

TP12 — Durcissement d'une machine Windows

Dossier explicatif : comment, pourquoi, et la justification CIS

Machine : Windows Server 2022 Standard (SRV-TP12) — VM Proxmox UEFI + TPM 2.0

Référentiel : CIS Microsoft Windows Server 2022 Benchmark v5.0.0 — profil Member Server (L1, + L2 pour VBS)

Résultat : 12 / 13 points durcis et prouvés · 1 documenté comme limite d'environnement (VBS)

Date : 03/07/2026

1. Introduction — qu'est-ce que le durcissement, et pourquoi ?

Durcir (ou *hardening*) une machine, c'est réduire sa **surface d'attaque** : désactiver ce qui est inutile, verrouiller ce qui est exploitable, et journaliser ce qui se passe. Une installation Windows par défaut privilégie la compatibilité et la facilité, pas la sécurité : de nombreux services et protocoles hérités sont actifs, les secrets d'authentification sont peu protégés, et rien n'est tracé. Un attaquant qui obtient un accès administrateur peut alors voler les identifiants en mémoire, se déplacer latéralement, et rester invisible.

Plutôt que de durcir « au feeling », on s'appuie sur un **référentiel reconnu** : le **CIS Benchmark**. Le Center for Internet Security publie, pour chaque système, une liste de recommandations numérotées, chacune avec un réglage précis, une justification et une procédure d'audit. On a utilisé la version **v5.0.0 pour Windows Server 2022**, profil **Member Server niveau 1** (durcissement fort sans casser les fonctionnalités courantes), complété par le **niveau 2** pour la virtualisation de sécurité (VBS).

Le TP demande d'auditer puis de durcir 13 domaines, et surtout de **prouver le changement d'état avant / après**. Ce dossier explique, pour chacun, **le risque, l'action menée, la recommandation CIS correspondante, et la preuve**.

2. La machine et les choix de plateforme

La cible est un **Windows Server 2022 Standard** dans une VM Proxmox. Ces choix ne sont pas anodins — ils conditionnent ce qu'on peut durcir :

- **UEFI + Secure Boot** (au lieu du vieux BIOS) : prérequis pour Credential Guard et pour verrouiller certaines protections au niveau firmware (RunAsPPL « UEFI lock »).
- **TPM 2.0** (puce cryptographique virtuelle) : indispensable pour **BitLocker**, qui scelle la clé de chiffrement du disque au TPM et ne la libère qu'à un démarrage sain.
- **CPU en mode « host » + virtualisation imbriquée** : expose les instructions de virtualisation à la VM, condition pour tenter VBS / Credential Guard.
- **Profil CIS Member Server** (et non Domain Controller) : la machine est autonome (workgroup), on applique donc les réglages via la **stratégie locale**, pas via des GPO de domaine.

Cette plateforme est capable de couvrir **100 % du sujet** — c'est justement pour cela qu'on l'a montée en UEFI + TPM + virtualisation imbriquée dès le départ.

3. Une démarche prouvable (le « comment »)

Le cœur du TP n'est pas seulement de durcir, mais de le **démontrer**. Notre méthode, entièrement scriptée et reproductible :

1. **Audit initial en lecture seule** : un script PowerShell lit l'état de chaque point (aucune modification) et produit une preuve horodatée. C'est l'état « AVANT ».
2. **Snapshot Proxmox « pre-hardening »** : photo de la VM avant durcissement, pour pouvoir rejouer l'avant/après ou revenir en arrière.
3. **Durcissement scripté** : un second script applique les réglages CIS, domaine par domaine.
4. **Reboot + snapshot « core-hardened »** : certains réglages (RunAsPPL, retrait de SMBv1) ne prennent effet qu'au redémarrage ; on re-photographie l'état durci.
5. **Ré-audit + captures** : on relance le même script d'audit — état « APRÈS » — et on capture une image par point. La comparaison avant/après est la preuve.

Avantage : tout est **rejouable** et **vérifiable**. Chaque affirmation du rapport est adossée à la sortie réelle d'une commande, pas à une capture d'écran isolée.

