocker dans Active Directory* Élevé

MITRE ATT&CK : T1486 (Data Encrypted for Impact)

DESCRIPTION :

Les clés de récupération BitLocker doivent être sauvegardées dans Active Directory pour permettre le déverrouillage en cas de perte du protecteur principal (changement de TPM, oubli du PIN). Sans sauvegarde AD, la perte du protecteur principal rend les données irrécupérables. La sauvegarde AD stocke les clés de récupération de manière sécurisée avec les permissions appropriées.

Impact métier : La perte de la clé de récupération BitLocker rend les données du serveur irréversiblement inaccessibles.

```
# Vérifier la configuration de sauvegarde AD
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\FVE" -Name "FDVActiveDirectoryBackup" -ErrorAction SilentlyContinue
# Vérifier la clé de récupération
(Get-BitLockerVolume -MountPoint "C:").KeyProtector | Where-Object { $_.KeyProtectorType -eq "RecoveryPassword" }
# Vérifier dans AD (depuis un DC)
Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'} -SearchBase "CN=SERVERNAME,OU=Servers,DC=domain,DC=com" -ErrorAc
```

AUDIT :

- Valeur attendue : **Clé de récupération sauvegardée dans AD**

REMÉDIATION :

1. Via GPO : `Chiffrement de lecteur BitLocker > Lecteurs du système d'exploitation > Choisir la méthode de récupération des lecteurs du système d'exploitation protégés par BitLocker` → **Sauvegarder les informations de récupération dans les services de domaine AD**
2. Forcer la sauvegarde :

```
$recoveryKey = (Get-BitLockerVolume -MountPoint "C:").KeyProtector | Where-Object { $_.KeyProtectorType -eq "RecoveryPassword" }
Backup-BitLockerKeyProtector -MountPoint "C:" -KeyProtectorId $recoveryKey.KeyProtectorId
```

VALEUR PAR DÉFAUT :

Non configuré

13.1.4 *Chiffrement EFS — Restrictions et audit* Moyen

MITRE ATT&CK : T1486 (Data Encrypted for Impact)

DESCRIPTION :

EFS (Encrypting File System) permet le chiffrement au niveau fichier. Dans un environnement contrôlé, l'utilisation d'EFS doit être soit désactivée (si BitLocker est utilisé), soit configurée avec des certificats gérés par la PKI d'entreprise. L'utilisation d'EFS sans agent de récupération (DRA — Data Recovery Agent) peut rendre les données irrécupérables si le certificat utilisateur est perdu.

Impact métier : EFS mal configuré peut rendre des données irrécupérables ou offrir une protection insuffisante.

```
# Vérifier la configuration EFS
cipher /status C:\
# Vérifier les certificats DRA
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\EFS" -ErrorAction SilentlyContinue
```

AUDIT :

- Valeur attendue : **EFS désactivé ou configuré avec un DRA**

REMÉDIATION :

1. Désactiver EFS si non nécessaire via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique > Système de fichiers EFS`
2. Configurer un agent de récupération si EFS est utilisé

VALEUR PAR DÉFAUT :

Activé

14.0 — SÉCURITÉ MATÉRIELLE ET BOOT

14.1.1 *Vérifier que Secure Boot est activé*

Critique

MITRE ATT&CK : T1542.003 (Pre-OS Boot: Bootkit)

DESCRIPTION :

Secure Boot est une fonctionnalité UEFI qui vérifie la signature numérique de tous les composants du processus de démarrage (firmware, chargeur de démarrage, pilotes, noyau) avant leur exécution. Sans Secure Boot, un attaquant peut installer un bootkit qui s'exécute avant le système d'exploitation et est invisible pour les outils de sécurité Windows. Secure Boot est un prérequis pour Credential Guard et HVCI.

Impact métier : Sans Secure Boot, le processus de démarrage est vulnérable aux bootkits persistants et indétectables.

```
Confirm-SecureBootUEFI
# Ou
[System.Security.SecurityElement]::IsValidText((Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot\State" -N
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot\State" -Name "UEFISecureBootEnabled"
```

AUDIT :

- Valeur attendue : **True / UEFISecureBootEnabled = 1**

REMÉDIATION :

1. Activer Secure Boot dans le BIOS/UEFI du serveur
2. ⚠️ S'assurer que tous les pilotes sont signés avant l'activation

VALEUR PAR DÉFAUT :

Activé (sur le matériel compatible)

14.1.2 *Vérifier la présence et l'état du TPM 2.0*

Critique

MITRE ATT&CK : T1542 (Pre-OS Boot)

DESCRIPTION :

Le TPM (Trusted Platform Module) 2.0 est un composant matériel cryptographique qui fournit le stockage sécurisé des clés, la mesure de l'intégrité du démarrage (PCR) et la génération de nombres aléatoires matériels. Le TPM 2.0 est un prérequis pour BitLocker avec protecteur matériel, Credential Guard et l'attestation de santé du système. Windows Server 2025 exige TPM 2.0 pour Secured-core server.

Impact métier : Sans TPM, BitLocker ne peut pas utiliser de protecteur matériel, et Credential Guard ne peut pas sécuriser les identifiants avec VBS.

```
Get-Tpm | Select-Object TpmPresent, TpmReady, TpmEnabled, TpmActivated, ManufacturerId, ManufacturerVersion
# Version TPM
Get-WmiObject -Namespace "root\cimv2\Security\MicrosoftTpm" -Class Win32_Tpm | Select-Object SpecVersion
```

AUDIT :

- Valeur attendue : **TpmPresent = True, TpmReady = True, SpecVersion ≥ 2.0**

REMÉDIATION :

1. Activer le TPM dans le BIOS/UEFI
2. Initialiser le TPM : `Initialize-Tpm`
3. Si le TPM est en état limité : `Clear-Tpm` puis `Initialize-Tpm`

VALEUR PAR DÉFAUT :

Dépend du matériel

14.1.3 *Activer l'intégrité du code protégée par l'hyperviseur (HVCI)* Élevé

MITRE ATT&CK : T1068 (Exploitation for Privilege Escalation)

DESCRIPTION :

HVCI (Hypervisor-Protected Code Integrity) utilise la virtualisation matérielle pour vérifier l'intégrité de chaque page de code avant son exécution en mode noyau. HVCI empêche le chargement de pilotes non signés ou malveillants et protège contre les exploits de corruption de mémoire du noyau. Windows Server 2025 améliore les performances HVCI et l'intègre dans le concept « Secured-core server ».

Impact métier : Sans HVCI, des pilotes non signés ou malveillants peuvent être chargés dans le noyau, permettant un contrôle total et indétectable du système.

```
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Select-Object SecurityServicesRunning,
# VirtualizationBasedSecurityStatus : 0=Off, 1=Configured, 2=Running
# SecurityServicesRunning contient : 1=Credential Guard, 2=HVCI
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard" -Name "EnableVirtualizationBasedSecurity" -ErrorAction
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity" -Name "Enable
```

AUDIT :

- Valeur attendue : **VBS activé, HVCI activé (Enabled = 1)**

REMÉDIATION :

1. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Système > Device Guard > Activer la sécurité basée sur la virtualisation` → **Activé**
2. Protection de l'intégrité du code basée sur la virtualisation → **Activé avec verrouillage UEFI**
3. Via registre :

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard" -Name "EnableVirtualizationBasedSecurity" -Value 1 -Typ
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity" -Force
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity" -Name "Enable
```

REMÉDIATION :

⚠️ **Redémarrage nécessaire. Vérifier la compatibilité des pilotes avant activation.**

VALEUR PAR DÉFAUT :

Non configuré (activé par défaut sur Secured-core server)

14.1.4 *Secured-core server (Windows Server 2025)* Élevé

MITRE ATT&CK : T1542 (Pre-OS Boot)

DESCRIPTION :

Secured-core server est un ensemble de fonctionnalités de sécurité matérielle intégrées dans Windows Server 2025 : Secure Boot, TPM 2.0, VBS, Credential Guard, HVCI, System Guard, et DRTM (Dynamic Root of Trust for Measurement). Sur le matériel compatible, Secured-core fournit le plus haut niveau de protection contre les attaques firmware et les menaces avancées persistantes (APT).

Impact métier : Secured-core server offre la protection la plus complète contre les attaques matérielles et firmware sur Windows Server.

