04/02/2026

RAPPORT DE PROJET - EXIGENCES DE SECURITE POUR LES POSTES DE TRAVAIL

CARNET PAUL (BTS Prépa SIO NDLP AVRANCHES)

Stagiaire chez CESIO

RAPPORT DE PROJET - EXIGENCES DE SECURITE POUR LES POSTES DE TRAVAIL

Référentiel : CSN Exigences sécurité postes de travail v1.0 (23/04/2024)

Périmètre : Postes Clients Windows 10/11 (Domaine Active Directory)

Auteur : CARNET Paul | https://carnetpaul.fr

Organisation : CESIO

Date : 04 Février 2026

Crédits & Remerciements : Ce projet a été réalisé dans le cadre de mon stage de seconde année de BTS Services Informatiques aux Organisations (SIO), dans l'entreprise CESIO. L'implémentation technique s'appuie sur les recommandations de l'ANSSI et les bonnes pratiques Microsoft Security. Validation technique réalisée sur environnement de laboratoire virtualisé (Windows Server 2019) avec des tests sur des machines physiques liés au domaine active directory.

À titre informatif, et afin d'améliorer la lisibilité ainsi que la clarté technique, ce document a été rédigé avec l'assistance d'une intelligence artificielle, s'appuyant sur le référentiel « CSN – Exigences de sécurité des postes de travail v1.0 (23/04/2024) », afin de garantir l'exactitude, la cohérence et la conformité des informations présentées.

SOMMAIRE

1. CONTEXTE ET OBJECTIF

1.1 CONTEXTE DU PROJET

Dans un paysage numérique marqué par la recrudescence des cyberattaques (rançongiciels, vol de données, espionnage industriel), le poste de travail utilisateur constitue souvent le maillon faible et la porte d'entrée privilégiée pour les attaquants au sein du système d'information.

Ce projet s'inscrit dans une démarche de **durcissement (hardening)** de l'infrastructure informatique de mises à disposition des notaires clients de CESIO. Il vise à élever le niveau de sécurité des postes clients Windows 10/11 intégrés au domaine Active Directory, afin de limiter les risques de compromission initiale et de propagation latérale.

L'environnement technique repose sur un contrôleur de domaine Windows Server 2019 et des clients virtualisés, simulant un réseau d'entreprise standard soumis à des contraintes de production et de sécurité strictes.

1.2 LE REFERENTIEL EXG-SEC

Le projet est piloté par la mise en conformité vis-à-vis du référentiel d'exigences internes **"EXG-SEC"**. Ce référentiel s'inspire largement des recommandations de l'**ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) et des bonnes pratiques de Microsoft Security.

Il couvre plusieurs domaines critiques :

- La sécurité physique et périphérique (USB, BIOS).
- La gestion des identités et des accès (Mots de passe, Administrateurs locaux).
- La sécurité réseau et les communications.
- La surveillance et la journalisation des événements (Logging).

1.3 OBJECTIFS DE SECURITE

Les travaux réalisés répondent à quatre objectifs stratégiques majeurs :

1. **Réduire la surface d'attaque :** En désactivant les fonctionnalités inutiles (services superflus), en bloquant les vecteurs d'infection courants (clés USB, scripts PowerShell non signés) et en appliquant le principe de moindre privilège.
2. **Endiguer les mouvements latéraux :** En empêchant l'utilisation d'identifiants uniques sur tout le parc (mise en place de LAPS) et en cloisonnant les privilèges des administrateurs de domaine.

3. **Garantir l'intégrité du système :** En protégeant le processus de démarrage (ELAM, Secure Boot) et en interdisant les modifications non autorisées par l'utilisateur (verrouillage du Panneau de configuration).
4. **Assurer la traçabilité (Forensic) :** En activant une journalisation avancée (lignes de commandes, scripts, NTLM) permettant de détecter et d'analyser les incidents de sécurité a posteriori.

