Sécurisation du poste de travail

AGENCEE

REDACTION & VALIDATION

pour la relation commerciale

Francis DELPORT
Directeur

mob. : +33 (0) 6 18 16 87 63
e-mail : fdelport@agencee.fr

pour la relation commerciale

pour la relation commerciale

HISTORIQUE DES EVOLUTIONS

Version	date	paragraphe	action	nature de l'évolution
000	17/06/2020	Tous	C	Création du document

SOMMAIRE

S

1. INTRODUCTION 7

2. LES PREMIERES PRIORITES. 8

2.1. Renforcement des applications 8

2.2. Versions et correctifs d'application 9

2.3. Liste blanche des applications 9

2.4. Réduction de la surface d'attaque 12

2.5. Mise en cache des informations d'identification 13

2.6. Accès contrôlé aux dossiers 15

2.7. Saisie des informations d'identification 15

2.8. Antimalware à lancement précoce 16

2.9. Elévation de privilèges 16

2.10. Protection contre les exploits 17

2.11. Compte des administrateurs locaux 18

2.12. Mesures au niveau du BOOT System 19

2.13. Microsoft Edge 19

2.14. Multi-facteur d'authentification 20

2.15. Operating system architecture 20

2.16. Operating system patching 20

2.17. Version du système d'exploitation 21

2.18. La politique des mots de passe 22

2.19. Restreindre les comptes privilégiés 22

2.20. Secure Boot 22

3. LES PRIORITES MOYENNES 23

3.1. Politique de verrouillage de compte 23

3.2. Connections anonymes 23

3.3. Logiciel Antivirus 24
3.4. Gestionnaire de pièces jointes 25
3.5. Gérer les événements d'audit 26
3.6. Autoplay and AutoRun 28
3.7. BIOS and UEFI passwords 28
3.8. Boot devices 28
3.9. Bridging networks 28
3.10. Comptes invités intégrés 29
3.11. CD burner access 29
3.12. Centralised audit event logging 30
3.13. Command Prompt 30
3.14. Direct Memory Access 30
3.15. Endpoint device control 31
3.16. Partage de fichiers et d'imprimantes 32
3.17. Group Policy processing 32
3.18. Hard drive encryption 33
3.19. Installation des applications et des drivers 35
3.20. Listes héritées et à exécution unique 36
3.21. Comptes Microsoft 36
3.22. MSS settings 37
3.23. NetBIOS over TCP/IP 38
3.24. Network authentication 38
3.25. NoLMHash policy 38
3.26. Operating system functionality 39
3.27. Gestion de l'alimentation 39
3.28. PowerShell 40
3.29. Outils d'édition de la base de registre 40
3.30. Remote Assistance 40
3.31. Remote Desktop Services 41

3.32. Remote Procedure Call 42
3.33. Reporting system information 42
3.34. Safe Mode 43
3.35. Secure channel communications 43
3.36. Security policies 44
3.37. Server Message Block sessions 45
3.38. Verrouillage des sessions 45
3.39. Software-based firewalls 46
3.40. Sound Recorder 47
3.41. Standard Operating Environment 47
3.42. System backup and restore 47
3.43. System cryptography 48
3.44. User rights policies 48
3.45. Virtualised web and email access 49
3.46. Web Proxy Auto Discovery protocol 49
3.47. Windows Remote Management 49
3.48. Windows Remote Shell access 50
3.49. Windows Search and Cortana 50
3.50. Windows To Go 51

4. PRIORITES FAIBLES 52
4.1. Displaying file extensions 52
4.2. File and folder security properties 52
4.3. Location awareness 52
4.4. Microsoft Store 53
4.5. Resultant Set of Policy reporting 53

1. INTRODUCTION

Les stations de travail sont souvent ciblées par un adversaire utilisant des pages Web malveillantes, des e-mails avec des pièces jointes malveillantes et des supports amovibles avec du contenu malveillant dans le but d'extraire des informations sensibles.

Le renforcement des postes de travail est un élément important de la réduction de ce risque.

Ce document fournit des conseils sur le renforcement des postes de travail à l'aide des éditions Entreprise et Éducation de Microsoft Windows 10 version 1709.

Certains paramètres de stratégie de groupe utilisés dans ce document peuvent ne pas être disponibles ou compatibles avec Professional, Home ou S éditions de Microsoft Windows 10 version 1709.

Bien que ce document se réfère aux postes de travail, la plupart des paramètres de stratégie de groupe sont également applicables aux serveurs (à l'exception des contrôleurs de domaine) utilisant Microsoft Windows Server, version 1709 ou Microsoft Windows Server 2016.

Les noms et emplacements des paramètres de stratégie de groupe utilisés dans ce document sont issus de Microsoft Windows 10 version 1709; certaines différences existent pour les versions antérieures de Microsoft Windows.

Avant de mettre en œuvre les recommandations dans ce document, des tests approfondis doivent être entrepris pour s'assurer que le potentiel d'impacts négatifs involontaires sur les processus métier est réduit autant que possible.

Ce document est destiné aux technologies de l'information et à la sécurité de l'information.

Les professionnels au sein des organisations qui souhaitent entreprendre des évaluations des risques ou des vulnérabilités ainsi que ceux qui souhaitent développer un environnement d'exploitation standard renforcé pour les postes de travail.

2. LES PREMIERES PRIORITES.

Les contrôles de sécurité suivants, classés par ordre alphabétique, sont considérés comme ayant une excellente efficacité et doivent être traités comme des priorités élevées lors du renforcement des postes de travail Microsoft Windows 10 version 1709.

2.1. Renforcement des applications

Lorsque les applications sont installées, elles ne sont souvent pas préconfigurées dans un état sécurisé.

Par défaut, de nombreuses applications activent une fonctionnalité qui n'est requise par aucun utilisateur, tandis que la fonctionnalité de sécurité intégrée peut être désactivée ou définie à un niveau de sécurité inférieur.

Par exemple, Microsoft Office par défaut permet aux macros non approuvées dans les documents Office de s'exécuter automatiquement sans interaction avec l'utilisateur.

Pour réduire ce risque, les applications doivent avoir toutes les fonctionnalités de sécurité intégrées activées et configurées de manière appropriée ainsi que les fonctionnalités non requises désactivées.

Ceci est particulièrement important pour les applications clés telles que les suites de productivité bureautique (par exemple Microsoft Office), les lecteurs PDF (par exemple Adobe Reader), les navigateurs Web (par exemple Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome), les plug-ins de navigateur Web courants (par exemple Adobe Flash) , les clients de messagerie (Microsoft Outlook) et les plates-formes logicielles (par exemple Oracle Java Platform et Microsoft .NETFramework).

En outre, les fournisseurs peuvent fournir des conseils sur la configuration sécurisée de leurs produits.

Par exemple, Microsoft fournit des références de sécurité pour leurs produits sur leur blog Microsoft Security Guidance.

Dans de tels cas, les instructions du fournisseur doivent être suivies pour faciliter la configuration sécurisée de leurs produits.

2.2. Versions et correctifs d'application

Bien que certains fournisseurs puissent publier de nouvelles versions d'application pour remédier aux failles de sécurité, d'autres peuvent publier des correctifs (Patchs).

Si de nouvelles versions d'application et/ou des correctifs pour les applications ne sont pas installés, cela peut permettre à un adversaire de compromettre facilement les postes de travail.

Ceci est particulièrement important pour les applications clés qui interagissent avec du contenu provenant de sources non fiables telles que les suites de productivité bureautique (par exemple Microsoft Office), les lecteurs PDF (par exemple Adobe Reader), les navigateurs Web (par exemple Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome), le Web commun plug-ins de navigateur (par exemple Adobe Flash), clients de messagerie (Microsoft Outlook) et plates-formes logicielles (par exemple Oracle Java Platform et Microsoft .NETFramework).

Pour réduire ce risque, les nouvelles versions d'application et les nouveaux correctifs pour les applications doivent être appliqués dans un délai approprié, déterminé par la gravité des vulnérabilités de sécurité qu'ils traitent et les mesures d'atténuation déjà en place.

Dans les cas où une version précédente d'une application continue de recevoir un support sous forme de correctifs, elle doit toujours être mise à niveau vers la dernière version pour bénéficier de toute nouvelle fonctionnalité de sécurité ; cependant, cela peut être fait après plusieurs jours ou dès que possible suivant le degré de compromission des vulnérabilités couvertes par ce patching.

2.3. Liste blanche des applications

Un adversaire peut envoyer par courrier électronique du code malveillant ou héberger du code malveillant sur un site Web compromis et utiliser des techniques d'ingénierie sociale pour convaincre les utilisateurs de l'exécuter sur leur poste de travail.

Un tel code malveillant vise souvent à exploiter les vulnérabilités de sécurité dans les applications existantes et n'a pas besoin d'être installé sur le poste de travail pour réussir.

Pour réduire ce risque, une solution de liste blanche des applications doit être implémentée de manière appropriée.

La liste blanche des applications lorsqu'elle est implémentée sous sa forme la plus efficace (par exemple, en utilisant des hachages pour les exécutables, les bibliothèques de liens dynamiques, les scripts, les programmes d'installation et les applications packagées) peut être un mécanisme extrêmement efficace non seulement pour empêcher l'exécution de code malveillant, mais également pour garantir que seules les applications autorisées peuvent être installées sur les postes de travail.

Des implémentations moins efficaces de la liste blanche des applications (par exemple, en utilisant des chemins approuvés pour les applications installées en combinaison avec des contrôles d'accès nécessitant un accès privilégié pour écrire sur ces emplacements) peuvent être utilisées comme une première étape vers la mise en œuvre d'une solution de liste blanche d'applications plus complète et comment il peut être mis en œuvre de manière appropriée dans la mise en œuvre de la mise en liste blanche des applications.

Si Microsoft AppLocker est utilisé pour la liste blanche des applications, les règles suivantes peuvent être utilisées comme exemple d'implémentation basée sur le chemin.

À l'appui de cela, les règles, l'application des règles et le démarrage automatique du service d'identité d'application doivent être définis via la stratégie de groupe au niveau du domaine.

Règle de la liste blanche	Option recommandée
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\DLL Rules	
[Path] %ProgramFiles%*	Allow Everyone
[Path] %WinDir%*	Allow Everyone Exceptions : %System32%\spool\drivers\color* %System32%\Tasks* %WinDir%\Tasks* %WinDir%\Temp*
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\Executable Rules	
[Path] %ProgramFiles%*	Allow Everyone
[Path] %WinDir%*	Allow Everyone Exceptions : %System32%\spool\drivers\color* %System32%\Tasks* %WinDir%\Tasks* %WinDir%\Temp*
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\Packaged app Rules	
[Publisher] CN=Microsoft Corporation, O=Microsoft Corporation, L-Redmond, S=Washington, C=US	Allow Everyone
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\Script Rules	
[Path] %ProgramFiles%*	Allow Everyone
[Path] %WinDir%*	Allow Everyone Exceptions : %System32%\Com\dmp* %System32%\FxsTmp* %System32%\spool\drivers\color*

	%System32%\spool\PRINTERS* %System32%\spool\SERVERS* %System32%\Tasks* %WinDir%\Registration\CRMLog* %WinDir%\Tasks* %WinDir%\Temp* %WinDir%\tracing*
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\Windows Installer Rules	
[Publisher] CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Allow Everyone

Notez que pour les organisations utilisant la dernière version de Microsoft Windows 10 (c'est-à-dire la version 1709),

Les chemins suivants n'ont plus besoin d'être inclus comme exceptions :

- %WinDir%\servicing\Packages*
- %WinDir%\servicing\Sessions*

Une fonctionnalité de sécurité dans Microsoft Windows 10 version 1709 est Device Guard78.

Device Guard utilise une politique d'intégrité du code pour restreindre ce qui peut s'exécuter à la fois en mode noyau et sur le bureau en fonction de sa politique.

Device Guard utilise également la virtualisation pour se protéger du risque d'être désactivé par un adversaire qui a obtenu des privilèges d'administrateur.