```
# Vérifier le statut Secured-core
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Format-List *
# Vérifier tous les composants
$vbs = Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard
Write-Host "VBS Status: $($vbs.VirtualizationBasedSecurityStatus)"
Write-Host "Security Services Running: $($vbs.SecurityServicesRunning)"
Write-Host "Required Security Properties: $($vbs.RequiredSecurityProperties)"
# Vérifier System Guard
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\SystemGuard" -ErrorAction SilentlyContinue
```

AUDIT :

- Valeur attendue : **Tous les composants Secured-core activés**

REMÉDIATION :

1. Vérifier la compatibilité matérielle (HPE, Dell, Lenovo ont des modèles certifiés Secured-core)
2. Activer tous les composants via GPO Device Guard
3. Configurer DRTM si le matériel le supporte

VALEUR PAR DÉFAUT :

Dépend du matériel et de la configuration du firmware

15.0 — SÉCURITÉ IIS (si rôle installé)

15.1.1 *Supprimer les en-têtes de version IIS* — Élevé

MITRE ATT&CK : T1592.004 (Gather Victim Host Information: Client Configurations)

DESCRIPTION :

Par défaut, IIS expose sa version dans l'en-tête HTTP `Server` et dans les pages d'erreur. Cette information permet à un attaquant d'identifier les vulnérabilités spécifiques à la version d'IIS. La suppression de ces en-têtes complique la reconnaissance et l'identification des cibles.

Impact métier : L'exposition de la version IIS facilite le ciblage des exploits spécifiques à cette version.

```
# Vérifier l'en-tête Server
(Invoke-WebRequest -Uri "http://localhost" -UseBasicParsing -ErrorAction SilentlyContinue).Headers.Server
# Vérifier le paramètre removeServerHeader
Get-WebConfigurationProperty -Filter "system.webServer/security/requestFiltering" -Name "removeServerHeader" -PSPath "IIS:\" -Error
```

AUDIT :

- Valeur attendue : **removeServerHeader = True**

```
# Supprimer l'en-tête Server
Set-WebConfigurationProperty -Filter "system.webServer/security/requestFiltering" -Name "removeServerHeader" -Value $true -PSPath "
# Via web.config
# <system.webServer><security><requestFiltering removeServerHeader="true" /></security></system.webServer>
```

VALEUR PAR DÉFAUT :

False (en-tête exposé)

15.1.2 *Désactiver la navigation dans les répertoires* — Critique

MITRE ATT&CK : T1083 (File and Directory Discovery)

DESCRIPTION :

La navigation dans les répertoires (Directory Browsing) permet aux visiteurs de voir la liste des fichiers dans un répertoire web. Cette fonctionnalité est extrêmement dangereuse car elle peut exposer des fichiers de configuration, des sauvegardes, des scripts de déploiement et d'autres données sensibles.

Impact métier : L'exposition du contenu des répertoires peut révéler des fichiers de configuration contenant des identifiants ou des informations sensibles.

```
Get-WebConfigurationProperty -Filter "system.webServer/directoryBrowse" -Name "enabled" -PSPath "IIS:\" -ErrorAction SilentlyContin
```

AUDIT :

- Valeur attendue : **False (Désactivé)**

```
Set-WebConfigurationProperty -Filter "system.webServer/directoryBrowse" -Name "enabled" -Value $false -PSPath "IIS:\"
```

VALEUR PAR DÉFAUT :

Désactivé

15.1.3 *Configurer les en-têtes de sécurité HTTP* — Élevé

MITRE ATT&CK : T1189 (Drive-by Compromise)

DESCRIPTION :

Les en-têtes de sécurité HTTP protègent contre les attaques web courantes : X-Content-Type-Options (empêche le MIME sniffing), X-Frame-Options (empêche le clickjacking), Content-Security-Policy (empêche le XSS), Strict-Transport-Security (force HTTPS). Ces en-têtes doivent être configurés sur tous les sites IIS.

Impact métier : L'absence d'en-têtes de sécurité expose les applications web aux attaques XSS, clickjacking et injection de contenu.

```
# Vérifier les en-têtes personnalisés
Get-WebConfigurationProperty -Filter "system.webServer/httpProtocol/customHeaders" -Name "." -PSPath "IIS:\" | Select-Object name,
# Tester avec une requête
(Invoke-WebRequest -Uri "http://localhost" -UseBasicParsing).Headers | Format-Table
```

AUDIT :

- Valeur attendue : **X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Strict-Transport-Security: max-age=31536000**

```
Add-WebConfigurationProperty -Filter "system.webServer/httpProtocol/customHeaders" -Name "." -Value @{name="X-Content-Type-Options"
Add-WebConfigurationProperty -Filter "system.webServer/httpProtocol/customHeaders" -Name "." -Value @{name="X-Frame-Options";value=
Add-WebConfigurationProperty -Filter "system.webServer/httpProtocol/customHeaders" -Name "." -Value @{name="Strict-Transport-Securi
```

VALEUR PAR DÉFAUT :

Aucun en-tête de sécurité

15.1.4 *Configurer la journalisation IIS* Élevé

MITRE ATT&CK : T1070 (Indicator Removal)

DESCRIPTION :

La journalisation IIS doit être activée sur tous les sites avec le format W3C Extended et les champs pertinents pour la sécurité (adresse IP client, agent utilisateur, URI, code de statut, temps de réponse). Les journaux doivent être stockés dans un emplacement sécurisé et collectés par le SIEM.

Impact métier : Sans journalisation IIS, il est impossible de détecter et d'investiguer les attaques web.

```
Get-WebConfigurationProperty -Filter "system.applicationHost/sites/site/logFile" -Name "logFormat" -PSPath "IIS:\" -ErrorAction Sil
Get-WebConfigurationProperty -Filter "system.applicationHost/sites/site/logFile" -Name "directory" -PSPath "IIS:\" -ErrorAction Sil
```

AUDIT :

- Valeur attendue : **Format W3C, champs de sécurité activés**

```
Set-WebConfigurationProperty -Filter "system.applicationHost/sites/site/logFile" -Name "logFormat" -Value "W3C" -PSPath "IIS:\"
```

VALEUR PAR DÉFAUT :

W3C

15.1.5 *Forcer HTTPS et désactiver HTTP* Critique

MITRE ATT&CK : T1040 (Network Sniffing)

DESCRIPTION :

Toutes les communications IIS doivent transiter via HTTPS (TLS 1.2+). Le trafic HTTP doit être soit désactivé, soit redirigé vers HTTPS. Les sites en HTTP transmettent les données et potentiellement les identifiants en clair sur le réseau. La configuration d'un certificat TLS valide est un prérequis.

Impact métier : Le trafic HTTP en clair permet l'interception de données sensibles et d'identifiants d'authentification.

