DOCUMENTATION TECHNIQUE

Automatisation du durcissement Windows selon le guide DGA-MI et le CIS Benchmark

Audit, remédiation automatisée, enrichissement des règles et validation de conformité

Objet du document
Présenter l'évolution d'un script PowerShell d'audit en un outil de remédiation automatisée, capable de vérifier puis d'appliquer des règles issues du guide DGA-MI et du CIS Benchmark Windows 11.

Version	1.0
Type	Compte rendu technique et validation
Périmètre	Poste Windows 11 isolé / machine virtuelle
Référentiels	Guide DGA-MI Windows 11 - CIS Benchmark Windows 11 L1

1. Synthèse

Le guide DGA-MI contient un nombre important de règles de durcissement. Dans ce contexte, le script a été conçu comme une preuve de concept ciblée, puis progressivement enrichi pour devenir un outil modulaire d'audit et de remédiation.

L'approche retenue repose sur deux modes de fonctionnement : un mode Audit, qui vérifie l'état du poste sans modifier la configuration, et un mode Apply, qui applique automatiquement les mesures de durcissement avant de générer un rapport de conformité.

> **Principe directeur**
> Le script reste évolutif : de nouvelles règles peuvent être ajoutées progressivement à l'aide de cmdlets PowerShell comme Get-ItemProperty, Set-ItemProperty, Get-Service, Stop-Service ou Set-NetFirewallProfile.

2. Évolution fonctionnelle du script

Étape	Objectif	Mécanisme technique	Résultat attendu
PoC d'audit	Contrôler un échantillon de règles critiques	Lecture registre, services et paramètres système	Rapport de conformité initial
Mode Apply	Automatiser la remédiation	Paramètre [switch]$Apply et commandes correctives	Bascule des indicateurs en conforme
Profil complet	Intégrer les profils Minimal et Toutes les règles	Clés de registre avancées et fonctions utilitaires	Durcissement plus strict
Chapitres avancés	Couvrir pare-feu, ASR et services	Set-NetFirewallProfile, règles Defender, désactivation services	Conformité sur règles sensibles
CIS Benchmark	Croiser DGA-MI et référentiel international	Colonnes ANSSI / CIS dans le reporting HTML	Conformité globale multi-référentiels

3. Mode Audit et remédiation automatique

La première évolution majeure a consisté à transformer le script d'audit en outil de remédiation. Le paramètre conditionnel -Apply permet de choisir entre une vérification passive et une correction automatique des paramètres ciblés.

```
.\script.ps1        # Mode Audit : vérification sans modification
.\script.ps1 -Apply   # Mode Apply : application des durcissements puis rapport
```

1. Audit initial sur une machine Windows 11 vierge afin d'identifier les écarts de conformité.
2. Application du durcissement avec le paramètre -Apply.
3. Audit de contrôle pour confirmer que les indicateurs sont passés à l'état conforme.

durcissement evolue.

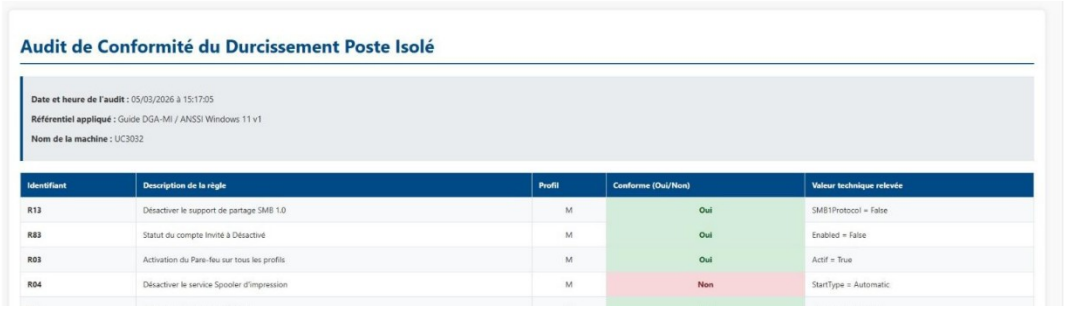


Figure 1 - Exemple de rapport d'audit initial et contexte de remédiation automatisée.