1.4 CONTRAINTES ET ADAPTATIONS

La mise en œuvre a dû prendre en compte des contraintes techniques spécifiques à l'environnement :

- **Infrastructure "Legacy" :** Utilisation de Windows Server 2019 nécessitant le déploiement de la version "Legacy" de LAPS (Local Administrator Password Solution).
- **Environnement isolé :** L'absence de connexion internet directe sur certains segments a imposé des méthodes de configuration manuelles (GPO et Registre) plutôt que l'usage de gestionnaires de paquets en ligne (Winget).
- **Limitations des modèles d'administration (ADMX) :** Certains paramètres de sécurité récents de Windows 10/11 n'étant pas exposés nativement dans les GPO du serveur 2019, l'usage des "Préférences de Registre" a été nécessaire pour forcer l'application des politiques de sécurité.

2. OUTILS ET STRUCTURE

Cette section détaille l'environnement technique, le référentiel normatif et l'organisation logique mis en place pour éprouver les exigences de sécurité.

2.1 REFERENTIEL DE CONFORMITE : LE STANDARD CSN

Le projet s'appuie strictement sur le référentiel **"Exigences de sécurité pour les postes de travail"** édicté par le **Conseil Supérieur du Notariat (CSN)**.

- **Version utilisée :** Version 1.0 du 23/04/2024.
- **Périmètre :** Ce document agrège les recommandations de l'ANSSI, de la CNIL, de Microsoft et des benchmarks CIS. Il définit un socle de sécurité obligatoire pour tout poste de travail traitant des données notariales.
- **Approche :** Chaque mesure implémentée dans ce projet correspond à un identifiant unique du référentiel (ex: *EXG-SEC-PDTxx*), garantissant une traçabilité parfaite entre la norme et la configuration technique.

2.2 ENVIRONNEMENT TECHNIQUE ET MATERIEL

L'infrastructure de test a été conçue pour reproduire fidèlement les conditions réelles d'une étude notariale ou d'une PME, en utilisant du matériel d'entreprise et une virtualisation de type "Type 1".

Infrastructure Serveur & Virtualisation

- **Serveur Physique :** DELL PowerEdge T430.
- **Hyperviseur :** Microsoft Hyper-V (Rôle installé sur le serveur physique).
- **Système d'exploitation Serveur (VM) : Windows Server 2019 Standard**.
    - *Justification du choix de version :* Bien que des versions plus récentes existent (2022/2025), Windows Server 2019 a été retenu car il représente la majorité du parc serveur actuellement en production chez les clients finaux. Cela permet de confronter les exigences de sécurité modernes (CSN 2024) aux contraintes réelles d'un OS serveur mature (niveau fonctionnel de domaine 2016/2019).

Infrastructure Réseau & Clients

- **Routage & Segmentation :** Routeur **Ubiquiti EdgeRouter X**. Il assure la séparation des flux et la simulation de la bordure réseau (Gateway).
- **Postes Clients :** PC physiques connectés au réseau labo, intégrés au domaine Active Directory pour valider l'application réelle des GPO (pas uniquement en virtuel).

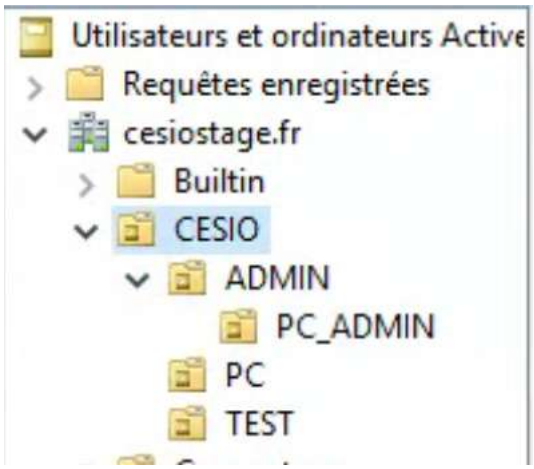
2.3 ORGANISATION DE L'ACTIVE DIRECTORY (SRV-AD)

L'annuaire Active Directory (cesiostage.fr) a été structuré de manière hiérarchique pour permettre une application granulaire des stratégies de sécurité (GPO). Cette segmentation est indispensable pour séparer les comptes d'administration, les postes de travail et les environnements de test.