```
# Vérifier les bindings HTTPS
Get-WebBinding | Select-Object protocol, bindingInformation, sslFlags | Format-Table
# Vérifier la redirection HTTP vers HTTPS
Get-WebConfigurationProperty -Filter "system.webServer/httpRedirect" -Name "enabled" -PSPath "IIS:\" -ErrorAction SilentlyContinue
```

AUDIT :

- Valeur attendue : **Tous les sites en HTTPS, HTTP redirigé vers HTTPS**

REMÉDIATION :

1. Installer un certificat TLS sur le site IIS
2. Configurer la redirection HTTP → HTTPS
3. Activer HSTS (HTTP Strict Transport Security)

VALEUR PAR DÉFAUT :

HTTP sur le port 80

15.1.6 *Configurer les pools d'applications avec un compte de service dédié* Élevé

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Chaque pool d'applications IIS doit s'exécuter sous une identité de compte de service dédiée avec les privilèges minimaux nécessaires. L'utilisation d'ApplicationPoolIdentity (identité virtuelle) est recommandée par Microsoft. L'exécution sous LocalSystem ou NetworkService donne au pool d'applications des privilèges excessifs.

Impact métier : Un pool d'applications compromis s'exécutant sous LocalSystem donne un accès SYSTEM complet au serveur.

```
Get-IISAppPool | Select-Object Name, ProcessModel.IdentityType, State
# Ou
Import-Module WebAdministration
Get-ChildItem IIS:\AppPools | ForEach-Object { [PSCustomObject]@{Name=$_.Name; Identity=$_.processModel.identityType; User=$_.proce
```

AUDIT :

- Valeur attendue : **IdentityType = ApplicationPoolIdentity ou compte de service dédié**

```
Set-WebConfigurationProperty -Filter "/system.applicationHost/applicationPools/add[@name='DefaultAppPool']/processModel" -Name "ide
```

VALEUR PAR DÉFAUT :

ApplicationPoolIdentity

15.1.7 *Désactiver les méthodes HTTP non nécessaires* Moyen

MITRE ATT&CK : T1190 (Exploit Public-Facing Application)

DESCRIPTION :

Les méthodes HTTP comme PUT, DELETE, TRACE, OPTIONS, CONNECT peuvent être utilisées pour des attaques (upload de fichiers malveillants, Cross-Site Tracing, etc.). Seules les méthodes nécessaires (GET, POST, HEAD) doivent être autorisées. La méthode TRACE est particulièrement dangereuse car elle peut être utilisée pour des attaques XST (Cross-Site Tracing).

Impact métier : Les méthodes HTTP dangereuses peuvent être exploitées pour l'upload de webshells ou le vol d'identifiants.

```
Get-WebConfigurationProperty -Filter "system.webServer/security/requestFiltering/verbs" -Name "." -PSPath "IIS:\" -ErrorAction Sile
```

AUDIT :

- Valeur attendue : **TRACE, PUT, DELETE bloqués sauf besoin explicite**

```
Add-WebConfigurationProperty -Filter "system.webServer/security/requestFiltering/verbs" -Name "." -Value @{verb="TRACE";allowed="fa
Add-WebConfigurationProperty -Filter "system.webServer/security/requestFiltering/verbs" -Name "." -Value @{verb="PUT";allowed="fals
```

VALEUR PAR DÉFAUT :

Toutes les méthodes autorisées

16.0 — GESTION DES CERTIFICATS ET PKI

16.1.1 *Vérifier les certificats racine de confiance* — Élevé

MITRE ATT&CK : T1553.004 (Subvert Trust Controls: Install Root Certificate)

DESCRIPTION :

Le magasin de certificats racine de confiance détermine quelles autorités de certification sont approuvées par le serveur. L'ajout d'un certificat racine malveillant permet à un attaquant de créer des certificats valides pour n'importe quel domaine, interceptant les communications TLS (man-in-the-middle). Le contenu du magasin racine doit être audité régulièrement.

Impact métier : Un certificat racine malveillant permet l'interception de toutes les communications HTTPS.

```
# Lister les certificats racine de confiance
Get-ChildItem Cert:\LocalMachine\Root | Select-Object Subject, Issuer, NotAfter, Thumbprint | Format-Table -AutoSize
# Compter les certificats
(Get-ChildItem Cert:\LocalMachine\Root).Count
# Identifier les certificats non-Microsoft
Get-ChildItem Cert:\LocalMachine\Root | Where-Object { $_.Issuer -notmatch "Microsoft" -and $_.Issuer -notmatch "VeriSign" -and $_.
```

AUDIT :

- Valeur attendue : **Uniquement des certificats racine légitimes et documentés**

REMÉDIATION :

1. Supprimer les certificats racine non autorisés
2. Désactiver la mise à jour automatique des certificats racine si contrôlé par GPO
3. Configurer via GPO : `Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique > Paramètres de validation du chemin des certificats`

VALEUR PAR DÉFAUT :

Certificats racine Microsoft et partenaires

16.1.2 *Vérifier les certificats expirés* — Moyen

MITRE ATT&CK : T1553 (Subvert Trust Controls)

DESCRIPTION :

Les certificats expirés doivent être identifiés et renouvelés ou supprimés. Un certificat expiré utilisé par un service (IIS, RDP, WinRM) ne fournit plus de protection valide et peut causer des erreurs de connexion ou des avertissements que les utilisateurs s'habituent à ignorer.

Impact métier : Les certificats expirés causent des interruptions de service et habituent les utilisateurs à ignorer les avertissements de sécurité.

```
# Certificats expirés
Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.NotAfter -lt (Get-Date) } | Select-Object Subject, NotAfter, Thumbprint
# Certificats expirant dans 30 jours
Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.NotAfter -lt (Get-Date).AddDays(30) -and $_.NotAfter -gt (Get-Date) } | Sel
```

AUDIT :

- Valeur attendue : **Aucun certificat expiré dans le magasin personnel**

REMÉDIATION :

1. Renouveler les certificats expirés ou en voie d'expiration
2. Supprimer les certificats obsolètes
3. Configurer le monitoring d'expiration des certificats

VALEUR PAR DÉFAUT :

N/A

16.1.3 *Configurer la révocation de certificats (CRL / OCSP)* — Moyen

MITRE ATT&CK : T1553.004 (Subvert Trust Controls: Install Root Certificate)

DESCRIPTION :

La vérification de révocation des certificats (CRL — Certificate Revocation List ou OCSP — Online Certificate Status Protocol) garantit que les certificats révoqués ne sont pas acceptés. Sans vérification de révocation, un certificat compromis et révoqué par la CA continue d'être accepté comme valide par le serveur.

Impact métier : L'acceptation de certificats révoqués permet l'utilisation de certificats compromis.