4. Le durcissement, mesure par mesure

Pour chaque domaine : **le risque**, **l'action**, **la justification CIS**, la preuve.

4.1 — Comptes locaux & mots de passe [CIS 1.1, 1.2, 2.3.1, 2.3.11](#)

Le risque — Un compte « Administrator » toujours nommé pareil (RID-500) est une cible connue ; sans verrouillage ni politique de mot de passe, il est vulnérable au **brute force** et aux mots de passe faibles. Le compte Invité et le protocole d'authentification hérité NTLMv1 élargissent l'exposition.

Ce qu'on a fait — Renommage de l'administrateur en **srvadmin** et de l'invité (désactivé) ; politique : mot de passe **14 caractères** minimum, complexité exigée, historique 24, âge max 365 j ; **verrouillage après 5 essais** ; NTLMv2 imposé (refus de LM/NTLMv1), pas de stockage du hash LM.

Pourquoi CIS le recommande — 1.1.1–1.1.7 fixent une politique de mot de passe résistante ; 1.2.1–1.2.4 freinent le brute force par verrouillage ; 2.3.1.3/2.3.1.4 rendent les comptes par défaut moins prévisibles ; 2.3.11.7 élimine les protocoles d'authentification cassés.

Preuve / vérification — net accounts et l'écran de connexion montrent le compte **srvadmin** et le seuil de verrouillage à 5. Capture après/01-comptes-locaux.

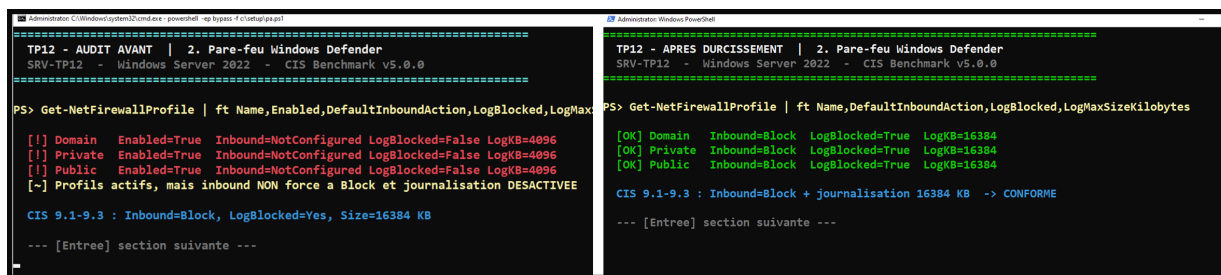
4.2 — Pare-feu Windows Defender [CIS 9.1 à 9.3](#)

Le risque — Les trois profils (Domaine/Privé/Public) étaient actifs mais **sans blocage explicite du trafic entrant** et **sans journalisation** : impossible de savoir ce qui est bloqué ou tenté.

Ce qu'on a fait — Sur les trois profils : **trafic entrant bloqué par défaut**, journalisation activée (paquets rejetés + connexions réussies), fichier de log porté à **16 Mo**.

Pourquoi CIS le recommande — 9.1.1/9.2.1/9.3.1 (pare-feu On), 9.x.2 (entrant = Block), 9.x.5 (log 16 384 Ko), 9.x.6/9.x.7 (journaliser rejets et succès) : un pare-feu qui bloque par défaut et qui trace est la base d'une défense réseau.