Cependant, alors que Device Guard peut implémenter et enrichir la liste blanche des applications,

Les organisations auront probablement besoin d'une solution supplémentaire de liste blanche d'applications pour compléter Device Guard, en particulier si elles choisissent d'utiliser une approche basée sur le chemin pour la liste blanche des applications.

Les paramètres de stratégie de groupe peuvent être implémentés en supposant que toutes les pré-demandes de logiciel, de micrologiciel et de matériel sont satisfaites.

paramètres de la stratégie du groupe	Option recommandée
Computer Configuration\Policies\Administrative Templates\System\Device Guard	
Deploy Windows Defender Application Control	Enabled Code Integrity Policy file path: <organisation defined>
Turn On Virtualization Based Security	Enabled Virtualization Based Protection of Code Integrity :

	Enabled with UEFI lock

2.4. Réduction de la surface d'attaque

Attack Surface Reduction (ASR) est une fonctionnalité de sécurité de Microsoft Windows 10 version 1709 qui fait partie de Windows Defender Exploit Guard.

Il est conçu pour lutter contre la menace des logiciels malveillants exploitant des fonctionnalités légitimes dans les applications Microsoft Office.

Pour utiliser ASR, Windows Defender Antivirus doit être configuré en tant que principal moteur d'analyse antivirus en temps réel sur les postes de travail.

ASR propose un certain nombre de règles de réduction de la surface d'attaque,

Notamment :

- block executable content from email client and webmail:
  - BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550
- block Office applications from creating child processes:
  - D4F940AB-401B-4EFC-AADC-AD5F3C50688A
- block Office applications from creating executable content:
  - 3B576869-A4EC-4529-8536-B80A7769E899
- block Office applications from injecting code into other processes:
  - 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84
- block JavaScript and VBScript from launching downloaded executable content:
  - D3E037E1-3EB8-44C8-A917-57927947596D
- block execution of potentially obfuscated scripts:
  - 5BEB7EFE-FD9A-4556-801D-275E5FFC04CC
- block Win32 API calls from Office macro:
  - 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B.

Les organisations doivent implémenter ASR à l'aide de Windows Defender Antivirus ou utiliser des solutions antivirus tierces qui offrent des fonctionnalités similaires à celles fournies par ASR.

Pour les anciennes versions de Microsoft Windows, des mesures alternatives devront être mises en œuvre pour atténuer certaines menaces traitées par ASR, telles que les attaques Dynamic Data Exchange (DDE).

Pour les organisations utilisant Windows Defender Antivirus,

Les paramètres de stratégie de groupe suivants peuvent être implémentés pour appliquer les règles ASR ci-dessus.

paramètres de la stratégie du groupe	Option recommandée	
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Attack Surface Reduction		
Configure Attack Surface Reduction rules	Enabled Set the state for each ASR rule: 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 3b576869-a4ec-4529-8536-b80a7769e899 d4f940ab-401b-4efc-aadc-ad5f3c50688a 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B 5beb7efe-fd9a-4556-801d-275e5ffc04cc d3e037e1-3eb8-44c8-a917-57927947596d be9ba2d9-53ea-4cdc-84e5-9b1eeee46550	 1 1 1 1 1 1 1

2.5. Mise en cache des informations d'identification

Les informations d'identification mises en cache sont stockées dans la base de données du Gestionnaire de comptes de sécurité (SAM) et peuvent permettre à un utilisateur de se connecter à un poste de travail auquel il s'est précédemment connecté même si le domaine n'est pas disponible.

Bien que cette fonctionnalité puisse être souhaitable du point de vue de la disponibilité des services,

Cette fonctionnalité peut être utilisée abusivement par un adversaire qui peut récupérer ces informations d'identification mises en cache (potentiellement les informations d'identification de l'administrateur de domaine dans le pire des cas).

Pour réduire ce risque :

Les informations d'identification mises en cache doivent être limitées à une seule connexion précédente.

Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour désactiver la mise en cache des informations d'identification.

Paramètres de la stratégie du groupe	Option recommandée
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon : Number of previous logons to cache (in case domain controller is not available)	Only one logon
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled

Dans la session de l'utilisateur actif :

Les informations d'identification sont mises en cache dans le processus LSASS (Local Security Authority Subsystem Service) (y compris la phrase secrète de l'utilisateur en texte en clair si l'authentification WDigest est activée) pour permettre l'accès aux ressources réseau sans que les utilisateurs n'aient à saisir continuellement leurs informations d'identification.

Malheureusement, ces informations d'identification risquent d'être volées par un adversaire.

Pour réduire ce risque, l'authentification WDigest doit être désactivée.

Credential Guard11 est une fonctionnalité de sécurité de Microsoft Windows10 version 1709,

Elle est également conçue pour aider à protéger le processus LSASS.

Les paramètres de la stratégie de groupe suivants peuvent être mis en œuvre pour désactiver l'authentification WDigest et activer la fonctionnalité Credential Guard, en supposant que toutes les pré-demandes de logiciel, de micrologiciel et de matériel sont satisfaites.

paramètres de la stratégie du groupe	Option recommandée
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
WDigest Authentication	Disabled
Computer Configuration\Policies\Administrative Templates\System\Device Guard	
Turn OnVirtualization Based Security	Enabled Select Platform Security Level: Secure Boot and DMA Protection Credential Guard Configuration : Enabled with UEFI lock

2.6. Accès contrôlé aux dossiers

L'accès contrôlé aux dossiers est une fonctionnalité de sécurité de Microsoft Windows 10 version 1709 qui fait partie de Windows Defender Exploit Guard.

Il est conçu pour lutter contre la menace des ransomwares.

Pour utiliser l'accès contrôlé aux dossiers, l'antivirus Windows Defender doit être configuré comme le moteur d'analyse antivirus principal en temps réel sur les postes de travail.

D'autres solutions antivirus tierces peuvent offrir des fonctionnalités similaires dans le cadre de leurs offres.

Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour implémenter l'accès contrôlé aux dossiers.

Paramètres de la stratégie du groupe	Option recommandée
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ Windows Defender Exploit Guard\Controlled Folder Access	
Configure allowed applications	Enabled Enter the applications that should be trusted: <organisation defined>
Configure Controlled folder access	Enabled Configure the guard my folders feature: Block
Configure protected folders	Enabled Enter the folders that should be guarded: <organisation defined>

2.7. Saisie des informations d'identification

Lorsque les utilisateurs saisissent leurs informations d'identification sur un poste de travail, cela permet au code malveillant, tel qu'une application de journalisation des clés, de capturer les informations d'identification.

Pour réduire ce risque, les utilisateurs doivent être authentifiés en utilisant un chemin de confiance pour entrer leurs informations d'identification sur Secure Desktop.

Les paramètres de stratégie de groupe suivants peuvent être implémentés pour garantir que les informations d'identification sont entrées de manière sécurisée et empêcher la divulgation des noms d'utilisateur des utilisateurs précédents.

Paramètres de la stratégie du groupe	Option recommandée
Computer Configuration\Policies\Administrative Templates\System\Logon	
Do not display network selection UI	Enabled
Enumerate local users on domain-joined computers	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface	
Do not display the password reveal button	Enabled
Enumerate administrator accounts on elevation	Disabled

Require trusted path for credential entry	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options	
Disable or enable software Secure Attention Sequence	Disabled
Sign-in last interactive user automatically after a system-initiated restart	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display username at sign-in	Enabled

2.8. Antimalware à lancement précoce

Une autre fonctionnalité de sécurité clé de Trusted Boot, prise en charge par Microsoft Windows 10 et les cartes mères avec une interface UEFI (Unified Extensible Firmware Interface), est le Early Launch Antimalware (ELAM) 14. Utilisé en conjonction avec Secure Boot, un pilote ELAM peut être enregistré en tant que premier pilote non-Microsoft qui sera initialisé sur un poste de travail dans le cadre du processus de démarrage, lui permettant ainsi de vérifier tous les pilotes suivants avant leur initialisation. Le pilote ELAM est capable de permettre uniquement l'initialisation des bons pilotes connus; pilotes connus et inconnus à initialiser; pilotes connus bons, inconnus et mauvais mais critiques à initialiser; ou tous les pilotes à initialiser. Pour réduire le risque de pilotes malveillants, seuls les pilotes connus et inconnus doivent être autorisés à être initialisés pendant le processus de démarrage.

Le paramètre de stratégie de groupe suivant peut être implémenté pour garantir que seuls les pilotes connus et inconnus seront initialisés au moment du démarrage.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware	
Boot-Start Driver Initialization Policy	Enabled Choose the boot-start drivers that can be initialized: Good and unknown

2.9. Elévation de privilèges

Microsoft Windows offre la possibilité d'exiger la confirmation des utilisateurs, via la fonctionnalité de contrôle d'accès utilisateur (UAC), avant toute action sensible. Les paramètres par défaut permettent aux utilisateurs privilégiés d'effectuer des actions sensibles sans fournir au préalable d'informations d'identification et, bien que les utilisateurs standard doivent fournir des informations d'identification privilégiées, ils ne sont pas obligés de le faire via un chemin approuvé sur Secure Desktop. Cela permet à un adversaire qui accède à une session ouverte d'un utilisateur privilégié d'effectuer des actions sensibles à volonté ou pour un code malveillant de capturer toutes les informations d'identification saisies via un utilisateur standard lors d'une tentative d'élever ses privilèges. Pour réduire ce risque, la fonctionnalité UAC doit être mise en œuvre pour garantir que toutes les actions sensibles sont autorisées en fournissant des informations d'identification sur le bureau sécurisé.

Les paramètres de stratégie de groupe suivants peuvent être implémentés pour configurer efficacement la fonctionnalité UAC.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for credentials on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

2.10. Protection contre les exploits

Un adversaire qui développe des exploits pour Microsoft Windows ou des applications tierces aura un taux de réussite plus élevé lorsque les mesures de sécurité conçues par Microsoft pour aider à empêcher l'exploitation des vulnérabilités de sécurité ne sont pas mises en œuvre. La protection contre les exploits de Windows Defender Exploit Guard, une fonctionnalité de sécurité de Microsoft Windows 10, fournit des mesures de sécurité à l'échelle du système et spécifiques à l'application. La protection contre les exploits est conçue pour remplacer la boîte à outils EMET (Enhanced Mitigation Experience Toolkit) qui était utilisée sur les versions antérieures de Microsoft Windows 10.
Les mesures de sécurité à l'échelle du système configurables via la protection contre les exploits incluent: Control Flow Guard (CFG), Data Execution Prevention (DEP), obligatoire Address Space Layout Randomization (ASLR), bottom-up ASLR, Structured Exception Handling Overwrite Protection (SEHOP) et la corruption de tas protection. De nombreuses autres mesures de sécurité spécifiques aux applications sont également disponibles.

Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour définir les paramètres de protection contre les exploits et pour empêcher les utilisateurs de modifier ces paramètres sur leurs appareils.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Exploit Guard\Exploit Protection	
Use a common set of exploit protection settings	Enabled Type the location (local path, UNC path, or URL) of the mitigation settings configuration XML file: *<organisation defined>*
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Security\App and browser protection	
Prevent users from modifying settings	Enabled

En outre, le paramètre de stratégie de groupe suivant peut être implémenté pour garantir que DEP n'est pas désactivé pour l'Explorateur de fichiers.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Turn off Data Execution Prevention for Explorer	Disabled

En outre, le paramètre de stratégie de groupe suivant peut être implémenté pour forcer l'utilisation de SEHOP. Notez que les paramètres de stratégie de groupe du guide de sécurité MS sont disponibles dans le cadre de la boîte à outils de conformité de la sécurité Microsoft.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
Enabled Structured Exception Handling Overwrite Protection (SEHOP)	Enabled

2.11. Compte des administrateurs locaux

Lorsque des comptes d'administrateur intégrés sont utilisés avec des noms de compte et des mots de passe communs, cela peut permettre à un adversaire qui compromet ces informations d'identification sur un poste de travail de transférer facilement sur le réseau vers d'autres postes de travail. Même si les comptes d'administrateur intégrés portent un nom unique et ont des mots de passe uniques, un adversaire peut toujours identifier ces comptes en fonction de leur identifiant de sécurité (c'est-à-dire S-1-5-21-domain-50017) et utiliser ces informations pour concentrer tout tente de forcer les informations d'identification sur un poste de travail s'ils peuvent accéder à la base de données SAM. Pour réduire ce risque, les comptes d'administrateur intégrés doivent être désactivés. À la place, les comptes de domaine dotés de privilèges administratifs locaux, mais sans privilèges administratifs de domaine, doivent être utilisés pour la gestion des postes de travail.