```
# Vérifier la configuration de révocation
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllVerifyRevocation" -ErrorAction SilentlyCont
# Vérifier via certutil
certutil -verify -urlfetch C:\path\to\cert.cer 2>$null | Select-String "Revocation"
```

AUDIT :

- Valeur attendue : **Vérification de révocation activée (CRL ou OCSP)**

REMÉDIATION :

1. Configurer la vérification CRL dans les GPO
2. Configurer les points de distribution CRL accessibles
3. Configurer OCSP si disponible

VALEUR PAR DÉFAUT :

Vérification de révocation activée par défaut

17.0 — MONITORING ET DÉTECTION

17.1.1 *Déployer Sysmon pour une visibilité avancée*

Élevé

MITRE ATT&CK : T1059 (Command and Scripting Interpreter)

DESCRIPTION :

Sysmon (System Monitor) est un outil Microsoft Sysinternals qui fournit une visibilité bien supérieure à l'audit Windows natif sur les activités système : création de processus avec hash et ligne de commande, connexions réseau, modification de fichiers, chargement de DLL, accès au registre, injection de processus, etc. Sysmon est considéré comme indispensable par les équipes SOC et les analystes forensiques.

Impact métier : Sans Sysmon, la détection des menaces avancées (APT, mouvement latéral, malware sans fichier) est significativement réduite.

```
# Vérifier si Sysmon est installé et actif
Get-Service -Name "Sysmon" -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
Get-Service -Name "Sysmon64" -ErrorAction SilentlyContinue | Select-Object Name, Status, StartType
# Vérifier la configuration Sysmon
sysmon -c 2>$null
# Vérifier les événements Sysmon
Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 5 -ErrorAction SilentlyContinue | Select-Object TimeCreated
```

AUDIT :

- Valeur attendue : **Sysmon installé, actif, avec une configuration ANSSI ou SwiftOnSecurity**

REMÉDIATION :

1. Télécharger Sysmon : https://docs.microsoft.com/sysinternals/downloads/sysmon
2. Installer avec une configuration recommandée :

```
sysmon64.exe -accepteula -i sysmon-config.xml
# Configuration recommandée : https://github.com/SwiftOnSecurity/sysmon-config
```

VALEUR PAR DÉFAUT :

Non installé

17.1.2 *Configurer Windows Event Forwarding (WEF)*

Élevé

MITRE ATT&CK : T1070.001 (Indicator Removal: Clear Windows Event Logs)

DESCRIPTION :

Windows Event Forwarding (WEF) permet la collecte centralisée des événements Windows vers un serveur collecteur. WEF est une alternative à l'agent SIEM pour la collecte des journaux et offre l'avantage d'être intégré nativement dans Windows sans logiciel tiers. La collecte centralisée empêche un attaquant de détruire les traces en effaçant les journaux locaux.

Impact métier : Sans collecte centralisée, un attaquant qui efface les journaux locaux détruit toutes les traces de l'intrusion.

```
# Vérifier la configuration WEF source
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\EventLog\EventForwarding\SubscriptionManager" -ErrorAction Silent
# Vérifier le service WinRM (nécessaire pour WEF)
Get-Service -Name "WinRM" | Select-Object Name, Status, StartType
# Lister les souscriptions
wecutil es 2>$null
```

AUDIT :

- Valeur attendue : **WEF configuré vers un collecteur central ou agent SIEM déployé**

REMÉDIATION :

1. Configurer le serveur collecteur WEF
2. Via GPO : `Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Transfert d'événements > Configurer le gestionnaire d'abonnements cible`
3. Alternative : déployer un agent SIEM (Splunk, Elastic, Sentinel)

VALEUR PAR DÉFAUT :

Non configuré

17.1.3 *Configurer Microsoft Defender Antivirus* Critique

MITRE ATT&CK : T1562.001 (Impair Defenses: Disable or Modify Tools)

DESCRIPTION :

Microsoft Defender Antivirus est intégré à Windows Server 2025 et doit être activé et à jour. La protection en temps réel, la protection cloud (MAPS), la soumission automatique d'échantillons et la protection contre les PUA (Potentially Unwanted Applications) doivent être configurées. Si un antivirus tiers est utilisé, vérifier qu'il est actif et à jour.

Impact métier : Un antivirus désactivé ou obsolète permet l'exécution de malware connu sans détection.

```
Get-MpComputerStatus | Select-Object AntivirusEnabled, RealTimeProtectionEnabled, AntivirusSignatureLastUpdated, AMServiceEnabled,
# Vérifier les définitions
$sigAge = ((Get-Date) - (Get-MpComputerStatus).AntivirusSignatureLastUpdated).Days
Write-Host "Age des signatures : $sigAge jours"
```

AUDIT :

- Valeur attendue : **Activé, protection en temps réel activée, signatures < 3 jours**

```
Set-MpPreference -DisableRealtimeMonitoring $false
Set-MpPreference -MAPSReporting Advanced
Set-MpPreference -SubmitSamplesConsent SendAllSamples
Update-MpSignature
```

VALEUR PAR DÉFAUT :

Activé

17.1.4 *Activer la réduction de la surface d'attaque (ASR)* Élevé

MITRE ATT&CK : T1059 (Command and Scripting Interpreter)

DESCRIPTION :

Les règles ASR (Attack Surface Reduction) de Microsoft Defender bloquent les comportements malveillants courants : création de processus enfants par les applications Office, exécution de contenu téléchargé par les applications Office, injection de processus, vol d'identifiants depuis LSASS, etc. Windows Server 2025 supporte un ensemble étendu de règles ASR qui doivent être configurées en mode blocage.

Impact métier : Les règles ASR bloquent les techniques d'attaque les plus courantes utilisées par les ransomwares et les malwares.

```
Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Ids
Get-MpPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules_Actions
```

AUDIT :

- Valeur attendue : **Règles ASR critiques activées en mode Block (1) ou Warn (6)**

```
# Activer les règles ASR critiques
# Bloquer le vol d'identifiants depuis LSASS
Add-MpPreference -AttackSurfaceReductionRules_Ids "9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2" -AttackSurfaceReductionRules_Actions Enabl
# Bloquer la création de processus enfants par les applications Office
Add-MpPreference -AttackSurfaceReductionRules_Ids "d4f940ab-401b-4efc-aadc-ad5f3c50688a" -AttackSurfaceReductionRules_Actions Enabl
# Bloquer l'exécution de scripts potentiellement obfusqués
Add-MpPreference -AttackSurfaceReductionRules_Ids "5beb7efe-fd9a-4556-801d-275e5ffc04cc" -AttackSurfaceReductionRules_Actions Enabl
```

VALEUR PAR DÉFAUT :

Non configuré

17.1.5 *Configurer l'intégration SIEM* Élevé

MITRE ATT&CK : T1070 (Indicator Removal)

DESCRIPTION :

L'intégration avec un SIEM (Security Information and Event Management) centralise la collecte, la corrélation et l'analyse des événements de sécurité. Sans SIEM, les événements de sécurité restent isolés sur chaque serveur et ne peuvent pas être corrélés pour détecter les attaques multi-étapes. Le SIEM doit collecter au minimum les journaux Security, Sysmon, PowerShell et Application.

Impact métier : Sans corrélation centralisée, les attaques complexes multi-étapes passent inaperçues.