4. Enrichissement du profil de durcissement

Le script a ensuite été enrichi afin d'intégrer non seulement le profil Minimal, mais également les restrictions du profil « Toutes les règles ». Cette évolution permet de pousser le poste vers un niveau de durcissement plus exigeant.

- Désactivation de l'exécution automatique des médias amovibles avec NoDriveTypeAutoRun.
- Interdiction de la résolution de noms locale LLMNR.
- Renforcement du contrôle de compte utilisateur UAC.
- Création automatique des arborescences de registre manquantes avant écriture des valeurs.

> **Validation**
> Le protocole de validation repose sur une machine virtuelle Windows 11 restaurée à l'état vierge, puis auditée avant et après application du script. Le rapport final confirme la conformité des règles testées.

. Non).

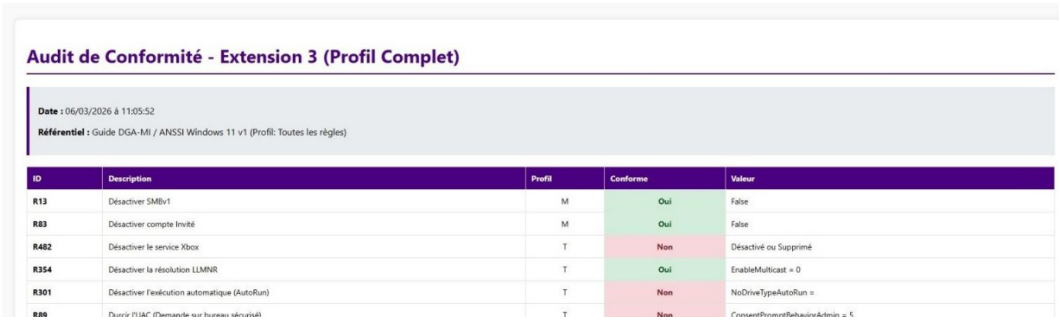


Figure 2 - Exemple d'audit initial sur profil complet, avant remédiation.

5. Intégration des chapitres avancés du guide DGA-MI

L'outil a été complété par l'intégration de règles issues des chapitres 6, 7 et 9 du guide. Ces chapitres concernent notamment le pare-feu Windows, Microsoft Defender Exploit Protection et la gestion des services.

Chapitre	Règles	Mesures appliquées	Exemples techniques
6 - Pare-feu Windows	R188 / R189	Blocage par défaut des flux entrants et sortants sur les profils Domaine, Privé et Public.	InboundAction / OutboundAction bloquées
7 - Defender Exploit	R216 / R217 / R220 / R221	Activation de règles ASR pour	Protection lsass.exe, pilotes

Protection		réduire la surface d'attaque.	vulnérables, outils système copiés
9 - Gestion des services	R408 / R411 / R412 / R413	Désactivation de services inutiles ou vulnérables.	UserDataSvc, iphlpsvc, wlidsvc, CaptureService

vulnérables listés dans le référentiel, notamment la désactivation forcée des services *UserDataSvc* (**R408**), *iphlpsvc* (**R411**), *wlidsvc* (**R412**) et *CaptureService* (**R413**).

ID	Titre de la règle (Conforme au PDF)	Chapitre	Conforme	Valeur technique
R188	Bloquer par défaut tous les flux entrants pour les profils public, privé et de domaine	Chap 6.1	**Oui**	InboundAction bloquée
R189	Bloquer par défaut tous les flux sortants pour les profils public, privé et de domaine	Chap 6.1	**Oui**	OutboundAction bloquée
R216	Activer le mécanisme (...) Bloquer le vol d'informations d'identification (lsass.exe)	Chap 7.2	**Oui**	Etat ASR: 1
R217	Activer le mécanisme (...) Bloquer l'utilisation abusive des pilotes signés vulnérables	Chap 7.2	**Oui**	Etat ASR: 1
R220	Activer le mécanisme (...) Empêcher le redémarrage en mode Sans échec	Chap 7.2	**Oui**	Etat ASR: 1
R221	Activer le mécanisme (...) Bloquer l'utilisation des outils système copiés	Chap 7.2	**Oui**	Etat ASR: 1
R408	Désactiver le service Accès aux données utilisateurs	Chap 9.2	**Oui**	Disabled
R411	Désactiver le service Assistance IP	Chap 9.2	**Oui**	Disabled