Preuve / vérification — Get-NetFirewallProfile → Inbound=Block, LogBlocked=True, 16384 sur les 3 profils.



```
TP12 - AUDIT AVANT | 2. Pare-feu Windows Defender
SRV-TP12 - Windows Server 2022 - CIS Benchmark v5.0.0

PS> Get-NetFirewallProfile | ft Name,Enabled,DefaultInboundAction,LogBlocked,LogMaxSizeKilobytes

[!] Domain Enabled=True Inbound=NotConfigured LogBlocked=False LogKB=4096
[!] Private Enabled=True Inbound=NotConfigured LogBlocked=False LogKB=4096
[!] Public Enabled=True Inbound=NotConfigured LogBlocked=False LogKB=4096
[~] Profils actifs, mais inbound NON force a Block et journalisation DESACTIVEE

CIS 9.1-9.3 : Inbound=Block, LogBlocked=Yes, Size=16384 KB
--- [Entree] section suivante ---

TP12 - APRES DURCISSEMENT | 2. Pare-feu Windows Defender
SRV-TP12 - Windows Server 2022 - CIS Benchmark v5.0.0

PS> Get-NetFirewallProfile | ft Name,DefaultInboundAction,LogBlocked,LogMaxSizeKilobytes

[OK] Domain Inbound=Block LogBlocked=True LogKB=16384
[OK] Private Inbound=Block LogBlocked=True LogKB=16384
[OK] Public Inbound=Block LogBlocked=True LogKB=16384

CIS 9.1-9.3 : Inbound=Block + journalisation 16384 KB -> CONFORME
--- [Entree] section suivante ---
```

Avant (rouge) : entrant non forcé, journalisation OFF, 4 Mo — Après (vert) : Block + logs 16 Mo sur les 3 profils.

4.3 — Microsoft Defender [CIS 18.10.42](#)

Le risque — L'antivirus tournait, mais la **protection contre les applications indésirables (PUA)** et la **protection réseau** (blocage des sites/IP malveillants) étaient désactivées : des vecteurs d'infection restaient ouverts.

Ce qu'on a fait — Activation de la protection PUA (blocage), de la protection réseau (blocage), et du cloud Microsoft MAPS en mode avancé.

Pourquoi CIS le recommande — 18.10.42.16 (PUA = Block), 18.10.42.6.3.1 (protection réseau = Block), 18.10.42.5.2 (MAPS Advanced) : ces options ferment des chemins d'attaque courants (logiciels parasites, sites de phishing/C2).

Preuve / vérification — Get-MpPreference → PUAProtection=1, EnableNetworkProtection=1. Capture après/03-defender.

4.4 — ASR (réduction de la surface d'attaque) [CIS 18.10.42.6.1](#)

Le risque — Sans règles ASR, les techniques d'attaque les plus courantes passent : macros Office qui lancent du code, exécution depuis une clé USB ou un mail, **vol d'identifiants depuis LSASS**, abus de outils système (LOLBins).

Ce qu'on a fait — Déploiement des **12 règles ASR recommandées en mode blocage**.

Pourquoi CIS le recommande — 18.10.42.6.1.1 (activer ASR) et 18.10.42.6.1.2 (fixer chaque règle) : chaque règle neutralise une technique offensive précise et documentée (mapping ATT&CK).

Preuve / verification — `(Get-MpPreference).AttackSurfaceReductionRules_Actions` → 12 valeurs à 1 (Block). Capture apres/04-asr.

4.5 — SMBv1 [CIS 18.4.2, 18.4.3](#)

Le risque — SMBv1 est un protocole de partage de fichiers **obsolète et vulnérable** — c'est le vecteur d'EternalBlue (WannaCry, NotPetya). Même inactif côté serveur, le composant restait présent.

Ce qu'on a fait — Désactivation du protocole côté serveur, désactivation du **pilote client**, et retrait du composant Windows SMBv1.

Pourquoi CIS le recommande — 18.4.2 (pilote client = Disable) et 18.4.3 (serveur = Disabled) : un protocole cassé sans usage moderne doit simplement disparaître.

Preuve / verification — `Get-WindowsOptionalFeature SMB1Protocol` → Disabled. Capture apres/06-smbv1.

4.6 — Journalisation PowerShell [CIS 18.10.88](#)

Le risque — PowerShell est l'outil favori des attaquants (scripts en mémoire, obfuscation). Sans journalisation, **aucune trace** de ce qui a été exécuté : la réponse à incident est aveugle.

Ce qu'on a fait — Activation du **Script Block Logging** (chaque bloc de code exécuté est enregistré, événement 4104) et de la **Transcription** (journal texte complet des sessions).