```
# Vérifier la présence d'un agent SIEM
Get-Service -Name "SplunkForwarder","winlogbeat","nxlog","OssecSvc","MicrosoftMonitoringAgent" -ErrorAction SilentlyContinue | Sele
# Vérifier WEF
wecutil es 2>$null
```

AUDIT :

- Valeur attendue : **Agent SIEM actif ou WEF configuré**

REMÉDIATION :

1. Installer et configurer l'agent SIEM approprié
2. Configurer les sources de journaux à collecter
3. Vérifier la réception des événements sur le SIEM central

VALEUR PAR DÉFAUT :

Non configuré

18.0 — CONFORMITÉ ET GOUVERNANCE

18.1.1 *Documentation de la configuration de référence (Security Baseline)*

Moyen

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Une configuration de référence (baseline) de sécurité doit être documentée, approuvée et maintenue pour le serveur. Cette baseline définit les paramètres de sécurité attendus et sert de référence pour la détection des dérives de configuration (configuration drift). Le présent document constitue cette baseline pour les serveurs Windows Server 2025. La baseline doit être révisée au minimum annuellement.

Impact métier : Sans baseline documentée, il est impossible de détecter les dérives de configuration ou de reproduire une configuration sécurisée.

AUDIT :

- Vérifier l'existence de la documentation de baseline
- Vérifier la date de dernière révision
- Vérifier l'approbation par la direction

REMÉDIATION :

1. Utiliser ce document comme base de la configuration de référence
2. Exporter la configuration actuelle avec LGPO ou secedit
3. Documenter les écarts justifiés et les exceptions

VALEUR PAR DÉFAUT :

N/A

18.1.2 *Processus de gestion des changements*

Moyen

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Un processus formel de gestion des changements doit exister pour toute modification de la configuration du serveur. Ce processus doit inclure : la demande de changement, l'analyse d'impact, l'approbation, la mise en œuvre, la vérification et la documentation. Les modifications non autorisées doivent être détectées et investiguées.

Impact métier : Les changements non contrôlés peuvent introduire des vulnérabilités ou dégrader la posture de sécurité.

AUDIT :

- Vérifier l'existence du processus de gestion des changements
- Vérifier les derniers changements documentés
- Vérifier les outils de détection de drift (DSC, SCCM, etc.)

REMÉDIATION :

1. Implémenter un processus ITIL de gestion des changements
2. Utiliser PowerShell DSC (Desired State Configuration) pour la détection de drift
3. Configurer des alertes sur les modifications de configuration

VALEUR PAR DÉFAUT :

N/A

18.1.3 *Plan de réponse aux incidents*

Moyen

MITRE ATT&CK : T1078 (Valid Accounts)

DESCRIPTION :

Un plan de réponse aux incidents (IRP — Incident Response Plan) documenté et testé doit exister. Ce plan doit couvrir : la détection, l'analyse, le confinement, l'éradication et la récupération. Les coordonnées des contacts d'urgence, les procédures d'escalade et les outils d'investigation doivent être documentés et accessibles.

Impact métier : Sans plan de réponse aux incidents, la réaction à une compromission est désorganisée, prolongeant le temps d'exposition et augmentant les dommages.

AUDIT :

- Vérifier l'existence et la date du plan de réponse aux incidents
- Vérifier la date du dernier exercice (tabletop ou simulation)
- Vérifier les coordonnées des contacts d'urgence

REMÉDIATION :

1. Rédiger un plan de réponse aux incidents basé sur NIST SP 800-61
2. Planifier des exercices réguliers (au minimum annuels)
3. Documenter les leçons apprises de chaque incident

VALEUR PAR DÉFAUT :

N/A

18.1.4 *Sauvegarde et restauration de la configuration de sécurité* Élevé

MITRE ATT&CK : T1490 (Inhibit System Recovery)

DESCRIPTION :

La configuration de sécurité du serveur doit être sauvegardée régulièrement pour permettre la restauration rapide en cas de compromission ou de défaillance. Les sauvegardes doivent inclure : la configuration de sécurité locale (secedit), les GPO appliquées (gpresult), les certificats, les règles de pare-feu et la configuration des services.

Impact métier : Sans sauvegarde de la configuration, la restauration après incident nécessite une reconstruction complète et prolonge le temps d'indisponibilité.