Voici l'arborescence déployée sur le contrôleur de domaine **SRV-AD** :

A. Racine et Structure Principale (OU CESIO)

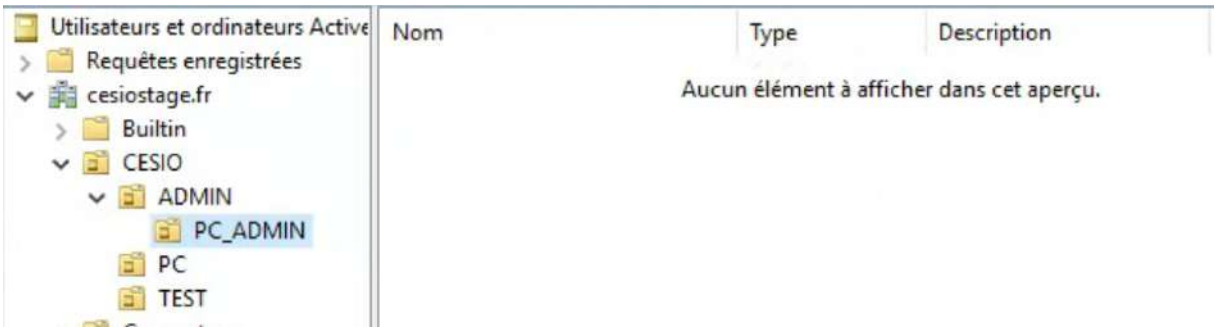
L'ensemble des objets gérés se trouve dans une Unité d'Organisation (OU) racine nommée **CESIO**, afin de ne pas impacter les conteneurs par défaut de Microsoft.



B. Gestion des Administrateurs (OU ADMIN)

Cette OU est critique. Elle contient les comptes à hauts privilèges et les groupes de sécurité dédiés à l'administration (LAPS, Support).

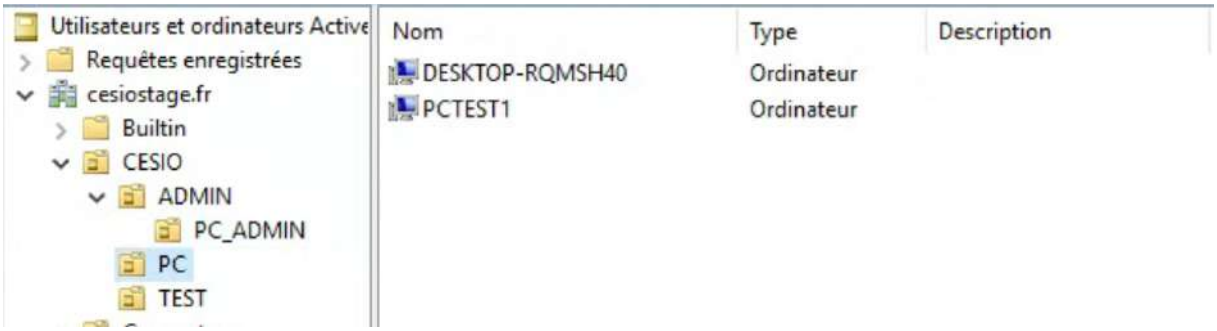
- **Contenu :** Comptes d'administration et groupes de sécurité (G_LAPS_Admins).
- **Sous-OU PC_ADMIN :** Destinée à accueillir les postes de travail dédiés aux administrateurs (conformément à l'exigence EXG-SEC-PDT61 sur le cloisonnement des postes d'administration). Actuellement vide pour les besoins du test, mais prête à l'emploi.



C. Gestion du Parc Informatique (OU PC)

C'est ici que sont appliquées la majorité des GPO de durcissement "Poste de Travail" (BitLocker, USB, LAPS, etc.).

- **Contenu :** Objets ordinateurs réels (DESKTOP-RQMSH40) et machines de test (PCTEST1).



D. Zone de Test Utilisateurs (OU TEST)

Cette zone permet de simuler des comportements utilisateurs standards sans droits d'administration, pour vérifier l'efficacité des restrictions (UAC, interdiction d'installation, etc.).

- **Contenu :** Utilisateurs lambda (test1, test2, test3) simulant des collaborateurs de l'étude.

