DOCUMENTATION TECHNIQUE

Qualification des outils Microsoft et open-source pour le durcissement Windows

Security Compliance Toolkit - Policy Analyzer - LGPO.exe - HardeningKitty

Objet du document
Présenter, qualifier et comparer plusieurs outils de durcissement Windows, puis valider leur efficacité à l'aide d'un contre-audit réalisé avec l'IHM d'audit interne.

Version	1.0
Type	Qualification technique et retour d'expérience
Périmètre	Poste Windows 11 / durcissement local
Auteur	Kevin

1. Synthèse

Cette documentation présente deux familles d'outils permettant d'auditer et d'appliquer des règles de durcissement sur un poste Windows : les outils officiels Microsoft fournis dans le Security Compliance Toolkit, et l'outil open-source HardeningKitty.

L'objectif est de comprendre leur apport, leur méthode d'utilisation, leurs limites, puis de vérifier concrètement les effets du durcissement grâce à un contre-audit réalisé avec l'IHM d'audit développée en interne.

> **Point important**
> Ces outils permettent d'industrialiser le durcissement, mais leur utilisation massive peut provoquer un effet « boîte noire ». Une validation règle par règle reste indispensable avant un déploiement large.

2. Outils étudiés

Outil	Éditeur / origine	Usage principal	Atout clé
Microsoft Security Compliance Toolkit	Microsoft	Analyser et appliquer les Security Baselines	Référentiel officiel et maintenu
Policy Analyzer	Microsoft	Comparer l'état d'une machine ou de GPO avec une baseline	Lecture visuelle des écarts
LGPO.exe	Microsoft	Injecter localement des stratégies de groupe	Application propre via registry.pol
HardeningKitty	Communauté open-source	Auditer et appliquer des règles CIS via PowerShell	Score global et sauvegarde intégrée

3. Microsoft Security Compliance Toolkit

Le Microsoft Security Compliance Toolkit 1.0 est une suite gratuite d'outils Microsoft destinée aux administrateurs. Elle permet de télécharger, analyser, tester et appliquer les Security Baselines recommandées pour Windows et certaines applications Microsoft, comme Office ou Edge.

3.1 Apports par rapport à un script personnalisé

- Exhaustivité : les baselines Microsoft couvrent plusieurs centaines de paramètres de sécurité.
- Mise à jour : les référentiels suivent les nouvelles versions de Windows 11, par exemple 24H2 ou 25H2.
- Lisibilité : Policy Analyzer facilite la comparaison graphique entre la configuration réelle et la référence.
- Application propre : LGPO.exe modifie les stratégies locales via registry.pol, ce qui rend les paramètres visibles dans gpedit.msc.

3.2 Préparation des éléments

Les archives officielles doivent être téléchargées puis extraites localement :

- Windows 11 Security Baseline.zip
- PolicyAnalyzer.zip
- LGPO.zip

4. Analyse des écarts avec Policy Analyzer

Policy Analyzer est exécuté avec les privilèges administrateur afin de comparer la configuration actuelle du poste avec la baseline Microsoft. Cette étape permet d'éviter un durcissement aveugle et d'identifier précisément les paramètres à corriger.

4.1 Déroulement de l'audit comparatif

- Importer la baseline via le bouton Add en sélectionnant les dossiers GPOs extraits.
- Cocher les éléments importés afin de compiler les règles dans une matrice de comparaison.
- Analyser les différences entre les recommandations Microsoft et l'état réel de la machine.

4.2 Interprétation du code couleur

Couleur	Signification	Action à envisager
Gris	Conformité parfaite : le paramètre recommandé est déjà appliqué.	Aucune action requise.
Jaune	Conflit de valeur : le paramètre existe, mais sa valeur diffère de la recommandation.	Vérifier le risque et corriger si nécessaire.
Blanc	Non configuré : la baseline attend une restriction absente de la machine.	Prioriser l'analyse, car cela peut révéler une faille importante.