```
# Exporter la configuration de sécurité
secedit /export /cfg C:\ANC-Audit\secpol-backup.cfg
# Exporter les GPO appliquées
gpresult /h C:\ANC-Audit\gpresult-backup.html /f
# Exporter les règles de pare-feu
netsh advfirewall export C:\ANC-Audit\firewall-backup.wfw
# Exporter la liste des services
Get-Service | Export-Csv C:\ANC-Audit\services-backup.csv -NoTypeInformation
```

AUDIT :

- Valeur attendue : **Sauvegarde récente (< 30 jours) de la configuration de sécurité**

REMÉDIATION :

1. Planifier une sauvegarde régulière de la configuration
2. Stocker les sauvegardes dans un emplacement sécurisé hors du serveur
3. Tester la restauration régulièrement

VALEUR PAR DÉFAUT :

N/A

18.1.5 *Conformité aux cadres réglementaires applicables* Moyen

MITRE ATT&CK : N/A

DESCRIPTION :

Vérifier la conformité du serveur aux cadres réglementaires applicables : RGPD (protection des données personnelles), NIS2 (sécurité des infrastructures critiques), PCI DSS (traitement des données de cartes bancaires), HDS (hébergement de données de santé), SOC 2, ISO 27001. Les exigences spécifiques de chaque cadre doivent être mappées aux contrôles de ce document.

Impact métier : La non-conformité réglementaire expose l'organisation à des sanctions financières et juridiques significatives.

AUDIT :

- Identifier les cadres réglementaires applicables
- Vérifier la couverture des exigences par les contrôles de ce document
- Documenter les écarts et les plans de remédiation

REMÉDIATION :

1. Réaliser une analyse d'écart (gap analysis) pour chaque cadre applicable
2. Prioritiser les actions de remédiation selon le risque
3. Documenter la conformité et maintenir les preuves d'audit

VALEUR PAR DÉFAUT :

N/A

Annexe : Checklist (221 controles)

#	Recommandation	Niveau	Oui	Non	N/A
Section 1 — POLITIQUE DE COMPTES (Account Policies)					
1.1.1	Appliquer l'historique des mots de passe	Critique	☐	☐	☐
1.1.2	Âge maximum du mot de passe	Élevé	☐	☐	☐
1.1.3	Âge minimum du mot de passe	Élevé	☐	☐	☐
1.1.4	Longueur minimale du mot de passe	Critique	☐	☐	☐
1.1.5	Le mot de passe doit respecter des exigences de complexité	Critique	☐	☐	☐
1.1.6	Assouplir les limites de longueur minimale du mot de passe	Moyen	☐	☐	☐
1.1.7	Stocker les mots de passe en utilisant un chiffrement réversible	Critique	☐	☐	☐
1.1.8	Audit de longueur minimale du mot de passe	Moyen	☐	☐	☐
1.2.1	Durée de verrouillage des comptes	Critique	☐	☐	☐
1.2.2	Seuil de verrouillage du compte	Critique	☐	☐	☐
1.2.3	Réinitialiser le compteur de verrouillage du compte après	Critique	☐	☐	☐
1.2.4	Autoriser le verrouillage du compte Administrateur	Critique	☐	☐	☐
1.3.1	Application des restrictions d'ouverture de session utilisateur	Moyen	☐	☐	☐
1.3.2	Durée de vie maximale du ticket de service	Moyen	☐	☐	☐
1.3.3	Durée de vie maximale du ticket utilisateur	Moyen	☐	☐	☐
1.3.4	Durée de vie maximale pour le renouvellement du ticket utilisateur	Moyen	☐	☐	☐
1.3.5	Tolérance maximale pour la synchronisation de l'horloge	Moyen	☐	☐	☐
1.4.1	Windows LAPS — Gestion du mot de passe administrateur local	Critique	☐	☐	☐
1.4.2	Renommer le compte administrateur local	Élevé	☐	☐	☐
1.4.3	Renommer le compte Invité	Moyen	☐	☐	☐
1.4.4	Désactiver le compte Invité	Élevé	☐	☐	☐
1.4.5	Désactiver le compte Administrateur local intégré	Élevé	☐	☐	☐
1.4.6	Utilisation de comptes de service gérés de groupe (gMSA)	Élevé	☐	☐	☐
1.4.7	Restreindre l'utilisation de mots de passe vides pour les comptes locaux	Critique	☐	☐	☐
1.4.8	Bloquer les comptes Microsoft pour l'authentification	Élevé	☐	☐	☐
Section 2 — STRATÉGIES LOCALES (Local Policies)					
2.1.1	Accéder à cet ordinateur depuis le réseau	Élevé	☐	☐	☐
2.1.2	Agir en tant que partie du système d'exploitation	Critique	☐	☐	☐
2.1.3	Permettre l'ouverture de session locale	Élevé	☐	☐	☐
2.1.4	Autoriser l'ouverture de session par les services Bureau à distance	Critique	☐	☐	☐
2.1.5	Sauvegarder les fichiers et les répertoires	Moyen	☐	☐	☐
2.1.6	Créer un objet-jeton	Critique	☐	☐	☐
2.1.7	Créer des objets globaux	Moyen	☐	☐	☐
2.1.8	Créer des objets partagés permanents	Moyen	☐	☐	☐
2.1.9	Créer des liens symboliques	Moyen	☐	☐	☐
2.1.10	Déboguer les programmes	Critique	☐	☐	☐
2.1.11	Refuser l'accès à cet ordinateur depuis le réseau	Critique	☐	☐	☐
2.1.12	Refuser l'ouverture de session en tant que tâche	Moyen	☐	☐	☐
2.1.13	Refuser l'ouverture de session en tant que service	Moyen	☐	☐	☐
2.1.14	Refuser l'ouverture de session locale	Élevé	☐	☐	☐
2.1.15	Refuser l'ouverture de session par les services Bureau à distance	Critique	☐	☐	☐
2.1.16	Autoriser l'approbation des ordinateurs et des comptes utilisateurs pour la délégation	Critique	☐	☐	☐
2.1.17	Forcer l'arrêt à partir d'un système distant	Moyen	☐	☐	☐
2.1.18	Générer des audits de sécurité	Moyen	☐	☐	☐
2.1.19	Emprunter l'identité d'un client après authentification	Élevé	☐	☐	☐
2.1.20	Augmenter la priorité de planification	Moyen	☐	☐	☐
2.1.21	Charger et décharger les pilotes de périphériques	Critique	☐	☐	☐
2.1.22	Gérer le journal d'audit et de sécurité	Élevé	☐	☐	☐
2.1.23	Modifier les valeurs de l'environnement du microprogramme	Moyen	☐	☐	☐
2.1.24	Effectuer des tâches de maintenance de volume	Moyen	☐	☐	☐
2.1.25	Restaurer les fichiers et les répertoires	Moyen	☐	☐	☐
2.1.26	Arrêter le système	Moyen	☐	☐	☐
2.1.27	Prendre possession de fichiers ou d'autres objets	Critique	☐	☐	☐
2.1.28	Ajuster les quotas de mémoire pour un processus	Moyen	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
2.1.29	Modifier l'heure système	Moyen	☐	☐	☐
2.1.30	Remplacer un jeton de niveau processus	Moyen	☐	☐	☐
2.2.1	Audit : Forcer les paramètres de sous-catégorie de stratégie d'audit	Élevé	☐	☐	☐
2.2.2	Audit : Arrêter le système immédiatement si les audits de sécurité ne peuvent pas être journalisés	Moyen	☐	☐	☐
2.2.3	Périphériques : Autorisation de formatage et d'éjection des médias amovibles	Moyen	☐	☐	☐
2.2.4	Périphériques : Empêcher les utilisateurs d'installer des pilotes d'imprimante	Moyen	☐	☐	☐
2.2.5	Membre de domaine : Chiffrer ou signer numériquement les données de canal sécurisé (toujours)	Critique	☐	☐	☐
2.2.6	Membre de domaine : Chiffrer numériquement les données de canal sécurisé (si possible)	Élevé	☐	☐	☐
2.2.7	Membre de domaine : Signer numériquement les données de canal sécurisé (si possible)	Élevé	☐	☐	☐