3. DETAIL DES MESURES TECHNIQUES (EXIGENCES)

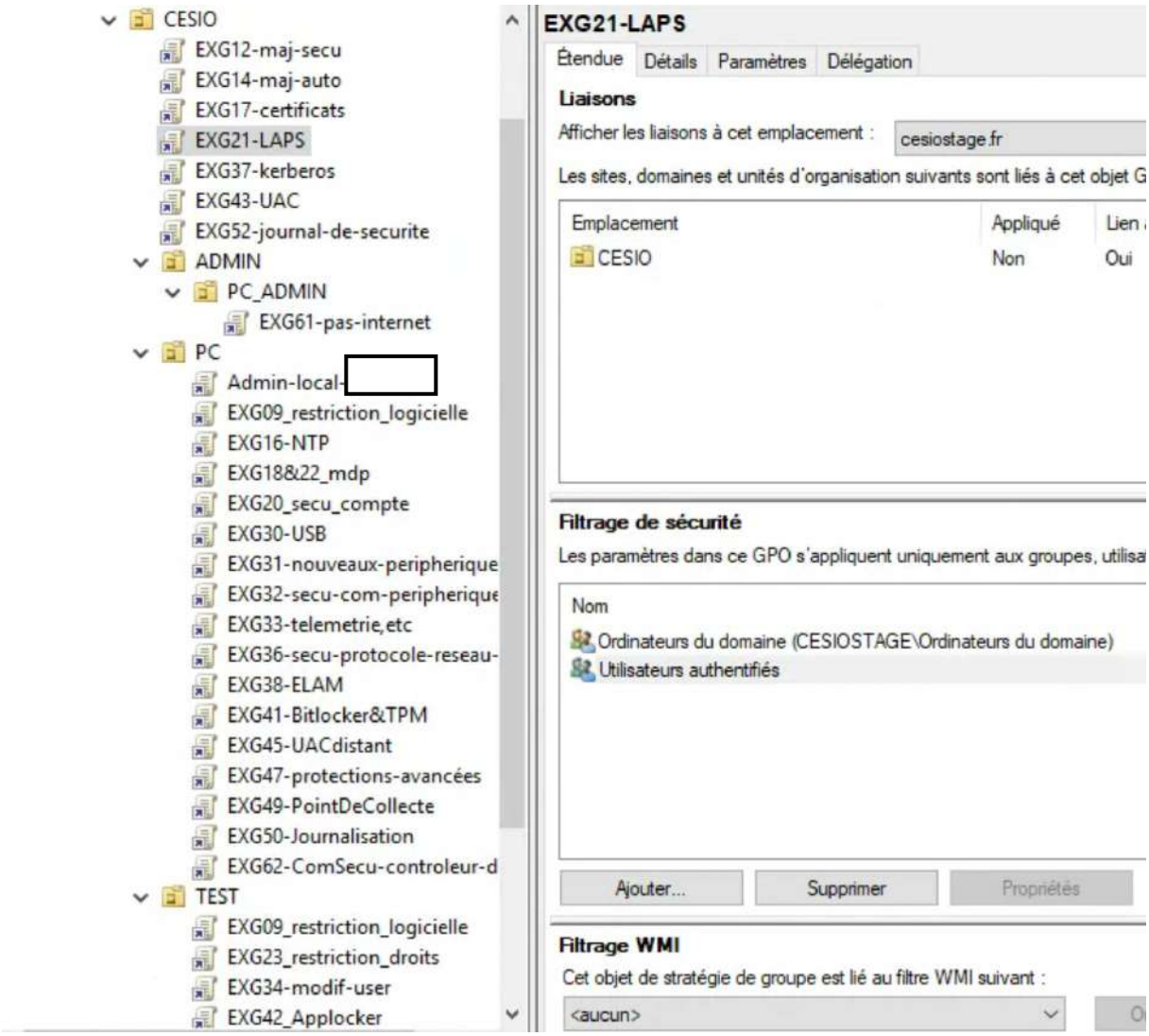
Ce chapitre détaille l'implémentation technique des contrôles de sécurité. La conformité repose majoritairement sur l'application de Stratégies de Groupe (GPO) centralisées, complétées par des scripts de configuration pour les éléments non couverts par les modèles d'administration standards.