Pourquoi CIS le recommande — 18.10.88.1 et 18.10.88.2 : rendre PowerShell **traçable** transforme l'outil d'attaque préféré en source de preuves.

Preuve / verification — On tape une commande témoin, puis on la retrouve immédiatement dans le journal 4104. Capture apres/07-powershell-logging.

4.7 — Politique d'audit avancée [CIS 17.x + 2.3.2.1](#)

Le risque — Par défaut, des événements clés ne sont pas audités : **création de processus**, ouvertures de session, accès aux partages, périphériques amovibles. Sans eux, on ne peut ni détecter ni investiguer une intrusion.

Ce qu'on a fait — Activation d'une vingtaine de **sous-catégories d'audit** (succès/échec selon le cas) et forçage de la granularité par sous-catégorie.

Pourquoi CIS le recommande — 2.3.2.1 (forcer les sous-catégories) + 17.x (Credential Validation, Process Creation, Logon/Logoff, File Share, Removable Storage, Policy Change...) : ces journaux sont la matière première de toute détection.

Preuve / verification — `auditpol /get` montre les sous-catégories passées de « No Auditing » à « Success/Failure ». Capture apres/08-audit.

4.8 — Services inutiles (Print Spooler) [CIS 5.2](#)

Le risque — Le service d'impression **Print Spooler** était actif. C'est la faille **PrintNightmare** (exécution de code à distance / élévation de privilèges). Sur un serveur qui n'imprime pas, c'est une surface d'attaque gratuite.

Ce qu'on a fait — Arrêt et **désactivation** du service Spooler (et des services superflus présents).

Pourquoi CIS le recommande — 5.2 impose Spooler = Disabled sur un serveur membre : supprimer un service non nécessaire élimine sa classe entière de vulnérabilités.

Preuve / verification — Get-Service Spooler → Stopped / Disabled. Capture apres/09-services.

4.9 — RDP (Bureau à distance) [CIS 18.10.57.3](#)

Le risque — Le RDP est un point d'entrée d'administration très ciblé. Avec un chiffrement faible et sans durcissement, il expose aux interceptions et au vol de session.

Ce qu'on a fait — Chiffrement forcé au **niveau haut**, authentification **NLA** obligatoire, RPC sécurisé, prompt de mot de passe, et **redirection des lecteurs bloquée**.

Pourquoi CIS le recommande — 18.10.57.3.9.5 (chiffrement High), .9.4 (NLA), .9.3 (couche SSL), .9.2 (RPC sécurisé), .9.1 (prompt), 18.10.57.3.3.3 (pas de redirection de disque) : on garde le RDP utilisable mais sûr.

Preuve / verification — Registre TS : MinEncryptionLevel=3, UserAuthentication=1. Capture apres/10-rdp.

4.10 — WDigest [ex-CIS 18.4.8 \(retiré en v5.0.0\)](#)

Le risque — WDigest, s'il est activé, garde les **mots de passe en clair en mémoire** — un cadeau pour mimikatz. Non forcé explicitement, un attaquant peut le réactiver.

Ce qu'on a fait — Verrouillage explicite : UseLogonCredential = 0.

Pourquoi CIS le recommande — Point d'**honnêteté méthodologique** : cette recommandation était le CIS 18.4.8 jusqu'aux versions précédentes, mais elle a été **retirée en v5.0.0** car le défaut est sûr depuis 2012 R2. On l'a quand même forcée en défense en profondeur (le figer empêche sa réactivation).

Preuve / verification — Registre WDigest → UseLogonCredential=0. Capture apres/11-wdigest.