2.2.8	Membre de domaine : Désactiver les modifications de mot de passe du compte ordinateur	Élevé	☐	☐	☐
2.2.9	Membre de domaine : Âge maximal du mot de passe du compte ordinateur	Moyen	☐	☐	☐
2.2.10	Membre de domaine : Nécessite une clé de session forte (Windows 2000 ou ultérieur)	Élevé	☐	☐	☐
2.2.11	Ouverture de session interactive : Ne pas afficher le dernier nom d'utilisateur connecté	Élevé	☐	☐	☐
2.2.12	Ouverture de session interactive : Ne pas demander la combinaison CTRL+ALT+SUPPR	Moyen	☐	☐	☐
2.2.13	Ouverture de session interactive : Limite d'inactivité de l'ordinateur	Élevé	☐	☐	☐
2.2.14	Ouverture de session interactive : Texte du message pour les utilisateurs	Moyen	☐	☐	☐
2.2.15	Ouverture de session interactive : Titre du message pour les utilisateurs	Moyen	☐	☐	☐
2.2.16	Ouverture de session interactive : Comportement de retrait de carte à puce	Moyen	☐	☐	☐
2.2.17	Client réseau Microsoft : Communications signées numériquement (toujours)	Critique	☐	☐	☐
2.2.18	Client réseau Microsoft : Envoyer un mot de passe non chiffré aux serveurs SMB tiers	Critique	☐	☐	☐
2.2.19	Serveur réseau Microsoft : Communications signées numériquement (toujours)	Critique	☐	☐	☐
2.2.20	Serveur réseau Microsoft : Déconnecter les clients à l'expiration des horaires d'ouverture de session	Moyen	☐	☐	☐
2.2.21	Accès réseau : Ne pas autoriser l'énumération anonyme des comptes SAM	Critique	☐	☐	☐
2.2.22	Accès réseau : Ne pas autoriser l'énumération anonyme des comptes et partages SAM	Critique	☐	☐	☐
2.2.23	Accès réseau : Ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'authentification réseau	Élevé	☐	☐	☐
2.2.24	Accès réseau : Laisser les autorisations Tout le monde s'appliquer aux utilisateurs anonymes	Critique	☐	☐	☐
2.2.25	Accès réseau : Restreindre l'accès anonyme aux canaux nommés et aux partages	Élevé	☐	☐	☐
2.2.26	Accès réseau : Restreindre les clients autorisés à effectuer des appels distants vers SAM	Critique	☐	☐	☐
2.2.27	Sécurité réseau : Autoriser le système local à utiliser l'identité de l'ordinateur pour NTLM	Élevé	☐	☐	☐
2.2.28	Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos	Critique	☐	☐	☐
2.2.29	Sécurité réseau : Ne pas stocker la valeur de hachage de LAN Manager au prochain changement de mot de passe	Critique	☐	☐	☐
2.2.30	Sécurité réseau : Niveau d'authentification LAN Manager	Critique	☐	☐	☐
2.2.31	Sécurité réseau : Conditions requises pour la signature client LDAP	Critique	☐	☐	☐
2.2.32	Sécurité réseau : Sécurité de session minimale pour les clients NTLM SSP	Élevé	☐	☐	☐
2.2.33	Sécurité réseau : Sécurité de session minimale pour les serveurs NTLM SSP	Élevé	☐	☐	☐
2.2.34	Contrôle de compte d'utilisateur : Comportement de l'invite d'élévation pour les administrateurs	Critique	☐	☐	☐
2.2.35	Contrôle de compte d'utilisateur : Comportement de l'invite d'élévation pour les utilisateurs standard	Élevé	☐	☐	☐
2.2.36	Contrôle de compte d'utilisateur : Détecter les installations d'applications et demander l'élévation	Moyen	☐	☐	☐
2.2.37	Contrôle de compte d'utilisateur : Exécuter tous les administrateurs en mode d'approbation Administrateur	Critique	☐	☐	☐
2.2.38	Contrôle de compte d'utilisateur : Passer au bureau sécurisé lors de la demande d'élévation	Élevé	☐	☐	☐
2.2.39	Contrôle de compte d'utilisateur : Virtualiser les échecs d'écriture de fichiers et de registre	Moyen	☐	☐	☐
2.2.40	Contrôle de compte d'utilisateur : Élever uniquement les applications UIAccess installées dans des emplacements sécurisés	Moyen	☐	☐	☐
2.2.41	Cryptographie système : Utiliser des algorithmes conformes FIPS pour le chiffrement, le hachage et la signature	Moyen	☐	☐	☐
2.2.42	Arrêt : Permettre l'arrêt du système sans ouvrir de session	Moyen	☐	☐	☐
Section 3 — JOURNALISATION ET AUDIT (Event Log & Audit Policy)					
3.1.1	Auditer la validation des informations d'identification	Critique	☐	☐	☐
3.1.2	Auditer le service d'authentification Kerberos	Élevé	☐	☐	☐
3.1.3	Auditer la gestion des comptes d'ordinateur	Moyen	☐	☐	☐
3.1.4	Auditer la gestion des groupes de sécurité	Critique	☐	☐	☐
3.1.5	Auditer la gestion des comptes d'utilisateur	Critique	☐	☐	☐
3.1.6	Auditer l'activité DPAPI	Moyen	☐	☐	☐
3.1.7	Auditer la création de processus	Critique	☐	☐	☐
3.1.8	Auditer le verrouillage du compte	Élevé	☐	☐	☐
3.1.9	Auditer l'appartenance à un groupe	Élevé	☐	☐	☐
3.1.10	Auditer la fermeture de session	Moyen	☐	☐	☐
3.1.11	Auditer l'ouverture de session	Critique	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
3.1.12	Auditer d'autres événements d'ouverture/fermeture de session	Moyen	☐	☐	☐
3.1.13	Auditer l'ouverture de session spéciale	Élevé	☐	☐	☐
3.1.14	Auditer les modifications de la stratégie d'audit	Critique	☐	☐	☐
3.1.15	Auditer les modifications de la stratégie d'authentification	Élevé	☐	☐	☐
3.1.16	Auditer l'utilisation de privilèges sensibles	Critique	☐	☐	☐
3.1.17	Auditer l'intégrité du système et le pilote IPsec	Élevé	☐	☐	☐
3.1.18	Auditer d'autres événements système	Moyen	☐	☐	☐
3.1.19	Auditer l'extension du système de sécurité	Élevé	☐	☐	☐
3.1.20	Auditer l'accès au système de fichiers et aux objets du registre	Élevé	☐	☐	☐
3.2.1	Taille maximale du journal de sécurité	Critique	☐	☐	☐
3.2.2	Taille maximale du journal système	Élevé	☐	☐	☐
3.2.3	Taille maximale du journal d'application	Moyen	☐	☐	☐
3.2.4	Méthode de rétention du journal de sécurité	Élevé	☐	☐	☐
3.2.5	Activer le journal PowerShell/Operational	Critique	☐	☐	☐
Section 4 — PARE-FEU WINDOWS DEFENDER (Windows Defender Firewall)					
4.1.1	Pare-feu activé sur le profil Domaine	Critique	☐	☐	☐
4.1.2	Action par défaut pour les connexions entrantes — Profil Domaine	Critique	☐	☐	☐
4.1.3	Action par défaut pour les connexions sortantes — Profil Domaine	Moyen	☐	☐	☐
4.1.4	Journalisation du pare-feu — Profil Domaine	Élevé	☐	☐	☐
4.1.5	Interdire les notifications de fusion de règles locales — Profil Domaine	Moyen	☐	☐	☐
4.2.1	Pare-feu activé sur le profil Privé	Critique	☐	☐	☐
4.2.2	Configuration complète du profil Privé	Élevé	☐	☐	☐
4.3.1	Pare-feu activé sur le profil Public	Critique	☐	☐	☐
4.3.2	Configuration complète du profil Public	Critique	☐	☐	☐
4.3.3	Audit des règles de pare-feu existantes	Élevé	☐	☐	☐
Section 5 — SERVICES SYSTÈME (System Services)					
5.1.1	Désactiver le service Spouleur d'impression (Print Spooler)	Critique	☐	☐	☐
5.1.2	Désactiver le service Assistance à distance (Remote Assistance)	Élevé	☐	☐	☐