3.1 STRATEGIE ET ORGANISATION DES GPO

Afin de garantir la maintenabilité et la lisibilité de la configuration, nous avons opté pour une approche **granulaire** plutôt que monolithique. Contrairement à une stratégie unique contenant tous les paramètres ("Default Domain Policy" surchargée), chaque exigence ou cluster d'exigences du référentiel CSN fait l'objet d'un Objet de Stratégie de Groupe (GPO) dédié.

Principes d'organisation :

- **Nommage Normalisé :** Chaque GPO débute par l'identifiant de l'exigence (ex: EXG30-USB) suivi d'une description courte. Cela permet un audit immédiat de la couverture fonctionnelle.
- **Ciblage par Unité d'Organisation (OU) :** Les GPO sont liées au plus près des objets qu'elles doivent impacter (voir Figure 6) :
    - **Racine (CESIO) :** GPO globales (ex: EXG21-LAPS, EXG17-certificats).
    - **OU PC :** Cœur du durcissement des stations de travail (ex: EXG30-USB, EXG41-Bitlocker, EXG50-Journalisation).
    - **OU ADMIN :** Restrictions spécifiques aux postes d'administration (ex: EXG61-pas-internet).



3.2 PERIMETRE D'APPLICATION ET EXCLUSIONS

Le référentiel CSN couvre un spectre large de la sécurité de l'information. Par conséquent, certaines exigences listées dans le tableau de synthèse (Chapitre 2) ne font pas l'objet d'une fiche technique GPO dans ce rapport.

Ces exclusions sont justifiées par la nature même des mesures, qui sortent du périmètre de configuration logique de Windows Server :

- **Sécurité Physique :** Les exigences telles que la fixation par câble antivol (EXG-SEC-PST02) ou l'usage de filtres écrans (EXG-SEC-PST03) sont des mesures organisationnelles et matérielles non configurables par logiciel.
- **Infrastructure Réseau :** Les configurations des équipements actifs (Routeur Ubiquiti, bornes Wi-Fi, segmentation VLAN) répondant aux exigences réseau (EXG-SEC-PDT24 à PDT29) sont traitées directement sur les équipements concernés et non via l'Active Directory.
- **Systèmes Tiers et Sauvegardes :** Les exigences relatives à la sauvegarde des données (EXG-SEC-PDT53 à PDT58) sont gérées par des solutions dédiées (NAS,

Veeam, Agents de sauvegarde externes) ou des procédures manuelles, indépendantes des stratégies de groupe Windows.

Les fiches suivantes se concentrent donc exclusivement sur les mesures de **durcissement logique** (« Hardening ») du système d'exploitation et de l'environnement utilisateur.

3.4 DÉTAIL DES MESURES TECHNIQUES (TABLE DES MATIERES DETAILLEE)

DETAIL DES MESURES TECHNIQUES (EXIGENCES)

3.4.1. SOCLE APPLICATIF ET MISES A JOUR

FICHE EXIGENCE : EXG-SEC-PDT09 (RESTRICTION LOGICIELLE)

1. Objectif de sécurité (Synthèse) Cette mesure vise à neutraliser l'installation de logiciels non autorisés ("Shadow IT") et l'exécution de charges malveillantes. L'objectif est de passer d'une logique permissive (tout est autorisé sauf ce qui est interdit) à une logique restrictive de **"Liste Blanche"** : par défaut, aucun programme ne peut s'exécuter sauf s'il est situé dans un répertoire système protégé et administré. De plus, les mécanismes d'auto-élévation sont proscrits.

2. Configuration Technique (GPO) La restriction est appliquée via les **Stratégies de restriction logicielle (SRP)** définies dans l'objet de stratégie de groupe (GPO) nommé **EXG09_restriction_logicielle**.