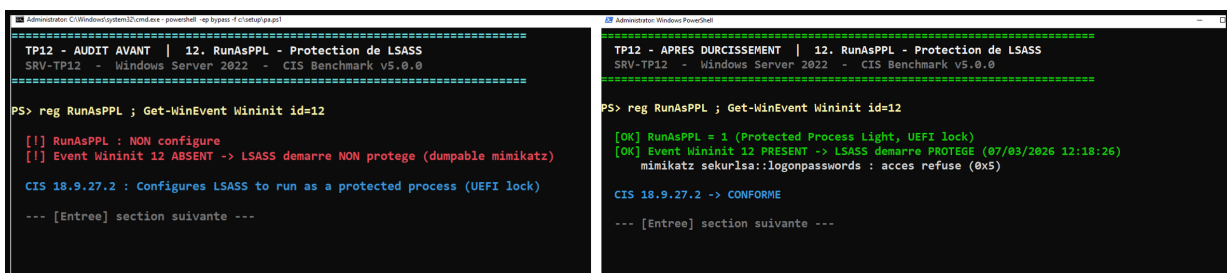
4.11 — RunAsPPL : protection de LSASS [CIS 18.9.27.2](#)

Le risque — C'est la mesure phare contre le vol d'identifiants. LSASS conserve en mémoire les secrets d'authentification (hashes, tickets Kerberos). Non protégé, un administrateur — ou un malware — peut vider sa mémoire avec mimikatz et usurper tous les comptes (pass-the-hash, mouvement latéral).

Ce qu'on a fait — Activation de **RunAsPPL** : LSASS démarre en **processus protégé (PPL)**, verrouillé par l'UEFI. Sa mémoire devient illisible, même pour un administrateur.

Pourquoi CIS le recommande — 18.9.27.2 (Enabled with UEFI Lock) : le verrou UEFI empêche un attaquant de simplement désactiver la protection par registre — elle résiste à la compromission.

Preuve / verification — Après reboot, l'**événement système Wininit 12** confirme que LSASS a démarré protégé ; une tentative de dump renvoie « accès refusé » (0x5), doublée par une règle ASR.



```
==== TP12 - AUDIT AVANT | 12. RunAsPPL - Protection de LSASS
SRV-TP12 - Windows Server 2022 - CIS Benchmark v5.0.0
=====
PS> reg RunAsPPL ; Get-WinEvent Wininit id=12

[!] RunAsPPL : NON configure
[!] Event Wininit 12 ABSENT -> LSASS démarre NON protege (dumpable mimikatz)

CIS 18.9.27.2 : Configure LSASS to run as a protected process (UEFI lock)
--- [Entree] section suivante ---

==== TP12 - APRES DURCISSEMENT | 12. RunAsPPL - Protection de LSASS
SRV-TP12 - Windows Server 2022 - CIS Benchmark v5.0.0
=====
PS> reg RunAsPPL ; Get-WinEvent Wininit id=12

[OK] RunAsPPL = 1 (Protected Process Light, UEFI lock)
[OK] Event Wininit 12 PRESENT -> LSASS démarre PROTEGE (07/03/2026 12:18:26)
mimikatz sekurlsa:logonpasswords : acces refuse (0x5)

CIS 18.9.27.2 -> CONFORME
--- [Entree] section suivante ---
```

Avant : LSASS dumpable (mimikatz). Après : RunAsPPL=1, Event 12 présent, dump refusé.

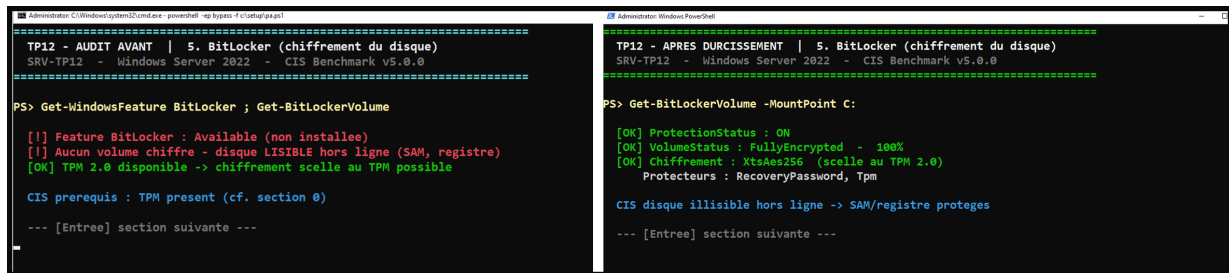
4.12 — BitLocker : chiffrement du disque Exigence du TP (bonne pratique)

Le risque — Sans chiffrement, un vol de la machine (ou du disque, ou du fichier de la VM) donne un accès **hors ligne** à la base de comptes SAM et au registre : les secrets peuvent être extraits tranquillement.