Le paramètre de stratégie de groupe suivant peut être implémenté pour désactiver les comptes d'administrateur intégrés

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Administrator account status	Disabled

Si un compte d'administrateur local commun doit absolument être utilisé pour la gestion des postes de travail, la solution de mot de passe d'administrateur local (LAPS) 18 de Microsoft doit être utilisée pour garantir l'utilisation de phrases de passe uniques pour chaque poste de travail. En outre, les restrictions de contrôle de compte d'utilisateur doivent être appliquées aux connexions à distance utilisant de tels comptes.
Remarque : les paramètres de stratégie de groupe du guide de sécurité MS sont disponibles dans le cadre de la boîte à outils Microsoft Security Compliance.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
Apply UAC restrictions to local accounts on network logons	Enabled

2.12. Mesures au niveau du BOOT System

La troisième fonctionnalité de sécurité clé de Trusted Boot, prise en charge par Microsoft Windows 10 et les cartes mères avec à la fois un UEFI et un Trusted Platform Module (TPM), est Measured Boot20. Le démarrage mesuré est utilisé pour développer un journal fiable des composants qui sont initialisés avant le pilote ELAM. Ces informations peuvent ensuite être examinées par un logiciel anti-programme malveillant à la recherche de signes d'altération des composants de démarrage. Pour réduire le risque que les modifications malveillantes apportées aux composants de démarrage passent inaperçues, le démarrage mesuré doit être utilisé sur les postes de travail qui le prennent en charge.

2.13. Microsoft Edge

Microsoft Edge est un navigateur Web qui a été introduit pour la première fois dans Microsoft Windows 10 pour remplacer Internet Explorer. Microsoft Edge contient des améliorations de sécurité significatives par rapport à Internet Explorer et doit être utilisé dans la mesure du possible. La version la plus récente de Microsoft Edge est basée sur Chromium et est disponible en téléchargement séparé avec des modèles de stratégie de groupe distincts21. Il peut être configuré avec une posture de sécurité équivalente aux paramètres de stratégie de groupe suggérés ci-dessous.
L'utilisation d'Internet Explorer 11 doit être limitée à la prise en charge des applications Web héritées hébergées sur les intranets d'entreprise. Si Internet Explorer 11 n'est pas nécessaire, il doit être désinstallé de Microsoft Windows 10 pour réduire la surface d'attaque du système d'exploitation.

Pour les organisations utilisant Microsoft Edge au lieu de navigateurs Web tiers, les paramètres de stratégie de groupe suivants peuvent être implémentés pour renforcer Microsoft Edge, y compris Windows Defender SmartScreen22.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge	
Allow Adobe Flash	Disabled
Allow Developer Tools	Disabled
Configure Do Not Track	Enabled
Configure Password Manager	Disabled
Configure Pop-up Blocker	Enabled
Configure Windows Defender SmartScreen	Enabled
Prevent access to the about:flags page in Microsoft Edge	Enabled

Prevent bypassing Windows Defender SmartScreen prompts for files	Enabled
Prevent bypassing Windows Defender SmartScreen prompts for sites	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ Windows Defender Exploit Guard\Network Protection	
Prevent users and apps from accessing dangerous websites	Enabled Block
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Application Guard	
Turn on Windows Defender Application Guard in Managed Mode	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Microsoft Edge	
Configure Windows Defender SmartScreen	Enabled
Prevent bypassing Windows Defender SmartScreen prompts for sites	Enabled

2.14. Multi-facteur d'authentification

Étant donné que les informations d'identification privilégiées permettent souvent aux utilisateurs de contourner les fonctionnalités de sécurité mises en place pour protéger les postes de travail et sont sensibles aux applications de journalisation des clés, il est important qu'elles soient correctement protégées contre toute compromission. En outre, un adversaire qui force brutalement les hachages de mots de passe capturés peut accéder aux postes de travail si l'authentification multifacteur n'a pas été mise en œuvre. Pour réduire ce risque, l'authentification multifacteur basée sur le matériel doit être utilisée pour les utilisateurs lorsqu'ils exécutent une action privilégiée ou accèdent à des référentiels de données importants ou sensibles.
Pour plus d'informations sur la mise en œuvre efficace de l'authentification multifacteur, consultez la publication Implémentation de l'authentification multifacteur.

2.15. Operating system architecture

Les versions x64 (64 bits) de Microsoft Windows incluent des fonctionnalités de sécurité supplémentaires qui manquent aux versions x86 (32 bits). Cela inclut la prise en charge native du noyau de la prévention de l'exécution des données (DEP) basée sur le matériel, la protection contre les correctifs du noyau (PatchGuard), la signature obligatoire des pilotes de périphérique et l'absence de prise en charge des pilotes 32 bits malveillants. L'utilisation de versions x86 (32 bits) de Microsoft Windows expose les organisations à exploiter des techniques atténuées par les versions x64 (64 bits) de Microsoft Windows. Pour réduire ce risque, les postes de travail doivent utiliser les versions x64 (64 bits) de Microsoft Windows.

2.16. Operating system patching

Les correctifs sont publiés soit en réponse à des vulnérabilités de sécurité précédemment révélées, soit pour remédier de manière proactive aux vulnérabilités de sécurité qui n'ont pas encore été divulguées publiquement. Dans le cas de vulnérabilités de sécurité révélées, il est possible que des exploits aient déjà été développés et soient librement disponibles dans les outils de piratage courants. Dans le cas de correctifs pour des vulnérabilités de sécurité qui n'ont pas encore été divulgués publiquement, il est relativement facile pour un adversaire d'utiliser des outils disponibles gratuitement pour identifier la vulnérabilité de sécurité corrigée et développer un exploit associé. Cette activité peut être entreprise en moins d'un jour et a conduit à une augmentation des attaques d'un jour. Pour réduire ce risque, les correctifs du système

d'exploitation et les mises à jour des pilotes doivent être gérés, déployés et appliqués de manière centralisée dans un délai approprié, tel que déterminé par la gravité de la vulnérabilité de sécurité et les mesures d'atténuation déjà en place.
Le correctif du système d'exploitation peut être réalisé à l'aide de Microsoft Endpoint Configuration Manager24 ou de Microsoft Windows Server Update Services (WSUS) 25, ainsi que de la fonctionnalité Wake-on-LAN pour faciliter le correctif en dehors des heures de travail principales. Cependant, afin d'éviter la perte de tout travail non enregistré, il est conseillé aux utilisateurs de se déconnecter de leur poste de travail à la fin de chaque journée.
Pour plus d'informations sur la détermination de la gravité des vulnérabilités de sécurité et les délais d'application des correctifs, consultez la publication Évaluation des vulnérabilités de sécurité et application des correctifs26.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour garantir que les systèmes d'exploitation restent correctement corrigés.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update	
Allow Automatic Updates immediate installation	Enabled
Configure Automatic Updates	Enabled Configure automatic updating: 4 - Auto download and schedule the install Schedule install day: 0 - Every day Install updates for other Microsoft products
Do not include drivers with Windows Updates	Disabled
Enabling Windows Update Power management to automatically wake up the system to install scheduled updates	Enabled
No auto-restart with logged on users for scheduled automatic updates installations	Disabled
Remove access to use all Windows Update features	Disabled
Turn on recommended updates via Automatic Updates	Enabled

En outre, si un serveur Windows Server Update Services (WSUS) est utilisé, le paramètre de stratégie de groupe suivant peut être implémenté.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update	
Specify intranet Microsoft update service location	Enabled Set the intranet update service for detecting updates: *<server:port>*

Sinon, si Microsoft Endpoint Configuration Manager est utilisé à la place des serveurs de mise à jour Microsoft ou d'un serveur WSUS, des paramètres équivalents peuvent être implémentés pour obtenir un résultat similaire.

2.17. Version du système d'exploitation

Microsoft Windows 10 a introduit des améliorations dans les fonctionnalités de sécurité par rapport aux versions précédentes de Microsoft Windows27. Cela a rendu plus difficile pour un adversaire de créer des exploits fiables pour les vulnérabilités de sécurité découvertes. L'utilisation d'anciennes versions de Microsoft Windows, y compris les versions précédentes de Microsoft Windows 10, expose les organisations à exploiter des techniques qui ont depuis été atténuées dans les nouvelles versions de Microsoft Windows. Pour réduire ce risque, les postes de travail doivent utiliser la dernière version de Microsoft Windows 10.

2.18. La politique des mots de passe

L'utilisation de mots de passe faibles, tels que des mots de passe à huit caractères sans complexité, peut leur permettre d'être forcés brutalement en quelques minutes à l'aide d'applications disponibles gratuitement sur le Web. Pour réduire ce risque, une politique de mot de passe sécurisé doit être mise en œuvre.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour obtenir une stratégie de mot de passe à facteur unique sécurisé.
Remarque : les paramètres de stratégie de groupe pour les mots de passe utilisés dans le cadre de l'authentification multifacteur peuvent ne pas avoir besoin d'être aussi stricts (par exemple, une longueur de 6 caractères sans complexité).

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Logon	
Turn off picture password sign-in	Enabled
Turn on convenience PIN sign-in	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy	
Maximum password age	365 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Limit local account use of blank passwords to console logon only	Enabled

2.19. Restreindre les comptes privilégiés

Fournir aux utilisateurs un compte privilégié pour une utilisation quotidienne présente un risque qu'ils utilisent ce compte pour l'accès externe au Web et à la messagerie électronique. Ceci est particulièrement préoccupant car les utilisateurs privilégiés ont la possibilité d'exécuter du code malveillant avec un accès privilégié plutôt qu'un accès standard. Pour réduire ce risque, les utilisateurs qui n'ont pas besoin d'un accès privilégié ne doivent pas se voir attribuer de comptes privilégiés, tandis que les utilisateurs nécessitant un accès privilégié doivent avoir des comptes standard et privilégiés distincts avec des informations d'identification différentes. En outre, tout un compte privilégié utilisé doit avoir un accès externe au Web et à la messagerie électronique bloqué. Pour plus d'informations sur l'utilisation des comptes privilégiés et la minimisation de leur utilisation, consultez la publication Restricting Administrative Privileges.

2.20. Secure Boot

Une autre méthode permettant au code malveillant de maintenir la persistance et d'empêcher la détection consiste à remplacer le chargeur de démarrage par défaut pour Microsoft Windows par une version malveillante. Dans de tels cas, le chargeur de démarrage malveillant s'exécute au moment du démarrage et charge Microsoft Windows sans aucune indication de sa présence. Ces chargeurs de démarrage malveillants sont extrêmement difficiles à détecter et peuvent être utilisés pour dissimuler du code malveillant sur les postes de travail. Pour réduire ce risque, des cartes mères dotées de la fonctionnalité Secure Boot doivent être utilisées. Secure Boot, un composant de Trusted Boot, est une fonctionnalité de sécurité de Microsoft Windows 10 et des cartes mères avec un UEFI29. Secure Boot fonctionne en vérifiant au moment du démarrage que le chargeur de démarrage est signé et correspond à un certificat signé Microsoft stocké dans l'UEFI. Si les signatures de certificat correspondent, le chargeur de démarrage est autorisé à s'exécuter, sinon il est empêché de s'exécuter et le poste de travail ne démarrera pas.