> **Avantage technique**
> Un clic sur une ligne jaune ou blanche affiche le chemin exact de la GPO ou de la clé de registre concernée, par exemple HKLM\Software\Policies\...

5. Application de la baseline avec LGPO.exe

Pour appliquer globalement le durcissement Microsoft, la baseline Windows 11 est injectée dans la stratégie locale du poste à l'aide de LGPO.exe lancé en administrateur.

```
.\LGPO.exe /g "C:\Chemin\Vers\Windows 11 Security Baseline\GPOs"
```

LGPO.exe parse les fichiers .pol et les injecte dans la stratégie de sécurité locale. Après redémarrage, la machine est alignée sur le standard entreprise recommandé par Microsoft.

6. HardeningKitty

HardeningKitty est un outil open-source PowerShell spécialisé dans l'audit et l'application de recommandations de durcissement Windows. Il s'appuie sur des référentiels stricts, notamment les CIS Benchmarks.

6.1 Points forts

- Mode Audit : évaluation de la posture de sécurité sans modification du système.
- Mode HailMary : application massive des recommandations présentes dans le fichier de règles.
- Sauvegarde intégrée : possibilité d'exporter les valeurs avant modification grâce à l'option -Backup.
- Scoring : attribution d'une note globale permettant de mesurer l'amélioration après durcissement.

6.2 Préparation de l'environnement PowerShell

```
Get-ChildItem -Recurse | Unblock-File
Set-ExecutionPolicy Bypass -Scope Process -Force
Import-Module .\HardeningKitty.psm1
```

7. Audit et durcissement avec HardeningKitty

7.1 Audit initial

L'audit initial permet de mesurer l'état du poste avant modification. Le script génère un rapport détaillé et attribue un score de départ.

```
Invoke-HardeningKitty -Mode Audit -Log -Report -FileFindingList .\lists\finding_list_0x6d69636b_machine.csv
```

7.2 Application du durcissement

Le mode HailMary applique les recommandations du fichier CSV dans la base de registre. L'option -Backup permet de conserver une sauvegarde avant modification.

```
Invoke-HardeningKitty -Mode HailMary -Log -Report -Backup -FileFindingList .\lists\finding_list_0x6d69636b_machine.csv
```

> **Attention**
> Le mode HailMary est puissant et doit être utilisé avec prudence. Avant tout déploiement en production, il est recommandé de tester sur une machine isolée ou une VM.

8. Interprétation du HardeningKitty Score

HardeningKitty utilise une échelle de score allant de 1.0 à 6.0. Cette note tient compte de la criticité des contrôles validés ou non validés.

Résultat du contrôle	Points attribués	Interprétation
Passed	4	Contrôle conforme
Low	2	Écart mineur
Medium	1	Écart moyen
High	0	Écart critique

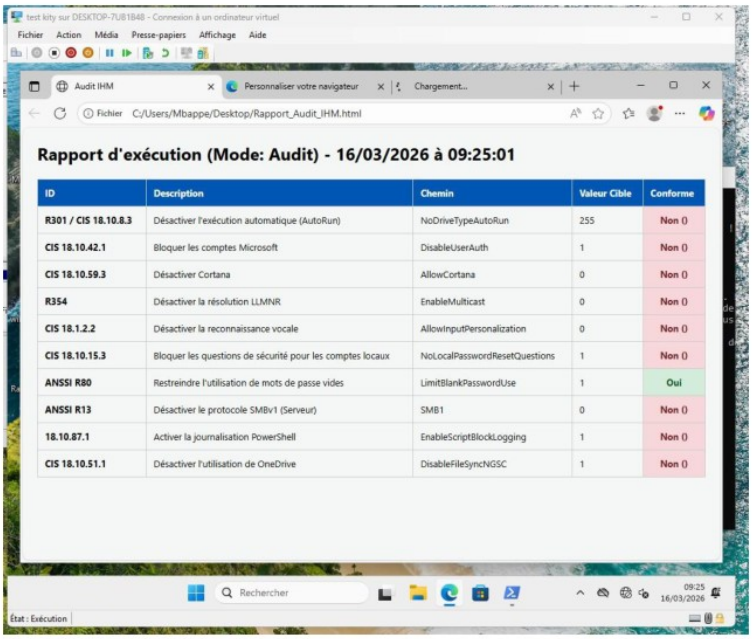
> **Formule de calcul**
> Score = (Points obtenus / Points maximum possibles) x 5 + 1. Un score inférieur à 4.0 est insuffisant, entre 4.0 et 5.0 il est suffisant, et proche de 6.0 il est excellent.