Ce qu'on a fait — Chiffrement du volume système en **XTS-AES 256 bits**, clé **scellée au TPM 2.0**, plus un mot de passe de récupération sauvegardé.

Pourquoi CIS le recommande — BitLocker n'est pas une recommandation L1 « automatisée » simple du CIS (le benchmark traite surtout la *configuration* de BitLocker) : c'est une **exigence explicite du TP**, appliquée selon les bonnes pratiques (algorithme fort, scellement TPM).

Preuve / vérification — `Get-BitLockerVolume` → FullyEncrypted, ProtectionStatus On, XTS-AES 256, 100 %.



The image shows two side-by-side screenshots of Windows PowerShell command prompts. The left window, titled 'Administration: C:\Windows\system32\cmd.exe - powershell - up bypass / c:\setup\ga.ps1', displays the output of 'Get-WindowsFeature BitLocker' and 'Get-BitLockerVolume'. It shows that BitLocker is available but not installed, and that the disk is currently unencrypted and visible to anyone with physical access. The right window, titled 'Administration: Windows PowerShell', shows the output of 'Get-BitLockerVolume -MountPoint C:'. It indicates that the volume is now fully encrypted (100%), the protection status is 'On', and the encryption method is 'XtsAes256' (sealed to TPM 2.0). The protectors listed are 'RecoveryPassword' and 'Tpm'.

```
TP12 - AUDIT AVANT | 5. BitLocker (chiffrement du disque)
SRV-TP12 - Windows Server 2022 - CIS Benchmark v5.0.0

PS> Get-WindowsFeature BitLocker ; Get-BitLockerVolume

[!] Feature BitLocker : Available (non installée)
[!] Aucun volume chiffré - disque LISIBLE hors ligne (SAM, registre)
[OK] TPM 2.0 disponible -> chiffrement scelle au TPM possible

CIS prerequisite : TPM present (cf. section 0)
--- [Entree] section suivante ---

TP12 - APRES DURCISSEMENT | 5. BitLocker (chiffrement du disque)
SRV-TP12 - Windows Server 2022 - CIS Benchmark v5.0.0

PS> Get-BitLockerVolume -MountPoint C:

[OK] ProtectionStatus : ON
[OK] VolumeStatus : FullyEncrypted - 100%
[OK] Chiffrement : XtsAes256 (scelle au TPM 2.0)
Protecteurs : RecoveryPassword, Tpm

CIS disque illisible hors ligne -> SAM/registre proteges
--- [Entree] section suivante ---
```

Avant : disque en clair. Après : chiffré 100 %, scellé au TPM, protection active.

4.13 — VBS / Credential Guard CIS 18.9.5 — « si possible »

Le risque — VBS (sécurité par virtualisation) isole les secrets LSASS dans un **enclave protégé par l'hyperviseur** : même RunAsPPL contourné, Credential Guard empêche l'extraction des identifiants.

Ce qu'on a fait — Réglages VBS/Credential Guard/HVCI posés (registre DeviceGuard + LsaCfgFlags), testés dans **deux variantes** (stricte avec HVCI + UEFI lock, et prudente sans HVCI).

Pourquoi CIS le recommande — 18.9.5.1 à 18.9.5.7 : c'est la protection la plus avancée contre le vol d'identifiants — le sujet la demande « si possible ».

Preuve / vérification — **Limite constatée** : dans les deux modes, la VM **fige au firmware au démarrage** (0 octet d'I/O disque) : l'hyperviseur VBS n'est pas stable en **virtualisation imbriquée**. Configuration correcte, activable sur matériel physique ; documentée comme limite d'environnement (rollback effectué). Détaillé au §5.