3. LES PRIORITES MOYENNES

Les recommandations suivantes, répertoriées par ordre alphabétique, doivent être traitées comme des priorités moyennes lors du renforcement des stations de travail Microsoft Windows 10

3.1. Politique de verrouillage de compte

Autoriser un nombre illimité de tentatives d'accès aux postes de travail ne parviendra pas à empêcher un adversaire de tenter de forcer les mesures d'authentification. Pour réduire ce risque, les comptes doivent être verrouillés après un nombre défini de tentatives d'authentification non valides. Le seuil de verrouillage des comptes n'a pas besoin d'être trop restrictif pour être efficace. Par exemple, un seuil de 5 tentatives incorrectes, avec une période de réinitialisation de 15 minutes pour le compteur de verrouillage, empêchera toute tentative de force brute tout en étant peu susceptible de verrouiller un utilisateur légitime qui saisit accidentellement son mot de passe de manière incorrecte à plusieurs reprises.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour atteindre une stratégie de verrouillage raisonnable.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy	
Account lockout duration	0
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

3.2. Connections anonymes

Un adversaire peut utiliser des connexions anonymes pour recueillir des informations sur l'état des postes de travail. Les informations qui peuvent être collectées à partir de connexions anonymes (c'est-à-dire en utilisant la commande « net use » pour se connecter au partage IPC $) peuvent inclure des listes d'utilisateurs et de groupes, des SID pour les comptes, des listes de partages, des politiques de poste de travail, des versions de système d'exploitation et des niveaux de correctifs. Pour réduire ce risque, les connexions anonymes aux postes de travail doivent être désactivées.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour désactiver l'utilisation de connexions anonymes.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation	
Enable insecure guest logons	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Restrict clients allowed to make remote calls to SAM	O:BAG:BAD:(A;;RC;;;BA)

Network security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Access this computer from the network	Administrators Remote Desktop Users
Deny access to this computer from the network	NT AUTHORITY\Local Account

3.3. Logiciel Antivirus

Un adversaire peut développer un code malveillant pour exploiter les vulnérabilités de sécurité des logiciels non détectés et corrigés par les fournisseurs lors des tests. Comme un temps et des efforts importants sont souvent impliqués dans le développement d'exploits fonctionnels et fiables, un adversaire réutilisera souvent ses exploits autant que possible avant d'être contraint de développer de nouveaux exploits. Pour réduire ce risque, des applications de sécurité des points finaux avec une fonctionnalité antivirus basée sur les signatures doivent être implémentées. Ce faisant, les signatures devraient être mises à jour au moins quotidiennement.
Bien que l'utilisation de la fonctionnalité antivirus basée sur les signatures puisse aider à réduire les risques, elles ne sont efficaces que lorsqu'un morceau particulier de code malveillant a déjà été profilé et que les signatures sont à jour. Un adversaire peut créer des variantes de code malveillant connu ou développer un nouveau code malveillant invisible pour contourner les mécanismes de détection traditionnels basés sur les signatures. Pour réduire ce risque, des applications de sécurité des points de terminaison avec une fonctionnalité de prévention d'intrusion basée sur l'hôte ou une fonctionnalité équivalente exploitant des services basés sur le cloud doivent également être implémentées. Ce faisant, cette fonctionnalité doit être définie au plus haut niveau disponible.
Si vous utilisez la solution antivirus Windows Defender de Microsoft30, les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour la configurer de manière optimale.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus	
Turn off Windows Defender Antivirus	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ MAPS	
Configure local setting override for reporting to Microsoft MAPS	Disabled
Configure the 'Block at First Sight' feature	Enabled
Join Microsoft MAPS	Enabled Join Microsoft MAPS: Advanced MAPS
Send file samples when further analysis is required	Enabled Send file samples when further analysis is required: Send safe samples
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ MpEngine	

Configure extended cloud check	Enabled Specify the extended cloud check time in seconds: 50
Select cloud protection level	Enabled Select cloud blocking level: High blocking level *or* High+ blocking level
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ Quarantine	
Configure removal of items from Quarantine folder	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ Real-time Protection	
Scan all downloaded files and attachments	Enabled
Turn off real-time protection	Disabled
Turn on behavior monitoring	Enabled
Turn on process scanning whenever real-time protection is enabled	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ Scan	
Allow users to pause scan	Disabled
Check for the latest virus and spyware definitions before running a scheduled scan	Enabled
Scan archive files	Enabled
Scan packed executables	Enabled
Scan removable drives	Enabled
Turn on e-mail scanning	Enabled
Turn on heuristics	Enabled

3.4. Gestionnaire de pièces jointes

Le Gestionnaire de pièces jointes de Microsoft Windows fonctionne en conjonction avec des applications telles que la suite Microsoft Office et Internet Explorer pour aider à protéger les postes de travail contre les pièces jointes reçues par courrier électronique ou téléchargées sur Internet. Le gestionnaire de pièces jointes classe les fichiers comme présentant un risque élevé, moyen ou faible en fonction de la zone dont ils proviennent et du type de fichier. En fonction du risque pour le poste de travail, le gestionnaire de pièces jointes émettra un avertissement à un utilisateur ou l'empêchera d'ouvrir un fichier. Si les informations de zone ne sont pas conservées ou peuvent être supprimées, cela peut permettre à un adversaire de créer socialement un utilisateur pour contourner les protections offertes par le gestionnaire de pièces jointes. Pour réduire ce risque, le gestionnaire de pièces jointes doit être configuré pour conserver et protéger les informations de zone pour les fichiers.

Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour garantir que les informations de zone associées aux pièces jointes sont conservées et protégées.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager	
Do not preserve zone information in file attachments	Disabled
Hide mechanisms to remove zone information	Enabled

3.5. Gérer les événements d'audit

Le fait de ne pas capturer et d'analyser les événements d'audit liés à la sécurité à partir des postes de travail peut entraîner des intrusions qui passent inaperçues. En outre, le manque de telles informations peut entraver considérablement les enquêtes suite à un incident de sécurité. Pour réduire ce risque, les événements d'audit liés à la sécurité des postes de travail doivent être capturés et régulièrement analysés.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour garantir que les événements d'audit liés à la sécurité sont correctement capturés.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation	
Include command line in process creation events	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application	
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 65536
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security	
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 2097152
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System	
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 65536
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Manage auditing and security log	Administrators

En outre, les paramètres de stratégie de groupe suivants peuvent être implémentés pour permettre une stratégie d'audit complète.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management	
Audit Computer Account Management	Success and Failure
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking	
Audit Process Creation	Success
Audit Process Termination	Success
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff	
Account Lockout	Failure
Audit Group Membership	Success
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access	
Audit File Share	Success and Failure
Audit File System	Success and Failure
Audit Kernel Object	Success and Failure
Audit Other Object Access Events	Success and Failure
Audit Registry	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change	
Audit Audit Policy Change	Success and Failure
Audit Other Policy Change Events	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System	
Audit System Integrity	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled

3.6. Autoplay and AutoRun

Lorsqu'elle est activée, la lecture automatique commence automatiquement la lecture à partir d'un lecteur ou d'une source multimédia dès qu'elle est utilisée avec un poste de travail, tandis que les commandes AutoRun, généralement dans un fichier autorun.inf sur le support, peuvent être utilisées automatiquement exécuter n'importe quel fichier sur le support sans intervention de l'utilisateur. Cette fonctionnalité peut être exploitée par un adversaire pour exécuter automatiquement du code malveillant. Pour réduire ce risque, les fonctionnalités de lecture automatique et d'exécution automatique doivent être désactivées.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour désactiver les fonctionnalités de lecture automatique et d'exécution automatique.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies	
Disallow Autoplay for non-volume devices	Enabled
Set the default behavior for AutoRun	Enabled Default AutoRun Behavior: Do not execute any autorun commands
Turn off Autoplay	Enabled Turn off Autoplay on: All drives

3.7. BIOS and UEFI passwords

Un adversaire ayant accès au système d'entrée / sortie de base (BIOS) ou à l'UEFI d'un poste de travail peut modifier la configuration matérielle du poste de travail pour introduire des vecteurs d'attaque ou affaiblir les fonctionnalités de sécurité au sein du système d'exploitation du poste de travail. Cela peut inclure la désactivation de la fonctionnalité de sécurité dans le processeur, la modification des périphériques de démarrage autorisés et l'activation d'interfaces de communication non sécurisées telles que FireWire et Thunderbolt. Pour réduire ce risque, des mots de passe BIOS et UEFI forts doivent être utilisés pour toutes les stations de travail afin d'empêcher tout accès non autorisé.

3.8. Boot devices

Par défaut, les postes de travail sont souvent configurés pour démarrer à partir d'un support optique, voire d'un support USB, de préférence aux disques durs. Un adversaire disposant d'un accès physique à de telles stations de travail peut démarrer à partir de son propre support afin d'accéder au contenu des disques durs. Avec cet accès, un adversaire peut réinitialiser les mots de passe des comptes d'utilisateurs locaux ou accéder à la base de données SAM locale pour voler des hachages de mots de passe pour des tentatives de craquage par force brute hors ligne. Pour réduire ce risque, les stations de travail doivent être limitées au démarrage uniquement à partir du lecteur système principal désigné.

3.9. Bridging networks

Lorsque les postes de travail ont plusieurs interfaces réseau, telles qu'une interface Ethernet et une interface sans fil, il est possible d'établir un pont entre les réseaux connectés. Par exemple,

lorsque vous utilisez une interface Ethernet pour vous connecter au réseau filaire d'une organisation et une interface sans fil pour vous connecter à un autre réseau non contrôlé par l'organisation, tel qu'un point d'accès sans fil public. Lorsque des ponts sont créés entre ces réseaux, un adversaire peut accéder directement au réseau filaire à partir du réseau sans fil pour extraire des informations sensibles. Pour réduire ce risque, la possibilité d'installer et de configurer des ponts réseau entre différents réseaux doit être désactivée. Cela n'empêchera pas un adversaire de compromettre un poste de travail via le réseau sans fil, puis d'utiliser un logiciel malveillant comme moyen d'accéder indirectement au réseau câblé. Cela ne peut être évité qu'en désactivant manuellement toutes les interfaces sans fil lors de la connexion à des réseaux câblés.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour désactiver la possibilité d'installer et de configurer des ponts réseau.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Network\Network Connections	
Prohibit installation and configuration of Network Bridge on your DNS domain network	Enabled
Prohibit use of Internet Connection Sharing on your DNS domain network	Enabled
Route all traffic through the internal network	Enabled Select from the following states: Enabled State
Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager	
Prohibit connection to non-domain networks when connected to domain authenticated network	Enabled

3.10. Comptes invités intégrés

Lorsque des comptes invités intégrés sont utilisés, cela peut permettre à un adversaire de se connecter à un poste de travail sur le réseau sans avoir à compromettre au préalable les informations d'identification des utilisateurs légitimes. Pour réduire ce risque, les comptes invités intégrés doivent être désactivés.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour désactiver et renommer les comptes invités intégrés.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Guest account status	Disabled

3.11.CD burner access

Si la fonctionnalité de gravure de CD est activée et que des graveurs de CD sont installés sur les postes de travail, un adversaire peut tenter de voler des informations sensibles en les gravant sur CD. Pour réduire ce risque, les utilisateurs ne doivent pas avoir accès à la fonctionnalité de gravure de CD, sauf lorsque cela est explicitement requis.
Le paramètre de stratégie de groupe suivant peut être implémenté pour empêcher l'accès à la fonctionnalité de gravure de CD, bien que ce paramètre de stratégie de groupe n'empêche que l'accès à la fonctionnalité de gravure de CD native dans Microsoft Windows, les utilisateurs doivent également être empêchés d'installer des applications de gravure de CD tierces. Les lecteurs de CD peuvent également être utilisés dans les postes de travail au lieu des graveurs de CD.

Group Policy Setting	Recommended Option

User Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Remove CD Burning features	Enabled

3.12. Centralised audit event logging

Le stockage des journaux d'événements d'audit sur les postes de travail présente un risque qu'un adversaire tente de modifier ou de supprimer ces journaux lors d'une intrusion pour couvrir leurs traces. En outre, le fait de ne pas procéder à une journalisation centralisée des événements d'audit réduira la visibilité des événements d'audit sur tous les postes de travail, empêchera la corrélation des événements d'audit et augmentera la complexité des enquêtes après des incidents de sécurité. Pour réduire ce risque, les journaux d'événements d'audit des postes de travail doivent être transférés vers un serveur de journalisation central sécurisé.