Les paramètres suivants ont été configurés dans *Configuration ordinateur > Paramètres de sécurité > Stratégies de restriction logicielle* :

- **Niveau de sécurité par défaut :** Le niveau global est défini sur **Rejeté (Disallowed)**. Concrètement, cela signifie que tout exécutable ou script lancé par un utilisateur est bloqué par le système d'exploitation, sauf s'il correspond à une règle d'autorisation explicite.
- **Périmètre d'application (Application forcée) :**
  - La restriction s'applique à **tous les fichiers de logiciels**, à l'exception des bibliothèques (DLL) pour ne pas impacter la stabilité du système.
  - La stratégie s'applique à **tous les utilisateurs exceptés les administrateurs locaux**. Cette exception est cruciale pour permettre aux équipes de support d'intervenir et d'installer des logiciels légitimes.
- **Règles de chemins d'accès (Autorisations - Liste Blanche) :** Afin de permettre le fonctionnement de Windows et des applications déployées par l'entreprise, des règles "Non restreint" ont été créées pour les répertoires sécurisés suivants :
  - %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot% (Dossier Windows).
  - %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir% (Dossier Program Files).
  - C:\Program Files (x86) (Pour la compatibilité 32 bits).
  - Puisque seuls les administrateurs ont le droit d'écrire dans ces dossiers, tout exécutable qui s'y trouve est considéré comme "de confiance".
- **Règles de blocage spécifiques (Durcissement) :** Des règles explicites de niveau "Rejeté" ont été ajoutées pour interdire l'usage des interpréteurs de commandes, souvent utilisés pour contourner les restrictions, même s'ils sont situés dans des dossiers système :
  - powershell.exe (Versions v1.0, x86 et x64).
  - powershell_ise.exe (Versions v1.0, x86 et x64).

    - pwsh.exe (PowerShell Core).
- **Types de fichiers surveillés :** La liste des extensions considérées comme du code exécutable a été vérifiée pour inclure les scripts potentiellement dangereux (.BAT, .CMD, .VBS, .PS1, .MSI, etc.).

FICHE EXIGENCE : EXG-SEC-PDT12 (MISES A JOUR AUTOMATIQUES)

1. Objectif de sécurité (Synthèse) Garantir le maintien en condition de sécurité (MCS) du parc informatique en automatisant l'installation des correctifs de sécurité critiques et des mises à jour de fonctionnalités. Cette mesure vise à réduire la fenêtre d'exposition aux vulnérabilités (CVE) dès leur correction par l'éditeur. Conformément à l'exigence, l'utilisateur final est dépossédé de la capacité à bloquer, retarder indéfiniment ou désactiver ces mises à jour.

2. Configuration Technique (GPO) L'automatisation est pilotée par la Stratégie de Groupe **EXG12-maj-secu**. Les paramètres ont été définis pour forcer le téléchargement et l'installation sans intervention utilisateur.

Les réglages se situent dans : Configuration ordinateur > Modèles d'administration > Composants Windows > Windows Update.

- **Planification de l'installation :**
    - Le paramètre **Configuration du service Mises à jour automatiques** est **Activé**.
    - **Mode d'installation :** 4 - Téléchargement automatique et planification des installations.
    - **Fréquence :** 0 - Tous les jours.
    - **Heure :** 19:00.
    - *Note :* L'option *"Installer les mises à jour d'autres produits Microsoft"* est cochée pour couvrir également les outils comme Office.
- **Interdiction du blocage utilisateur :**
    - Le paramètre **Supprimer l'accès à la fonctionnalité "Interrompre les mises à jour"** est **Activé**.
    - Cela empêche un utilisateur de mettre en pause le service Windows Update pour éviter un redémarrage, garantissant ainsi l'application rapide des correctifs.
- **Gestion des délais et redémarrages (Windows Update for Business) :**
    - Le paramètre **Spécifier une date d'échéance avant le redémarrage automatique pour l'installation de la mise à jour** est **Activé**.
        - Mises à jour de qualité (Sécurité) : délai de grâce de **7 jours**.
        - Mises à jour de fonctionnalités : délai de grâce de **7 jours**.
    - Le paramètre **Choisir quand recevoir les mises à jour qualité** est **Activé**, avec un délai de réception différé de **7 jours** après publication, permettant de s'assurer de la stabilité des correctifs avant déploiement massif.

FICHE EXIGENCE : EXG-SEC-PDT14 (MISES A JOUR LOGICIELS TIERS)

1. Objectif de sécurité (Synthèse) Au-delà du système d'exploitation, les applications bureautiques (Suite Office, lecteurs PDF) constituent des vecteurs d'attaque privilégiés. L'objectif est d'assurer que ces logiciels critiques disposent de leurs propres mécanismes de mise à jour automatique activés et verrouillés, afin de corriger les failles applicatives sans délai et sans action de l'utilisateur.