Dans le cas étudié, le score de 5.96 après durcissement, avec 413 contrôles validés sur 418, démontre un niveau de conformité très élevé au regard des exigences CIS.

9. Validation croisée avec l'IHM d'audit interne

Pour vérifier l'effet réel du durcissement, l'IHM d'audit interne a été exécutée avant et après l'application de HardeningKitty. Cette comparaison permet de confirmer que les clés de registre suivies par l'outil interne ont bien été corrigées.

Moment du contrôle	Constat	Conclusion
Avant durcissement	Plusieurs règles ciblées apparaissent non conformes.	La machine nécessite un durcissement.
Après durcissement	La majorité des règles surveillées passent au vert avec le statut « Oui ».	Le durcissement est techniquement validé.



Après durcissement : Le contre-audit via notre IHM démontre que l'outil industriel a parfaitement corrigé les clés de registre surveillées. L'interface s'affiche en vert ("Oui" conforme), validant le succès technique de la manipulation globale.

Rapport d'exécution (Mode: Audit) - 16/03/2026 à 09:52:46

ID	Description	Chemin	Valeur Cible	Conforme
R301 / CIS 18.10.8.3	Désactiver l'exécution automatique (AutoRun)	NoDriveTypeAutoRun	255	Oui
CIS 18.10.42.1	Bloquer les comptes Microsoft	DisableUserAuth	1	Non ()
CIS 18.10.59.3	Désactiver Cortana	AllowCortana	0	Oui
R354	Désactiver la résolution LLMNR	EnableMulticast	0	Oui
CIS 18.1.2.2	Désactiver la reconnaissance vocale	AllowInputPersonalization	0	Oui
CIS 18.10.15.3	Bloquer les questions de sécurité pour les comptes locaux	NoLocalPasswordResetQuestions	1	Oui
ANSSI R80	Restreindre l'utilisation de mots de passe vides	LimitBlankPasswordUse	1	Oui
ANSSI R13	Désactiver le protocole SMBv1 (Serveur)	SMB1	0	Oui
18.10.87.1	Activer la journalisation PowerShell	EnableScriptBlockLogging	1	Oui
CIS 18.10.51.1	Désactiver l'utilisation de OneDrive	DisableFileSyncNGSC	1	Oui

Conclusion sur l'industrialisation du durcissement

Illustration issue du cas de test : comparaison du rapport IHM avant et après durcissement.

10. Conclusion

L’étude conjointe du Microsoft Security Compliance Toolkit et de HardeningKitty montre qu’il existe des solutions robustes pour automatiser la sécurisation d’un poste Windows. Ces outils accélèrent fortement l’audit, l’application des recommandations et la mesure de conformité.

Cependant, leur puissance impose une phase de validation. Un durcissement appliqué massivement peut modifier des paramètres sensibles et perturber certaines applications métiers. Le script PowerShell développé en interne, accompagné de son IHM d’audit, conserve donc un intérêt majeur : il permet une approche maîtrisée, pédagogique et granulaire, règle par règle.

> **Conclusion opérationnelle**
> Les outils industriels sont pertinents pour accélérer le durcissement, mais l’IHM interne reste indispensable pour contrôler, expliquer et sécuriser les changements appliqués.