3.13. Command Prompt

Un adversaire qui accède à un poste de travail peut utiliser l'invite de commande pour exécuter des outils Microsoft Windows intégrés afin de collecter des informations sur le poste de travail ou le domaine et programmer l'exécution de code malveillant sur d'autres postes de travail du réseau. Pour réduire ce risque, les utilisateurs ne doivent pas avoir accès à l'invite de commandes ni pouvoir exécuter des fichiers de commandes et des scripts. S'il existe une exigence commerciale légitime pour permettre aux utilisateurs d'exécuter des fichiers batch (par exemple, des fichiers cmd et bat); exécuter des scripts de fichiers de commandes d'ouverture de session, de déconnexion, de démarrage ou d'arrêt; ou utiliser les services Bureau à distance, ce risque devra être accepté.
Le paramètre de stratégie de groupe suivant peut être implémenté pour empêcher l'accès à l'invite de commande et à la fonctionnalité de traitement de script.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\System	
Prevent access to the command prompt	Enabled Disable the command prompt script processing also: Yes

3.14. Direct Memory Access

Les interfaces de communication qui utilisent l'accès direct à la mémoire (DMA) peuvent permettre à un adversaire disposant d'un accès physique à un poste de travail d'accéder directement au contenu de la mémoire d'un poste de travail. Cela peut être utilisé pour lire des contenus sensibles tels que des clés cryptographiques ou pour écrire du code malveillant directement dans la mémoire. Pour réduire ce risque, les interfaces de communication qui autorisent le DMA (par exemple FireWire et Thunderbolt) doivent être désactivées. Cela peut être réalisé soit physiquement (par exemple en utilisant de l'époxy) ou en utilisant des commandes logicielles31 (par exemple en désactivant la fonctionnalité dans le BIOS ou UEFI; en supprimant le pilote SBP-2 et en désactivant les contrôleurs FireWire et Thunderbolt; ou en utilisant une solution de protection de point final).
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour supprimer le pilote SBP-2 ainsi que pour désactiver les contrôleurs FireWire et Thunderbolt. Notez que les systèmes Intel ont inclus une protection DMA du noyau intégrée pour Thunderbolt 3 par défaut32, cependant, ces protections ne sont pas infaillibles.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions	

Prevent installation of devices that match any of these device IDs	Enabled Prevent installation of devices that match any of these Device IDs: PCI\CC_0C0010, PCI\CC_0C0A Also apply to matching devices that are already installed.
Prevent installation of devices using drivers that match these device setup classes	Enabled Prevent installation of devices using drivers for these device setup classes: {d48179be-ec20-11d1-b6b8-00c04fa372a7} Also apply to matching devices that are already installed.

3.15. Endpoint device control

Un adversaire disposant d'un accès physique à un poste de travail peut tenter de connecter des supports USB non autorisés ou d'autres périphériques dotés d'une fonctionnalité de stockage de masse (par exemple, les smartphones, les lecteurs de musique numérique ou les appareils photo) pour faciliter les infections par code malveillant ou la copie non autorisée d'informations sensibles. Pour réduire ce risque, la fonctionnalité de contrôle des périphériques d'extrémité doit être mise en œuvre de manière appropriée pour contrôler l'utilisation de tous les périphériques de stockage amovibles.
Le paramètre de stratégie de groupe suivant peut être implémenté pour désactiver l'utilisation de périphériques de stockage amovibles.

Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access	
All Removable Storage classes: Deny all access	Enabled

Sinon, si des classes spécifiques de périphériques de stockage amovibles sont nécessaires pour répondre aux exigences de l'entreprise, les autorisations d'exécution, de lecture et d'écriture doivent être contrôlées classe par classe.
Les paramètres de stratégie de groupe suivants fournissent un exemple d'implémentation qui permet aux données d'être lues mais non exécutées ou écrites sur toutes les classes de périphériques de stockage amovibles.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access	
CD and DVD: Deny execute access	Enabled
CD and DVD: Deny read access	Disabled
CD and DVD: Deny write access	Enabled
Custom Classes: Deny read access	Disabled
Custom Classes: Deny write access	Enabled
Floppy Drives: Deny execute access	Enabled
Floppy Drives: Deny read access	Disabled
Floppy Drives: Deny write access	Enabled
Removable Disks: Deny execute access	Enabled
Removable Disks: Deny read access	Disabled
Removable Disks: Deny write access	Enabled
Tape Drives: Deny execute access	Enabled

Tape Drives: Deny read access	Disabled
Tape Drives: Deny write access	Enabled
WPD Devices: Deny read access	Disabled
WPD Devices: Deny write access	Enabled

3.16. Partage de fichiers et d'imprimantes

Les utilisateurs partageant des fichiers à partir de leur poste de travail peuvent entraîner un manque de contrôles d'accès appropriés appliqués aux informations sensibles et le potentiel de propagation de code malveillant si les partages de fichiers ont un accès en lecture / écriture. Pour réduire ce risque, le partage local de fichiers et d'imprimantes doit être désactivé. Idéalement, les informations sensibles devraient être gérées de manière centralisée (par exemple sur un partage réseau avec des contrôles d'accès appropriés). La désactivation du partage de fichiers et d'imprimantes n'affectera pas la capacité d'un utilisateur à accéder aux lecteurs et imprimantes partagés sur un réseau.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour empêcher les utilisateurs de partager des fichiers.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\HomeGroup	
Prevent the computer from joining a homegroup	Enabled
User Configurations\Policies\Administrative Templates\Windows Components\Network Sharing	
Prevent users from sharing files within their profile.	Enabled

3.17. Group Policy processing

S'appuyer sur les utilisateurs pour définir les paramètres de stratégie de groupe pour leurs postes de travail crée la possibilité pour les utilisateurs de mal configurer ou de désactiver par inadvertance les fonctionnalités de sécurité sans tenir compte de l'impact sur l'état de sécurité du poste de travail. Alternativement, un adversaire pourrait exploiter cela pour désactiver les paramètres de stratégie de groupe locale qui entravent ses efforts pour extraire des informations sensibles. Pour réduire ce risque, tous les paramètres d'audit, de droits d'utilisateur et de stratégie de groupe liés à la sécurité doivent être spécifiés pour les postes de travail au niveau d'une unité organisationnelle ou d'un domaine. Pour garantir que ces stratégies ne sont pas affaiblies, la prise en charge des paramètres de stratégie de groupe locale doit également être désactivée.

Les paramètres de stratégie de groupe suivants peuvent être implémentés pour garantir que seuls les paramètres de stratégie de groupe basés sur le domaine sont obtenus et appliqués aux postes de travail de manière sécurisée.

Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Network\Network Provider	
Hardened UNC Paths	Enabled Hardened UNC Paths: *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1
Computer Configuration\Policies\Administrative Templates\System\Group Policy	

Configure registry policy processing	Enabled Process even if the Group Policy objects have not changed
Configure security policy processing	Enabled Process even if the Group Policy objects have not changed
Turn off background refresh of Group Policy	Disabled
Turn off Local Group Policy Objects processing	Enabled

3.18. Hard drive encryption

Un adversaire ayant un accès physique à un poste de travail peut être en mesure d'utiliser un CD / DVD amorçable ou un support USB pour charger son propre environnement d'exploitation. À partir de cet environnement, ils peuvent accéder au système de fichiers local pour accéder aux informations sensibles ou à la base de données SAM pour accéder aux hachages de mots de passe. De plus, un adversaire qui accède à un disque dur volé ou non désinfecté sera de récupérer son contenu lorsqu'il est connecté à une autre machine sur laquelle il a un accès administratif et peut prendre possession des fichiers. Pour réduire ce risque, le chiffrement intégral du disque AES doit être utilisé pour protéger le contenu des disques durs contre tout accès non autorisé.
Si Microsoft BitLocker est utilisé, les paramètres de stratégie de groupe suivants doivent être implémentés.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption	
Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)	Enabled Select the encryption method for operating system drives: XTS-AES 128-bit
Select the encryption method for fixed data drives: XTS-AES 128-bit Select the encryption method for removable data drives: XTS-AES 128-bit	
Disable new DMA devices when this computer is locked	Enabled
Prevent memory overwrite on restart	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\ Fixed Data Drives	
Choose how BitLocker-protected fixed drives can be recovered	Enabled Allow data recovery agent Configure user storage of BitLocker recovery information: Allow 48-digit recovery password Allow 256-bit recovery key Omit recovery options from the BitLocker setup wizard Save BitLocker recovery information to AD DS for fixed data drives Configure storage of BitLocker recovery information to AD DS: Backup recovery passwords and key packages Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives
Configure use of passwords for fixed data drives	Enabled Require password for fixed data drive Configure password complexity for fixed data drives: Require password complexity

	Minimum password length for fixed data drive: 14
Deny write access to fixed drives not protected by BitLocker	Enabled
Enforce drive encryption type on fixed data drives	Enabled Select the encryption type: Full encryption
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\ Operating System Drives	
Allow devices compliant with InstantGo or HSTI to opt out of pre-boot PIN.	Disabled
Allow enhanced PINs for startup	Enabled
Allow network unlocked at startup	Enabled
Allow Secure Boot for integrity validation	Enabled
Choose how BitLocker-protected operating system drives can be recovered	Enabled Allow data recovery agent Configure user storage of BitLocker recovery information: Allow 48-digit recovery password Allow 256-bit recovery key Omit recovery options from the BitLocker setup wizard Save BitLocker recovery information to AD DS for operating system drives Configure storage of BitLocker recovery information to AD DS: Store recovery passwords and key packages Do not enable BitLocker until recovery information is stored to AD DS for operating system drives
Configure minimum PIN length for startup	Enabled Minimum characters: 14
Configure use of passwords for operating system drives	Enabled Configure password complexity for operating system drives: Require password complexity Minimum password length for operating system drive: 14
Disallow standard users from changing the PIN or password	Disabled
Enforce drive encryption type on operating system drives	Enabled Select the encryption type: Full encryption
Require additional authentication at startup	Enabled Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive) Settings for computers with a TPM Configure TPM startup: Do not allow TPM Configure TPM startup PIN: Allow startup PIN with TPM Configure TPM startup key: Allow startup key with TPM Configure TPM startup key and PIN: Allow startup key and PIN with TPM
Reset platform validation data after BitLocker recovery	Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\ Removable Data Drives	
Choose how BitLocker-protected removable drives can be recovered	Enabled Allow data recovery agent Configure user storage of BitLocker recovery information: Allow 48-digit recovery password Allow 256-bit recovery key Omit recovery options from the BitLocker setup wizard Save BitLocker recovery information to AD DS for removable data drives Configure storage of BitLocker recovery information to AD DS: Backup recovery passwords and key packages Do not enable BitLocker until recovery information is stored to AD DS for removable data drives
Configure use of passwords for removable data drives	Enabled Require password for removable data drive Configure password complexity for removable data drives: Require password complexity Minimum password length for removable data drive: 14
Control use of BitLocker on removable drives	Enabled Allow users to apply BitLocker protection on removable data drives
Deny write access to removable drives not protected by BitLocker	Enabled
Enforce drive encryption type on removable data drives	Enabled Select the encryption type: Full encryption
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy	
Interactive logon: Machine account lockout threshold	10