5.1.3	Désactiver le service WinRM (si non utilisé)	Moyen	☐	☐	☐
5.1.4	Désactiver le service de découverte SSDP (SSDP Discovery)	Moyen	☐	☐	☐
5.1.5	Désactiver le service Hôte de périphérique UPnP	Moyen	☐	☐	☐
5.1.6	Désactiver le service Xbox et services de jeu	Moyen	☐	☐	☐
5.1.7	Désactiver Bluetooth Support Service	Moyen	☐	☐	☐
5.1.8	Désactiver le service LxssManager (WSL)	Élevé	☐	☐	☐
5.1.9	Désactiver les services IIS inutiles	Élevé	☐	☐	☐
5.1.10	Désactiver le service FTP (FTPSVC)	Critique	☐	☐	☐
Section 6 — REGISTRE ET PERMISSIONS (Registry & File System)					
6.1.1	Permissions sur la ruche de registre SAM	Critique	☐	☐	☐
6.1.2	Permissions sur la ruche de registre SECURITY	Critique	☐	☐	☐
6.1.3	Protection du registre contre l'accès réseau distant	Élevé	☐	☐	☐
6.1.4	Permissions sur les fichiers système critiques	Élevé	☐	☐	☐
6.1.5	Désactiver l'enregistrement du nom NetBIOS	Élevé	☐	☐	☐
6.1.6	Désactiver LLMNR (Link-Local Multicast Name Resolution)	Critique	☐	☐	☐
6.1.7	Désactiver mDNS (Multicast DNS)	Élevé	☐	☐	☐
Section 7 — SÉCURITÉ RÉSEAU (Network Security)					
7.1.1	Signature SMB requise côté serveur	Critique	☐	☐	☐
7.1.2	Chiffrement SMB activé	Élevé	☐	☐	☐
7.1.3	Désactiver SMBv1	Critique	☐	☐	☐
7.1.4	SMB over QUIC (Windows Server 2025)	Moyen	☐	☐	☐
7.2.1	Signature LDAP côté client requise	Critique	☐	☐	☐
7.2.2	Channel Binding LDAP	Élevé	☐	☐	☐
7.3.1	Niveau d'authentification LAN Manager	Critique	☐	☐	☐
7.3.2	Audit et restriction du trafic NTLM	Élevé	☐	☐	☐
7.4.1	Désactiver SSL 2.0 et SSL 3.0	Critique	☐	☐	☐
7.4.2	Désactiver TLS 1.0 et TLS 1.1	Élevé	☐	☐	☐
7.4.3	Activer et configurer TLS 1.3	Élevé	☐	☐	☐
7.4.4	Configuration des suites de chiffrement TLS	Élevé	☐	☐	☐
7.5.1	Configurer DNS over HTTPS (DoH) ou DNS over TLS (DoT)	Moyen	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
7.6.1	Désactiver IPv6 (si non utilisé)	Moyen	☐	☐	☐
7.6.2	Configurer IPSec pour les communications sensibles	Moyen	☐	☐	☐
7.6.3	Désactiver WPAD (Web Proxy Auto-Discovery)	Élevé	☐	☐	☐
Section 8 — CREDENTIAL GUARD & PROTECTION DES IDENTIFIANTS					
8.1.1	Activer Credential Guard (Virtualization-Based Security)	Critique	☐	☐	☐
8.1.2	Activer la protection LSA (LSA Protection / RunAsPPL)	Critique	☐	☐	☐
8.1.3	Désactiver WDigest Authentication	Critique	☐	☐	☐
8.1.4	Désactiver la mise en cache des identifiants de domaine	Élevé	☐	☐	☐
8.1.5	Remote Credential Guard pour les connexions RDP	Élevé	☐	☐	☐
Section 9 — CONTRÔLE DES APPLICATIONS (AppLocker / WDAC)					
9.1.1	Implémenter Windows Defender Application Control (WDAC)	Élevé	☐	☐	☐
9.1.2	Configurer AppLocker (alternative à WDAC)	Élevé	☐	☐	☐
9.1.3	Bloquer l'exécution de scripts non signés	Élevé	☐	☐	☐
9.1.4	Bloquer les LOLBins (Living Off the Land Binaries)	Élevé	☐	☐	☐
Section 10 — POWERSHELL ET SCRIPTING					
10.1.1	Activer le Script Block Logging PowerShell	Critique	☐	☐	☐
10.1.2	Activer le Module Logging PowerShell	Élevé	☐	☐	☐
10.1.3	Activer la transcription PowerShell	Élevé	☐	☐	☐
10.1.4	Configurer le mode de langage contraint (Constrained Language Mode)	Élevé	☐	☐	☐
10.1.5	Désactiver PowerShell v2	Critique	☐	☐	☐
10.1.6	Configurer la politique d'exécution PowerShell	Moyen	☐	☐	☐
Section 11 — BUREAU À DISTANCE (RDP / Remote Desktop)					
11.1.1	Exiger l'authentification au niveau du réseau (NLA)	Critique	☐	☐	☐
11.1.2	Configurer le niveau de chiffrement RDP	Élevé	☐	☐	☐
11.1.3	Configurer le délai d'inactivité des sessions RDP	Élevé	☐	☐	☐
11.1.4	Configurer le délai de déconnexion des sessions	Moyen	☐	☐	☐
11.1.5	Interdire la redirection du presse-papiers RDP	Élevé	☐	☐	☐
11.1.6	Interdire la redirection des lecteurs RDP	Élevé	☐	☐	☐
11.1.7	Configurer le certificat TLS pour RDP	Élevé	☐	☐	☐
11.1.8	Limiter le nombre de sessions RDP simultanées	Moyen	☐	☐	☐
11.1.9	Configurer le délai d'expiration du mot de passe RDP	Moyen	☐	☐	☐
Section 12 — MISES À JOUR ET MAINTENANCE (Windows Update / WSUS)					
12.1.1	Vérifier que les mises à jour de sécurité sont à jour	Critique	☐	☐	☐
12.1.2	Configurer Windows Update via WSUS ou WUfB	Élevé	☐	☐	☐
12.1.3	Configurer le redémarrage automatique après installation des mises à jour	Moyen	☐	☐	☐
12.1.4	Activer les hotpatches (Windows Server 2025)	Moyen	☐	☐	☐
Section 13 — CHIFFREMENT ET PROTECTION DES DONNÉES					
13.1.1	Activer BitLocker sur le volume système	Critique	☐	☐	☐
13.1.2	Configurer l'algorithme de chiffrement BitLocker	Élevé	☐	☐	☐
13.1.3	Sauvegarder les clés de récupération BitLocker dans Active Directory	Élevé	☐	☐	☐
13.1.4	Chiffrement EFS — Restrictions et audit	Moyen	☐	☐	☐
Section 14 — SÉCURITÉ MATÉRIELLE ET BOOT					
14.1.1	Vérifier que Secure Boot est activé	Critique	☐	☐	☐
14.1.2	Vérifier la présence et l'état du TPM 2.0	Critique	☐	☐	☐
14.1.3	Activer l'intégrité du code protégée par l'hyperviseur (HVCI)	Élevé	☐	☐	☐
14.1.4	Secured-core server (Windows Server 2025)	Élevé	☐	☐	☐
Section 15 — SÉCURITÉ IIS (si rôle installé)					
15.1.1	Supprimer les en-têtes de version IIS	Élevé	☐	☐	☐
15.1.2	Désactiver la navigation dans les répertoires	Critique	☐	☐	☐
15.1.3	Configurer les en-têtes de sécurité HTTP	Élevé	☐	☐	☐
15.1.4	Configurer la journalisation IIS	Élevé	☐	☐	☐
15.1.5	Forcer HTTPS et désactiver HTTP	Critique	☐	☐	☐
15.1.6	Configurer les pools d'applications avec un compte de service dédié	Élevé	☐	☐	☐
15.1.7	Désactiver les méthodes HTTP non nécessaires	Moyen	☐	☐	☐
Section 16 — GESTION DES CERTIFICATS ET PKI					
16.1.1	Vérifier les certificats racine de confiance	Élevé	☐	☐	☐
16.1.2	Vérifier les certificats expirés	Moyen	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
16.1.3	Configurer la révocation de certificats (CRL / OCSP)	Moyen	☐	☐	☐
Section 17 — MONITORING ET DÉTECTION					
17.1.1	Déployer Sysmon pour une visibilité avancée	Élevé	☐	☐	☐
17.1.2	Configurer Windows Event Forwarding (WEF)	Élevé	☐	☐	☐
17.1.3	Configurer Microsoft Defender Antivirus	Critique	☐	☐	☐
17.1.4	Activer la réduction de la surface d'attaque (ASR)	Élevé	☐	☐	☐
17.1.5	Configurer l'intégration SIEM	Élevé	☐	☐	☐
Section 18 — CONFORMITÉ ET GOUVERNANCE					
18.1.1	Documentation de la configuration de référence (Security Baseline)	Moyen	☐	☐	☐
18.1.2	Processus de gestion des changements	Moyen	☐	☐	☐
18.1.3	Plan de réponse aux incidents	Moyen	☐	☐	☐
18.1.4	Sauvegarde et restauration de la configuration de sécurité	Élevé	☐	☐	☐
18.1.5	Conformité aux cadres réglementaires applicables	Moyen	☐	☐	☐