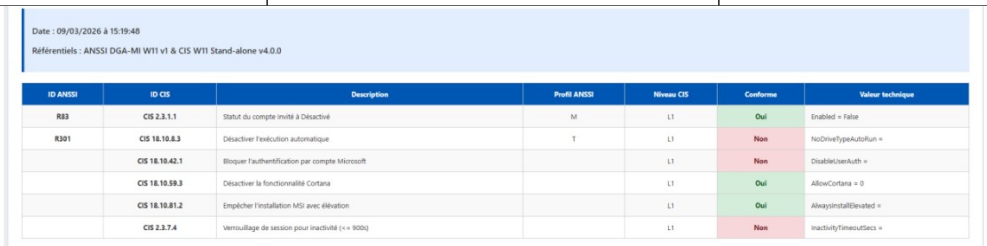
Figure 3 - Tableau de validation des règles avancées DGA-MI : pare-feu, ASR et services.

6. Couplage avec le CIS Benchmark Windows 11

Afin de compléter le cadre national par une référence internationale, le script a été enrichi avec des recommandations issues du CIS Benchmark Windows 11 Stand-alone, en se concentrant sur le niveau 1, adapté à un durcissement standard.

- Ajout d'une matrice de reporting distinguant les règles ANSSI, les règles CIS et les règles communes.
- Validation simultanée de la désactivation du compte Invité pour les exigences ANSSI R83 et CIS 2.3.1.1.
- Ajout de règles CIS dédiées à la confidentialité et au verrouillage comportemental.

Référence CIS	Objectif	Type de durcissement
CIS 18.8.21.2	Désactiver l'ID publicitaire	Confidentialité
CIS 18.8.20.1.1	Désactiver Cortana	Réduction des services et collecte
CIS 18.4.1	Restreindre les privilèges d'installation MSI	Contrôle des installations
CIS 2.3.7.4	Limiter le verrouillage automatique à 900 secondes	Sécurité de session


Date : 09/03/2026 à 15:19:48
Référentiels : ANSSI DGA-MI W11 v1 & CIS W11 Stand-alone v4.0.0

ID ANSSI	ID CIS	Description	Profil ANSSI	Niveau CIS	Conforme	Valeur technique
R83	CIS 2.3.1.1	Statut du compte invité à Désactivé	M	L1	Oui	Enabled = False
R301	CIS 18.10.8.3	Désactiver l'exécution automatique	T	L1	Non	NoDriveTypeAutoRun =
	CIS 18.10.42.1	Bloquer l'authentification par compte Microsoft		L1	Non	DisableUserAuth =
	CIS 18.10.59.3	Désactiver la fonctionnalité Cortana		L1	Oui	AllowCortana = 0
	CIS 18.10.81.2	Empêcher l'installation MSI avec élévation		L1	Oui	AlwaysInstallElevated =
	CIS 2.3.7.4	Verrouillage de session pour inactivité (<= 900s)		L1	Non	InactivityTimeoutSecs =

Le lancement avec paramètre (.\extension5.ps1 -Apply) a fusionné le durcissement de l'ANSSI et du CIS.

L'audit final a certifié une conformité globale (verte) sur les deux référentiels couplés.

Figure 4 - Exemple de rapport croisé ANSSI / CIS après intégration du référentiel CIS.

7. Protocole de validation global

4. Restaurer une machine virtuelle Windows 11 vierge.
5. Exécuter le script en mode Audit pour produire un état initial de conformité.
6. Relancer le script avec le paramètre -Apply afin d'appliquer les durcissements.
7. Exécuter un audit final pour vérifier la bascule des indicateurs en conformité.
8. Comparer les résultats ANSSI et CIS dans le rapport HTML généré.

8. Bilan

Cette évolution démontre qu'un environnement Windows peut être audité puis durci de façon industrielle, depuis un état vierge jusqu'à une configuration fortement sécurisée. La modularité du script permet d'ajouter progressivement de nouvelles règles, sans remettre en cause l'architecture existante.

> **Conclusion**
> Le script constitue une base solide pour standardiser l'application du guide DGA-MI et l'enrichir avec le CIS Benchmark. Avant tout déploiement à grande échelle, il reste recommandé de valider les effets sur les applications métiers afin d'éviter toute régression fonctionnelle.