3.19. Installation des applications et des drivers

Si la possibilité d'installer des applications peut être une exigence commerciale pour les utilisateurs, ce privilège peut être exploité par un adversaire. Un adversaire peut envoyer un e-mail à une application malveillante, ou héberger une application malveillante sur un site Web compromis, et utiliser des techniques d'ingénierie sociale pour convaincre les utilisateurs d'installer l'application sur leur poste de travail. Même si un accès privilégié est requis pour installer des applications, les utilisateurs utiliseront leur accès privilégié s'ils croient ou peuvent être convaincus que la nécessité d'installer l'application est légitime. De plus, si les applications sont configurées pour s'installer à l'aide de privilèges élevés, un adversaire peut exploiter cela en créant un package d'installation Windows Installer pour créer un nouveau compte qui appartient au groupe d'administrateurs intégrés local ou pour installer une application malveillante.
Alternativement, un adversaire peut tenter d'installer des pilotes qui ne sont pas pertinents pour un système afin d'introduire des failles de sécurité. Pour réduire ce risque, toutes les installations d'application et de pilote doivent être strictement contrôlées.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour contrôler les installations d'applications et de pilotes.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Configure Windows Defender SmartScreen	Enabled Pick one of the following settings: Warn and prevent bypass
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Explorer	
Configure Windows Defender SmartScreen	Enabled Pick one of the following settings: Warn and prevent bypass
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer	
Allow user control over installs	Disabled
Always install with elevated privileges	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Devices: Prevent users from installing printer drivers	Enabled
User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer	
Always install with elevated privileges	Disabled

3.20. Listes héritées et à exécution unique

Une fois que le code malveillant a été copié sur un poste de travail, un adversaire disposant d'un accès au registre peut le programmer à distance pour qu'il s'exécute (c'est-à-dire en utilisant la liste d'exécution unique) ou pour qu'il s'exécute automatiquement à chaque démarrage de Microsoft Windows (c'est-à-dire en utilisant l'ancienne liste d'exécution). Pour réduire ce risque, les listes héritées et à exécution unique doivent être désactivées. Cela peut interférer avec le fonctionnement des applications légitimes qui doivent s'exécuter automatiquement à chaque démarrage de Microsoft Windows. Dans de tels cas, le paramètre de stratégie de groupe Exécuter ces programmes à l'ouverture de session de l'utilisateur peut être utilisé pour exécuter la même fonction de manière plus sécurisée lorsqu'il est défini au niveau du domaine; toutefois, s'il n'est pas utilisé, ce paramètre de stratégie de groupe doit être désactivé plutôt que laissé dans son état non défini par défaut.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour désactiver l'utilisation des listes héritées et à exécution unique.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Logon	
Do not process the legacy run list	Enabled
Do not process the run once list	Enabled
Run these programs at user logon	Disabled

3.21. Comptes Microsoft

Une fonctionnalité de Microsoft Windows 10 est la possibilité de lier des comptes Microsoft (anciennement Windows Live ID) à des comptes locaux ou de domaine. Lorsque cela se produit, les paramètres et les fichiers d'un utilisateur sont stockés dans le cloud à l'aide de OneDrive plutôt que localement ou sur un contrôleur de domaine. Bien que cela puisse avoir l'avantage de permettre aux utilisateurs d'accéder à leurs paramètres et fichiers à partir de n'importe quel poste de travail (par exemple, un poste de travail d'entreprise, un ordinateur personnel, un café Internet), cela peut également poser un risque pour une organisation car ils perdent le contrôle de l'endroit où les

informations sensibles peuvent être consultées. . Pour réduire ce risque, les utilisateurs ne doivent pas lier des comptes Microsoft à des comptes locaux ou de domaine.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour désactiver la possibilité de lier des comptes Microsoft à des comptes locaux ou de domaine.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft account	
Block all consumer Microsoft account user authentication	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive	
Prevent the usage of OneDrive for file storage	Enabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Block Microsoft accounts	Users can't add or log on with Microsoft accounts

3.22. MSS settings

Les paramètres MSS sont des valeurs de registre précédemment identifiées par les experts en sécurité Microsoft qui peuvent être utilisées pour une sécurité accrue. Bien que bon nombre de ces valeurs de registre ne soient plus applicables dans les versions modernes de Microsoft Windows, certaines offrent toujours un avantage de sécurité. En ne spécifiant pas ces paramètres MSS, un adversaire peut être en mesure d'exploiter les faiblesses de la position de sécurité d'un poste de travail pour accéder à des informations sensibles. Pour réduire ce risque, les paramètres MSS qui sont toujours pertinents pour les versions modernes de Microsoft Windows doivent être spécifiés à l'aide des paramètres de stratégie de groupe.
Les modèles d'administration de stratégie de groupe pour les paramètres MSS sont disponibles sur le blog Microsoft Security Guidance33. Les fichiers ADMX et ADML peuvent être placés dans% SystemDrive% \ Windows \ SYSVOL \ domain \ Policies \ PolicyDefinitions sur le contrôleur de domaine et ils seront automatiquement chargés dans l'éditeur de gestion des stratégies de groupe.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour configurer les paramètres MSS qui sont toujours pertinents pour les versions modernes de Microsoft Windows.

Group Policy Setting	**Recommended Option**
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)	
MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	Enabled DisableIPSourceRoutingIPv6: Highest protection, source routing is completely disabled
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Enabled DisableIPSourceRouting: Highest protection, source routing is completely disabled
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Disabled
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Enabled

3.23. NetBIOS over TCP/IP

NetBIOS sur TCP / IP facilite un certain nombre de méthodes d'intrusion. Pour réduire ce risque, NetBIOS sur TCP / IP doit être désactivé. Étant donné que NetBIOS sur TCP / IP n'est utilisé que pour prendre en charge les anciens systèmes d'exploitation Microsoft Windows, tels que ceux antérieurs à Microsoft Windows 2000, il ne devrait pas y avoir d'exigence professionnelle pour son utilisation, sauf dans de très rares circonstances. NetBIOS sur TCP / IP peut être désactivé en définissant les paramètres NetBIOS sous les paramètres WINS IPv4 sur chaque interface réseau sur Désactiver NetBIOS sur TCP / IP. NetBIOS sur TCP / IP n'est pas pris en charge par IPv6.

3.24. Network authentication

L'utilisation de méthodes d'authentification de réseau non sécurisées peut permettre à un adversaire d'obtenir un accès non autorisé au trafic et aux services du réseau. Pour réduire ce risque, seules les méthodes d'authentification réseau sécurisées, idéalement Kerberos, doivent être utilisées pour l'authentification réseau.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour configurer Kerberos et, si nécessaire à des fins héritées, utiliser NTLMv2.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: Configure encryption types allowed for Kerberos	AES128_HMAC_SHA1 AES256_HMAC_SHA1
Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security Require 128-bit encryption

3.25. NoLMHash policy

Lorsque Microsoft Windows hache un mot de passe de moins de 15 caractères, il stocke à la fois un hachage LAN Manager (hachage LM) et un hachage Windows NT (hachage NT) dans la base de données SAM locale pour les comptes locaux ou dans le répertoire d'activités pour les comptes de domaine. Le hachage LM est nettement plus faible que le hachage NT et peut facilement être forcé brutalement. Pour réduire ce risque, la stratégie NoLMHash doit être implémentée sur toutes les stations de travail et contrôleurs de domaine. Le hachage LM étant conçu pour l'authentification des systèmes d'exploitation Microsoft Windows hérités, tels que ceux antérieurs à Microsoft Windows 2000, il ne devrait pas y avoir d'exigence commerciale pour son utilisation, sauf dans de très rares circonstances.
Le paramètre de stratégie de groupe suivant peut être implémenté pour empêcher le stockage des hachages LM pour les mots de passe. Tous les utilisateurs doivent être encouragés à modifier leur mot de passe une fois que ce paramètre de stratégie de groupe a été défini, car jusqu'à ce qu'ils le fassent, ils resteront vulnérables.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	

Network security: Do not store LAN Manager hash value on next password change	Enabled

3.26. Operating system functionality

Laisser les fonctionnalités inutiles dans Microsoft Windows activées peut offrir de plus grandes opportunités pour que des fonctionnalités potentiellement vulnérables ou mal configurées soient exploitées par un adversaire. Pour réduire ce risque, les fonctionnalités inutiles de Microsoft Windows doivent être désactivées ou supprimées.

3.27. Gestion de l'alimentation

Une méthode pour réduire la consommation d'énergie des postes de travail consiste à entrer dans un état de veille, d'hibernation ou de veille hybride après une période d'inactivité prédéfinie. Lorsqu'un poste de travail entre dans un état de veille, il conserve le contenu de la mémoire tout en mettant hors tension le reste du poste de travail; en veille prolongée ou en veille hybride, il écrit le contenu de la mémoire sur le disque dur dans un fichier d'hibernation (hiberfil.sys) et met le reste du poste de travail hors tension. Lorsque cela se produit, les informations sensibles telles que les clés de chiffrement peuvent être conservées en mémoire ou écrites sur le disque dur dans un fichier d'hibernation. Un adversaire disposant d'un accès physique au poste de travail et à la mémoire ou au disque dur peut récupérer les informations sensibles à l'aide de techniques médico-légales. Pour réduire ce risque, les états de veille, d'hibernation et de veille hybride doivent être désactivés.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour garantir que les états de veille, d'hibernation et de veille hybride sont désactivés.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings	
Allow standby states (S1-S3) when sleeping (on battery)	Disabled
Allow standby states (S1-S3) when sleeping (plugged in)	Disabled
Require a password when a computer wakes (on battery)	Enabled
Require a password when a computer wakes (plugged in)	Enabled
Specify the system hibernate timeout (on battery)	Enabled System Hibernate Timeout (seconds): 0
Specify the system hibernate timeout (plugged in)	Enabled System Hibernate Timeout (seconds): 0
Specify the system sleep timeout (on battery)	Enabled System Sleep Timeout (seconds): 0
Specify the system sleep timeout (plugged in)	Enabled System Sleep Timeout (seconds): 0
Specify the unattended sleep timeout (on battery)	Enabled Unattended Sleep Timeout (seconds): 0
Specify the unattended sleep timeout (plugged in)	Enabled Unattended Sleep Timeout (seconds): 0
Turn off hybrid sleep (on battery)	Enabled
Turn off hybrid sleep (plugged in)	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	

Show hibernate in the power options menu	Disabled
Show sleep in the power options menu	Disabled

3.28. PowerShell

Autoriser tout script PowerShell à s'exécuter expose une station de travail au risque qu'un script malveillant puisse être exécuté involontairement par un utilisateur. Pour réduire ce risque, les utilisateurs ne doivent pas avoir la possibilité d'exécuter des scripts PowerShell; cependant, si l'utilisation de scripts PowerShell est une exigence métier essentielle, seuls les scripts signés doivent être autorisés à s'exécuter.
S'assurer que seuls les scripts signés sont autorisés à s'exécuter peut fournir un niveau d'assurance qu'un script est digne de confiance et a été approuvé comme ayant un objectif commercial légitime.
Pour plus d'informations sur l'implémentation efficace de PowerShell, consultez la publication Securing PowerShell dans la publication Enterprise34.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour contrôler l'utilisation des scripts PowerShell.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell	
Turn on PowerShell Script Block Logging	Enabled
Turn on Script Execution	Enabled Execution Policy: Allow only signed scripts

3.29. Outils d'édition de la base de registre

Une méthode permettant au code malveillant de maintenir la persistance (c'est-à-dire de rester après le redémarrage d'un poste de travail) consiste à utiliser des privilèges administratifs pour modifier le registre (car les privilèges standard permettent uniquement la visualisation du registre). Pour réduire ce risque, les utilisateurs ne devraient pas avoir la possibilité de modifier le registre à l'aide des outils d'édition du registre (c'est-à-dire regedit) ou d'apporter des modifications silencieuses au registre (c'est-à-dire en utilisant des fichiers .reg).
Le paramètre de stratégie de groupe suivant peut être implémenté pour empêcher les utilisateurs d'afficher ou de modifier le registre à l'aide des outils de modification du registre.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\System	
Prevent access to registry editing tools	Enabled Disable regedit from running silently: Yes