5. Analyse des limites (à assumer devant le jury)

VBS / Credential Guard non activable — En activant VBS, la VM se bloque au firmware OVMF, sans aucune activité disque, avant même le logo Windows. Cause : notre serveur est une **machine virtuelle imbriquée** (une VM dans un hyperviseur KVM) ; le lancement de l'hyperviseur de sécurité de Windows n'y est pas fiable. Ce n'est **pas une erreur de configuration** — les mêmes réglages fonctionneraient sur un poste physique. Le sujet prévoit d'ailleurs ce cas (« si possible »). On a testé deux variantes, constaté le blocage, et restauré proprement l'état durci via snapshot.

Tamper Protection (Defender) — La protection anti-sabotage de Defender ne s'active pas par script ou registre sur une machine hors gestion centralisée (MDM/Intune) : elle est justement auto-protégée. On a activé à la place PUA et protection réseau.

Durcir n'est pas détecter — On produit désormais des journaux (PowerShell, audit, pare-feu), mais ils ne servent que s'ils sont **collectés et corrélés** dans un SIEM. L'étape suivante logique serait leur centralisation (ex. Wazuh/ELK).

Périmètre local — Il s'agit d'un durcissement **local** (machine autonome). En entreprise, ces réglages passeraient par des GPO de domaine et seraient complétés (LAPS, tiering administrateur, délégation).

6. Conclusion

Une installation Windows Server par défaut cumulait des faiblesses critiques : LSASS exposé, aucune traçabilité, Print Spooler et SMBv1 actifs, disque en clair. En appliquant méthodiquement le **CIS Benchmark v5.0.0**, on a durci **12 des 13 domaines** et **prouvé chacun techniquement**, avant et après : le vol d'identifiants via LSASS est bloqué (RunAsPPL, prouvé par l'événement 12 et le refus de dump), le disque est chiffré (BitLocker XTS-AES 256), la surface est réduite (Spooler et SMBv1 supprimés), l'activité est journalisée, et le pare-feu filtre.

La seule mesure non aboutie — **VBS / Credential Guard** — l'est pour une raison d'**environnement** (virtualisation imbriquée), pas de configuration : prévue « si possible » par le sujet, testée dans deux variantes, et documentée avec sa preuve. **Bilan : 12/13 durcis et prouvés, 1/13 limite d'environnement assumée.**

Annexe — Correspondance élément ↔ CIS (synthèse)

Élément	Réf. CIS v5.0.0	Cible
Comptes / mots de passe	1.1.1-7 , 1.2.1-4 , 2.3.1.3/.4 , 2.3.11.7	mdp 14+compl., lockout 5, admin renommé, NTLMv2
Pare-feu (3 profils)	9.1.x / 9.2.x / 9.3.x	Inbound Block + journalisation 16 Mo
Defender	18.10.42.16 / .6.3.1 / .5.2	PUA + Protection réseau + MAPS
ASR	18.10.42.6.1.1 / .6.1.2	12 règles en Block
SMBv1	18.4.2 / 18.4.3	client + serveur désactivés
PowerShell logging	18.10.88.1 / 18.10.88.2	Script Block + Transcription
Audit avancé	2.3.2.1 + 17.x	~20 sous-catégories activées
Services (Spooler)	5.2	Print Spooler = Disabled
RDP	18.10.57.3.9.1-5 + .3.3.3	High + NLA + Secure RPC
WDigest	ex-18.4.8 (retiré v5.0.0)	UseLogonCredential = 0 (défense en profondeur)
RunAsPPL	18.9.27.2	Enabled with UEFI Lock (prouvé Event 12)
BitLocker	exigence TP (config CIS 18.10.x)	XTS-AES 256, scellé TPM
VBS / Credential Guard	18.9.5.1-7	posé, non activable (nested virt) — limite

Livrables associés : rapport (RAPPORT.md), présentation (TP12-durcissement-windows.pptx), captures avant/après, scripts d'audit et de durcissement, script vidéo. Référentiel : CIS Microsoft Windows Server 2022 Benchmark v5.0.0.