2. Configuration Technique (GPO) La configuration est centralisée dans la Stratégie de Groupe **EXG14-maj-auto**. Elle traite spécifiquement les deux logiciels cités dans l'exigence : Microsoft Office et Adobe Acrobat Reader.

- **Configuration Microsoft Office (via Modèles d'Administration) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Microsoft Office 2016 (ordinateur) > Mises à jour.
  - **Paramètre :** "Activer les mises à jour automatiques" est positionné sur **Activé**.
  - *Effet :* Force le moteur de mise à jour "Click-to-Run" d'Office à vérifier et installer les nouvelles versions en arrière-plan.
- **Configuration Adobe Acrobat Reader (via Registre) :**
  - En l'absence de modèles ADMX spécifiques déployés, la configuration est forcée via les **Préférences de Registre**.
  - *Chemin :* Configuration ordinateur > Préférences > Paramètres Windows > Registre.
  - **Clé configurée :** bUpdater.
    - **Ruche :** HKEY_LOCAL_MACHINE
    - **Chemin de la clé :** SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown
    - **Type :** REG_DWORD
    - **Valeur :** 1
  - *Effet :* La valeur 1 dans la clé FeatureLockDown force l'activation du service de mise à jour automatique d'Adobe et empêche sa désactivation par l'utilisateur.

FICHE EXIGENCE : EXG-SEC-PDT17 (MISE A JOUR DES CERTIFICATS)

1. Objectif de sécurité (Synthèse) La sécurité des communications (HTTPS, Signatures numériques, Authentification) repose sur une chaîne de confiance validée par des Autorités de Certification (CA). L'objectif est de s'assurer que le poste de travail dispose en permanence des dernières listes de révocation (CRL) et des certificats racines à jour. Cela permet de rejeter immédiatement un certificat compromis et d'accepter les nouvelles autorités légitimes sans intervention manuelle.

2. Configuration Technique (GPO) La gestion de la confiance numérique est centralisée dans la Stratégie de Groupe **EXG17-certificats**. Elle combine la gestion des stratégies de clé publique et les paramètres de communication internet.

- **Mise à jour automatique des racines (Modèles d'administration) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Système > Gestion de la communication Internet > Paramètres de communication Internet.
  - **Paramètre :** "Désactiver la mise à jour automatique des certificats racines" est positionné sur **Désactivé**.
  - *Explication technique :* En "Désactivant la désactivation", on **force l'activation**. Windows contactera donc automatiquement Windows Update pour récupérer les nouveaux certificats racines de confiance (CTL) et mettre à jour ceux existants.
- **Validation du chemin d'accès (Paramètres de Sécurité) :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique > Paramètres de validation du chemin d'accès du certificat.
  - **Magasins de confiance :** Le paramètre "Autorités de certification racine que les ordinateurs clients peuvent approuver" est configuré pour inclure à la fois les **"Autorités de certification racine tierce partie"** (publiques) et les **"Autorités de certification racine de l'entreprise"** (PKI interne).
  - Cela garantit que les postes valident correctement les certificats internes (Active Directory) tout en maintenant la confiance avec le web public.

3.4.2. GESTION DES IDENTITES ET ACCES

FICHE EXIGENCE : EXG-SEC-PDT16 (SYNCHRONISATION NTP)

1. Objectif de sécurité (Synthèse) La synchronisation précise de l'horloge système est critique pour la sécurité d'un domaine Active Directory. Elle répond à deux impératifs majeurs :

- **Authentification Kerberos :** Le protocole ne tolère qu'un décalage maximal de 5 minutes entre le client et le serveur. Au-delà, les tickets sont rejetés pour éviter les attaques par rejeu (Replay Attacks).
- **Traçabilité (Forensic) :** En cas d'incident, il est indispensable de pouvoir corréler les journaux d'événements de plusieurs machines à la seconde près.

2. Configuration Technique (GPO) La configuration est centralisée dans la Stratégie de Groupe **EXG16-NTP**. Elle force le service de temps Windows (W32Time) à utiliser des paramètres stricts.