3.30. Remote Assistance

Si l'assistance à distance peut être un outil professionnel utile pour permettre aux administrateurs système d'administrer à distance des postes de travail, elle peut également présenter un risque. Lorsqu'un utilisateur rencontre un problème avec son poste de travail, il peut générer une invitation d'assistance à distance. Cette invitation autorise toute personne qui y a accès à contrôler à distance le poste de travail qui a émis l'invitation. Les invitations peuvent être envoyées par e-mail, messagerie instantanée ou enregistrées dans un fichier. Si un adversaire parvient à intercepter une invitation, il pourra l'utiliser pour accéder au poste de travail de l'utilisateur. De plus, si le trafic réseau sur le port 3389 n'est pas bloqué pour accéder à Internet, les utilisateurs peuvent envoyer des invitations d'assistance à distance sur Internet, ce qui pourrait permettre l'accès à distance à leur poste de travail par un adversaire. Alors que l'assistance à distance n'accorde l'accès qu'aux privilèges de l'utilisateur qui a généré la demande, un adversaire peut installer une application de

journalisation des clés sur le poste de travail en préparation d'un administrateur système utilisant ses informations d'identification privilégiées pour résoudre les problèmes. Pour réduire ce risque, l'assistance à distance doit être désactivée.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour désactiver l'assistance à distance.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Remote Assistance	
Configure Offer Remote Assistance	Disabled
Configure Solicited Remote Assistance	Disabled

3.31. Remote Desktop Services

Si l'accès au bureau à distance peut être pratique pour les utilisateurs légitimes d'accéder aux postes de travail sur un réseau, il permet également à un adversaire d'accéder à d'autres postes de travail une fois qu'il a compromis un poste de travail initial et les informations d'identification de l'utilisateur. Ce risque peut être aggravé si un adversaire peut compromettre les informations d'identification d'administrateur de domaine ou les informations d'identification d'administrateur local communes. Pour réduire ce risque, les services Bureau à distance doivent être désactivés.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour désactiver les services Bureau à distance.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\ Remote Desktop Session Host\Connections	
Allow users to connect remotely by using Remote Desktop Services	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Allow log on through Remote Desktop Services	*<blank>*
Deny log on through Remote Desktop Services	Administrators NT AUTHORITY\Local Account

Sinon, si l'utilisation des services Bureau à distance est une exigence commerciale essentielle, elle doit être configurée de manière aussi sécurisée que possible et uniquement sur les postes de travail et pour les utilisateurs pour lesquels cela est explicitement requis.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour utiliser les services Bureau à distance de la manière la plus sécurisée possible.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation	
Remote host allows delegation of non-exportable credentials	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\ Remote Desktop Connection Client	
Configure server authentication for client	Enabled Authentication setting: Do not connect if authentication fails
Do not allow passwords to be saved	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\ Remote Desktop Session Host\Connections	

Allow users to connect remotely by using Remote Desktop Services	Enabled
Deny logoff of an administrator logged in to the console session	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\ Remote Desktop Session Host\Device and Resource Redirection	
Do not allow Clipboard redirection	Enabled
Do not allow drive redirection	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\ Remote Desktop Session Host\Security	
Always prompt for password upon connection	Enabled
Do not allow local administrators to customize permissions	Enabled
Require secure RPC communication	Enabled
Require use of specific security layer for remote (RDP) connections	Enabled Security Layer: SSL
Require user authentication for remote connections by using Network Level Authentication	Enabled
Set client connection encryption level	Enabled Encryption Level: High Level
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Allow log on through Remote Desktop Services	Remote Desktop Users
Deny log on through Remote Desktop Services	Administrators NT AUTHORITY\Local Account

3.32. Remote Procedure Call

L'appel de procédure à distance (RPC) est une technique utilisée pour faciliter les communications entre les applications client et serveur à l'aide d'une interface commune. RPC est conçu pour rendre l'interaction client et serveur plus facile et plus sûre en utilisant une bibliothèque commune pour gérer des tâches telles que la sécurité, la synchronisation et les flux de données. Si des communications non authentifiées sont autorisées entre les applications client et serveur, cela peut entraîner la divulgation accidentelle d'informations sensibles ou l'incapacité de tirer parti des fonctionnalités de sécurité RPC. Pour réduire ce risque, tous les clients RPC doivent s'authentifier auprès des serveurs RPC.
Le paramètre de stratégie de groupe suivant peut être implémenté pour garantir que les clients RPC s'authentifient auprès des serveurs RPC.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call	
Restrict Unauthenticated RPC clients	Enabled RPC Runtime Unauthenticated Client Restriction to Apply: Authenticated

3.33. Reporting system information

Microsoft Windows contient un certain nombre de fonctions intégrées pour, souvent automatiquement et de manière transparente, rapporter les informations système à Microsoft. Cela comprend les erreurs système et les informations de plantage ainsi que les inventaires des applications, fichiers, périphériques et pilotes du système. Si elles sont capturées par un

adversaire, ces informations peuvent exposer des informations potentiellement sensibles sur les postes de travail. Ces informations pourraient également être utilisées par la suite par un adversaire pour personnaliser le code malveillant afin de cibler des postes de travail ou des utilisateurs spécifiques. Pour réduire ce risque, toutes les fonctions intégrées qui signalent des informations système potentiellement sensibles doivent être dirigées vers un serveur de rapport d'erreurs Windows d'entreprise.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour empêcher que des informations système potentiellement sensibles soient signalées à Microsoft.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Microsoft Support Diagnostic Tool	
Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Application Compatibility	
Turn off Inventory Collector	Enabled
Turn off Steps Recorder	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds	
Allow Telemetry	Enabled 0 - Security [Enterprise Only]
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\ Advanced Error Reporting Settings	
Configure Corporate Windows Error Reporting	Enabled Corporate server name: *<organisation defined>* Connect using SSL Server port: *<organisation defined>*

3.34. Safe Mode

Un adversaire avec des informations d'identification utilisateur standard qui peut démarrer dans Microsoft Windows en utilisant le mode sans échec, le mode sans échec avec mise en réseau ou le mode sans échec avec les options d'invite de commande peut être en mesure de contourner les protections du système et les fonctionnalités de sécurité. Pour réduire ce risque, les utilisateurs disposant d'informations d'identification standard doivent être empêchés d'utiliser les options du mode sans échec pour se connecter.
L'entrée de registre suivante peut être implémentée à l'aide des préférences de stratégie de groupe pour empêcher les non-administrateurs d'utiliser les options du mode sans échec.

Registry Entry	Recommended Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	
SafeModeBlockNonAdmins	REG_DWORD 0x00000001 (1)

3.35. Secure channel communications

Périodiquement, les stations de travail connectées à un domaine communiquent avec les contrôleurs de domaine. Si un adversaire a accès à des communications réseau non protégées, il peut être en mesure de capturer ou de modifier des informations sensibles communiquées entre les postes de travail et les contrôleurs de domaine. Pour réduire ce risque, toutes les communications par canal sécurisé doivent être signées et chiffrées avec des clés de session fortes.

Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour garantir que les communications par canal sécurisé sont correctement signées et chiffrées.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Require strong (Windows 2000 or later) session key	Enabled

3.36. Security policies

En ne spécifiant pas de manière exhaustive les politiques de sécurité, un adversaire peut être en mesure d'exploiter les faiblesses des paramètres de stratégie de groupe d'un poste de travail pour accéder à des informations sensibles. Pour réduire ce risque, les politiques de sécurité doivent être spécifiées de manière exhaustive.
Les paramètres de stratégie de groupe suivants peuvent être implémentés, en plus de ceux spécifiquement mentionnés dans d'autres zones de ce document, pour former un ensemble complet de stratégies de sécurité.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Network\DNS Client	
Turn off multicast name resolution	Enabled
Computer Configuration\Policies\Administrative Templates\Network\WLAN Service\WLAN Settings	
Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Cloud Content	
Turn off Microsoft consumer experiences	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Turn off heap termination on corruption	Disabled
Turn off shell protocol protected mode	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds	
Prevent downloading of enclosures	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Search	
Allow indexing of encrypted files	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Game Recording and Broadcasting	
Enables or disables Windows Game Recording and Broadcasting	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Disabled
Network security: Force logoff when logon hours expire	Enabled

Network security: LDAP client signing requirements	Negotiate signing
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

3.37. Server Message Block sessions

Un adversaire qui a accès aux communications réseau peut tenter d'utiliser des outils de piratage de session pour interrompre, mettre fin ou voler une session SMB (Server Message Block). Cela pourrait potentiellement permettre à un adversaire de modifier des paquets et de les transmettre à un serveur SMB pour effectuer des actions indésirables ou se faire passer pour le serveur ou le client après qu'une authentification légitime a eu lieu pour accéder à des informations sensibles. Pour réduire ce risque, toutes les communications entre les clients et les serveurs SMB doivent être signées et tous les mots de passe doivent être correctement chiffrés.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour garantir la sécurité des communications entre les clients et les serveurs SMB. Notez que les paramètres de stratégie de groupe du guide de sécurité MS sont disponibles dans le cadre de Microsoft Security Compliance Toolkit.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
Configure SMB v1 client driver	Enabled Configure MrxSmb10 driver: Disable driver (recommended)
Configure SMB v1 server	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

3.38. Verrouillage des sessions

Un adversaire ayant un accès physique à un poste de travail sans surveillance avec une session déverrouillée peut tenter d'accéder de manière inappropriée à des informations sensibles ou mener des actions qui ne lui seront pas attribuées. Pour réduire ce risque, un verrouillage de session doit être configuré pour s'activer après un maximum de 15 minutes d'inactivité de l'utilisateur. De plus, sachez que des informations ou des alertes peuvent être affichées sur l'écran de verrouillage. Pour

réduire le risque de divulgation non autorisée d'informations, minimisez la quantité d'informations que l'écran de verrouillage est autorisé à afficher.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour définir le verrouillage de session

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	
Prevent enabling lock screen camera	Enabled
Prevent enabling lock screen slide show	Enabled
Computer Configuration\Policies\Administrative Templates\System\Logon	
Allow users to select when a password is required when resuming from connected standby	Disabled
Turn off app notifications on the lock screen	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Show lock in the user tile menu	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Ink Workspace	
Allow Windows Ink Workspace	Enabled Choose one of the following actions: On, but disallow access above lock
Computer Configuration\Policies\Windows Settings\Local Policies\Security Options	
Interactive logon: Machine inactivity limit	900 seconds
User Configuration\Policies\Administrative Templates\Control Panel\Personalization	
Enable screen saver	Enabled
Password protect the screen saver	Enabled
Screen saver timeout	Enabled Seconds: 900
User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications	
Turn off toast notifications on the lock screen	Enabled
User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content	
Do not suggest third-party content in Windows spotlight	Enabled

3.39. Software-based firewalls

Les pare-feu réseau échouent souvent à empêcher la propagation de code malveillant sur un réseau ou à un adversaire d'extraire des informations sensibles, car ils ne contrôlent généralement que les ports ou protocoles pouvant être utilisés entre les segments d'un réseau. De nombreuses formes de code malveillant sont conçues spécifiquement pour en tirer parti en utilisant des protocoles courants tels que HTTP, HTTPS, SMTP et DNS. Pour réduire ce risque, les pare-feu logiciels qui filtrent le trafic entrant et sortant doivent être correctement mis en œuvre. Les pare-feu logiciels sont plus efficaces que les pare-feu réseau car ils peuvent contrôler les applications et les services qui peuvent communiquer vers et depuis les postes de travail. Le pare-feu Windows intégré36 peut être utilisé pour contrôler le trafic entrant et sortant pour des applications spécifiques.

3.40. Sound Recorder

L'enregistreur de son est une fonctionnalité de Microsoft Windows qui permet d'enregistrer et de sauvegarder l'audio d'un appareil avec un microphone sous forme de fichier audio sur le disque dur local. Un adversaire disposant d'un accès distant à un poste de travail peut utiliser fonctionnalité pour enregistrer les conversations sensibles à proximité du poste de travail. Pour réduire ce risque, le magnétophone doit être désactivé.
Le paramètre de stratégie de groupe suivant peut être implémenté pour désactiver l'utilisation de Magnétophone.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Sound Recorder	
Do not allow Sound Recorder to run	Enabled

3.41. Standard Operating Environment

Lorsque les utilisateurs doivent installer, configurer et entretenir leurs propres postes de travail, cela peut très facilement conduire à un environnement incohérent et non sécurisé dans lequel des postes de travail particuliers sont plus vulnérables que d'autres. Cet environnement incohérent et non sécurisé peut facilement permettre à un adversaire de prendre pied dans un premier temps sur un réseau. Pour réduire ce risque, les postes de travail doivent se connecter à un domaine à l'aide d'un environnement d'exploitation standard contrôlé et configuré de manière centralisée par des professionnels expérimentés des technologies de l'information et de la sécurité de l'information.

3.42. System backup and restore

Un adversaire qui compromet un compte utilisateur avec des privilèges de sauvegarde de fichiers et de répertoires peut utiliser ce privilège pour sauvegarder le contenu d'un poste de travail. Ce contenu peut ensuite être transféré vers un poste de travail non connecté au domaine où l'adversaire a un accès administratif. De là, un adversaire peut restaurer le contenu et en prendre possession, contournant ainsi tous les contrôles d'accès d'origine qui étaient en place. De plus, si un utilisateur dispose de privilèges pour restaurer des fichiers et des répertoires, un adversaire pourrait exploiter ce privilège en l'utilisant pour restaurer les versions précédentes de fichiers qui ont pu être supprimés par les administrateurs système dans le cadre des activités de suppression de code malveillant ou pour remplacer des fichiers existants avec des variantes malveillantes. Pour réduire ce risque, la possibilité d'utiliser les fonctionnalités de sauvegarde et de restauration doit être limitée aux administrateurs.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour contrôler l'utilisation de la fonctionnalité de sauvegarde et de restauration.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Back up files and directories	Administrators
Restore files and directories	Administrators

3.43. System cryptography

Par défaut, lorsque les clés cryptographiques sont stockées dans Microsoft Windows, les utilisateurs peuvent y accéder sans saisir au préalable un mot de passe pour déverrouiller le magasin de certificats. Un adversaire qui compromet un poste de travail ou obtient un accès physique à un poste de travail déverrouillé peut utiliser ces clés utilisateur pour accéder à des informations sensibles ou à des ressources protégées par cryptographie. Pour réduire ce risque, des algorithmes de cryptage et une protection de clé solides doivent être utilisés sur les postes de travail.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour garantir l'utilisation d'algorithmes de chiffrement solides et une protection de clé renforcée.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
System cryptography: Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled

3.44. User rights policies

En ne spécifiant pas de manière exhaustive les stratégies de droits d'utilisateur, un adversaire peut être en mesure d'exploiter les faiblesses des paramètres de stratégie de groupe d'un poste de travail pour accéder à des informations sensibles. Pour réduire ce risque, les politiques de droits des utilisateurs doivent être spécifiées de manière exhaustive.
Les paramètres de stratégie de groupe suivants peuvent être implémentés, en plus de ceux spécifiquement mentionnés dans d'autres zones de ce document, pour former un ensemble complet de stratégies de droits d'utilisateur.

Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Access Credential Manager as a trusted caller	*<blank>*
Act as part of the operating system	*<blank>*
Allow log on locally	Administrators Users
Create a pagefile	Administrators
Create a token object	*<blank>*
Create global objects	Administrators LOCAL SERVICE NETWORK SERVICE SERVICE

Create permanent shared objects	*<blank>*
Debug programs	Administrators
Enable computer and user accounts to be trusted for delegation	*<blank>*
Force shutdown from a remote system	Administrators
Impersonate a client after authentication	Administrators LOCAL SERVICE NETWORK SERVICE SERVICE
Load and unload device drivers	Administrators
Lock pages in memory	*<blank>*
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Take ownership of files or other objects	Administrators

3.45. Virtualised web and email access

Un adversaire peut souvent fournir un code malveillant directement aux postes de travail via un accès Web et e-mail externe. Une fois qu'un poste de travail a été exploité, un adversaire peut utiliser ces mêmes voies de communication pour les communications bidirectionnelles afin de contrôler son code malveillant. Pour réduire ce risque, l'accès au Web et à la messagerie électronique sur les postes de travail doit se faire via un environnement virtuel non persistant (c'est-à-dire à l'aide de bureaux virtuels ou d'applications virtuelles). Lors de l'utilisation d'un environnement virtuel, les postes de travail recevront une protection supplémentaire contre les tentatives d'intrusion visant à exploiter les vulnérabilités de sécurité dans les navigateurs Web et les clients de messagerie, car toute tentative, en cas de succès, s'exécutera dans un environnement virtuel non persistant plutôt que sur un poste de travail local.

3.46. Web Proxy Auto Discovery protocol

Le protocole WPAD (Web Proxy Auto Discovery) aide à la détection automatique des paramètres de proxy pour les navigateurs Web. Malheureusement, WPAD a souffert d'un certain nombre de failles de sécurité graves. Les organisations qui ne comptent pas sur l'utilisation du protocole WPAD doivent le désactiver. Cela peut être réalisé en modifiant le fichier hôte de chaque poste de travail dans% SystemDrive% \ Windows \ System32 \ Drivers \ etc \ hosts pour créer l'entrée suivante: 255.255.255.255 wpad.

3.47. Windows Remote Management

Windows Remote Management (WinRM) 37 est l'implémentation Microsoft du WS-Management Protocol38 qui a été développé en tant que norme publique pour l'échange à distance de données de gestion entre les appareils qui implémentent le protocole. Si une authentification et un cryptage appropriés ne sont pas mis en œuvre pour ce protocole, le trafic peut être soumis à la création par

un adversaire. Pour réduire ce risque, la gestion à distance de Windows doit être configurée de manière sécurisée.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour sécuriser l'utilisation de la gestion à distance de Windows.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client	
Allow Basic authentication	Disabled
Allow unencrypted traffic	Disabled
Disallow Digest authentication	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service	
Allow Basic authentication	Disabled
Allow unencrypted traffic	Disabled
Disallow WinRM from storing RunAs credentials	Enabled

3.48. Windows Remote Shell access

Lorsque Windows Remote Shell est activé, il peut permettre à un adversaire d'exécuter à distance des scripts et des commandes sur les postes de travail. Pour réduire ce risque, Windows Remote Shell doit être désactivé.
Le paramètre de stratégie de groupe suivant peut être implémenté pour désactiver l'accès Windows Remote Shell.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell	
Allow Remote Shell Access	Disabled

3.49. Windows Search and Cortana

Dans le cadre de la fonctionnalité de recherche intégrée de Microsoft Windows, les utilisateurs peuvent rechercher des résultats Web en plus des résultats du poste de travail local. Cette fonctionnalité, si elle est utilisée, peut entraîner la divulgation accidentelle d'informations sensibles si des termes sensibles sont recherchés automatiquement sur le Web en plus du poste de travail local. Pour réduire ce risque, la possibilité de rechercher automatiquement sur le Web doit être désactivée.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour empêcher que les résultats de recherche Web ne soient renvoyés pour les termes de recherche des utilisateurs.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Search	
Allow Cortana	Disabled

Don’t search the web or display web results in Search	Enabled

3.50. Windows To Go

Une fonctionnalité de Microsoft Windows 10 est Windows To Go. Windows To Go permet aux utilisateurs de démarrer dans un espace de travail stocké sur un support USB à partir de n'importe quelle machine prenant en charge la configuration matérielle minimale requise. Bien que cela puisse être très bénéfique pour les initiatives BYOD ou d’accès à distance, cela peut également présenter un risque pour le réseau d’une organisation. Les postes de travail qui permettent le démarrage automatique des espaces de travail Windows To Go ne font pas de distinction entre les espaces de travail approuvés et les espaces de travail malveillants développés par un adversaire. En tant que tel, un adversaire peut utiliser un espace de travail malveillant qu'il a personnalisé avec la boîte à outils souhaitée pour tenter d'accéder à des informations sensibles sur le réseau. Pour réduire ce risque, le démarrage automatique du support Windows To Go doit être désactivé.
Le paramètre de stratégie de groupe suivant peut être implémenté pour désactiver le démarrage automatique du support Windows To Go.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Portable Operating System	
Windows To Go Default Startup Options	Disabled

4. PRIORITES FAIBLES

4.1. Displaying file extensions

Lorsque les extensions de types de fichiers connus sont masquées, un adversaire peut utiliser plus facilement des techniques d'ingénierie sociale pour convaincre les utilisateurs d'exécuter des pièces jointes malveillantes. Par exemple, un fichier nommé vulnérabilité_assessment.pdf.exe peut apparaître comme vulnérabilité_assessment.pdf pour un utilisateur. Pour réduire ce risque, le masquage des extensions pour les types de fichiers connus doit être désactivé. L'affichage des extensions pour tous les types de fichiers connus, combiné à l'éducation des utilisateurs et à la sensibilisation aux types de fichiers de pièces jointes dangereux, peut aider à réduire le risque que les utilisateurs exécutent des pièces jointes malveillantes.
L'entrée de registre suivante peut être implémentée à l'aide des préférences de stratégie de groupe pour empêcher le masquage des extensions des types de fichiers connus.

Registry Entry	Recommended Value
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	
HideFileExt	REG_DWORD 0x00000000 (0)

4.2. File and folder security properties

Par défaut, tous les utilisateurs ont la possibilité d'afficher les propriétés de sécurité des fichiers et des dossiers. Cela inclut les propriétés de sécurité associées aux fichiers et aux dossiers ainsi qu'aux utilisateurs et aux groupes auxquels ils se rapportent. Un adversaire pourrait utiliser ces informations pour cibler des comptes spécifiques qui ont accès à des informations sensibles. Pour réduire ce risque, les utilisateurs ne doivent pas avoir la possibilité d'afficher les propriétés de sécurité des fichiers et des dossiers.
Le paramètre de stratégie de groupe suivant peut être implémenté pour désactiver l'accès des utilisateurs à l'onglet de sécurité dans les propriétés des fichiers et des dossiers dans l'Explorateur de fichiers.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Remove Security tab	Enabled

4.3. Location awareness

Lorsque les utilisateurs interagissent avec Internet, leurs postes de travail fournissent souvent automatiquement des détails de géolocalisation aux sites Web ou aux services en ligne pour les aider à personnaliser le contenu spécifique à la région géographique de l'utilisateur (c'est-à-dire la ville à partir de laquelle il accède à Internet). Ces informations peuvent être capturées par un adversaire pour déterminer l'emplacement d'un utilisateur spécifique. Pour réduire ce risque, les services de localisation du système d'exploitation et des applications doivent être désactivés.
Les paramètres de stratégie de groupe suivants peuvent être mis en œuvre pour désactiver les services de localisation dans le système d'exploitation.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors	
Turn off location	Enabled
Turn off location scripting	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors\ Windows Location Provider	
Turn off Windows Location Provider	Enabled

4.4. Microsoft Store

Alors que les applications du Microsoft Store sont approuvées par Microsoft, il existe toujours un risque que les utilisateurs ayant accès au Microsoft Store puissent télécharger et installer des applications potentiellement malveillantes ou des applications qui provoquent des conflits avec d'autres applications approuvées sur leur poste de travail. Pour réduire ce risque, l'accès au Microsoft Store doit être désactivé.
Les paramètres de stratégie de groupe suivants peuvent être implémentés pour empêcher l'accès au Microsoft Store.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\ Internet Communication settings	
Turn off access to the Store	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Store	
Turn off the Store application	Enabled

4.5. Resultant Set of Policy reporting

Par défaut, tous les utilisateurs ont la possibilité de générer des rapports RSOP (Resultant Set of Policy) qui leur permet d'afficher les paramètres de stratégie de groupe appliqués à leur poste de travail et à leur compte d'utilisateur. Ces informations peuvent être utilisées par un adversaire pour déterminer les erreurs de configuration ou les faiblesses des paramètres de stratégie de groupe appliqués au poste de travail ou au compte d'utilisateur. Pour réduire ce risque, les utilisateurs ne doivent pas avoir la possibilité de générer des rapports RSOP.
Le paramètre de stratégie de groupe suivant peut être mis en œuvre pour désactiver la capacité des utilisateurs à générer des rapports RSOP.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\System\Group Policy	
Determine if interactive users can generate Resultant Set of Policy data	Enabled