- **Chemin :** Configuration ordinateur > Modèles d'administration > Système > Service de temps Windows > Fournisseurs de temps.
- **Activation du Client :**
  - Le paramètre **Activer le client NTP Windows** est positionné sur **Activé**.
- **Configuration du Client :**
  - Le paramètre **Configurer le client NTP Windows** est **Activé** avec les valeurs suivantes :
    - **NtpServer :** pool.ntp.org,0x9 (Serveur de référence défini, le flag 0x9 indique un mode Client/Serveur).
    - **Type :** NT5DS.
      - *Note technique importante :* La valeur NT5DS instruit le poste de travail de se synchroniser prioritairement via la hiérarchie du domaine (c'est-à-dire auprès du Contrôleur de Domaine), garantissant ainsi l'alignement parfait pour Kerberos.
    - **SpecialPollInterval :** 1024 (Intervalle d'interrogation en secondes).

FICHE EXIGENCE : EXG-SEC-PDT18 & 22 (POLITIQUE DE MOTS DE PASSE & COMPTE MACHINE)

1. Objectif de sécurité (Synthèse) Cette mesure vise à durcir la première ligne de défense du réseau : l'authentification.

- **Pour les utilisateurs (PDT18) :** Il s'agit de rendre les attaques par force brute ou par dictionnaire inefficaces en imposant une longueur et une complexité élevées. La rotation forcée limite la durée de vie d'un mot de passe potentiellement compromis.
- **Pour les ordinateurs (PDT22) :** Chaque poste joint au domaine possède son propre "compte machine" avec un mot de passe géré automatiquement par Windows. Accélérer la rotation de ce secret (par défaut 30 jours) réduit les risques d'usurpation d'identité de la machine (Machine-in-the-middle) ou d'exploitation de secrets LSA dumpés.

2. Configuration Technique (GPO) L'ensemble des stratégies de mots de passe (Utilisateurs et Machines) est regroupé dans l'objet GPO **EXG18&22_mdp**.

- **Politique de mot de passe utilisateur (Stratégies de comptes) :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de mot de passe.
  - **Paramètres configurés :**
    - **Longueur minimale du mot de passe :** 12 caractères (Bloque les mots de passe courts faciles à casser).
    - **Le mot de passe doit respecter des exigences de complexité :** Activé (Force l'usage de Majuscules, Minuscules, Chiffres, Spéciaux).
    - **Antériorité maximale du mot de passe :** 180 jours (Force le changement tous les 6 mois).
    - **Appliquer l'historique des mots de passe :** 12 mots de passe mémorisés (Empêche la réutilisation immédiate des anciens secrets).
    - **Antériorité minimale :** 1 jour (Empêche l'utilisateur de changer 12 fois de suite son mot de passe pour remettre le même).
- **Rotation du compte machine (Options de sécurité) :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité.
  - **Paramètre configuré :**
    - **Membre de domaine : ancienneté maximale du mot de passe du compte ordinateur :** 30 jours.
  - *Note technique :* Ce paramètre force le client Windows à initier une transaction de changement de mot de passe avec le Contrôleur de Domaine (DC) tous les mois, assurant la fraicheur du secret machine stocké dans la base SAM locale et l'Active Directory.

FICHE EXIGENCE : EXG-SEC-PDT20 (SECURISATION DES COMPTES ET SESSIONS)

1. Objectif de sécurité (Synthèse) Cette mesure vise à durcir les accès au poste de travail en traitant deux vecteurs de menaces :

- **Les attaques par force brute :** En verrouillant automatiquement un compte après plusieurs échecs, on rend inefficaces les attaques par dictionnaire ou les tentatives de devinette de mot de passe.
- **La fuite de données et le "Shoulder Surfing" :** En masquant les options de visualisation des mots de passe et en limitant les sollicitations de paramètres personnels (OOBE/Cloud), on garantit un environnement professionnel strict.

2. Configuration Technique (GPO) La configuration est centralisée dans la Stratégie de Groupe **EXG20_secu_compte**. Elle intervient à la fois sur les stratégies de sécurité locales et sur les modèles d'administration.

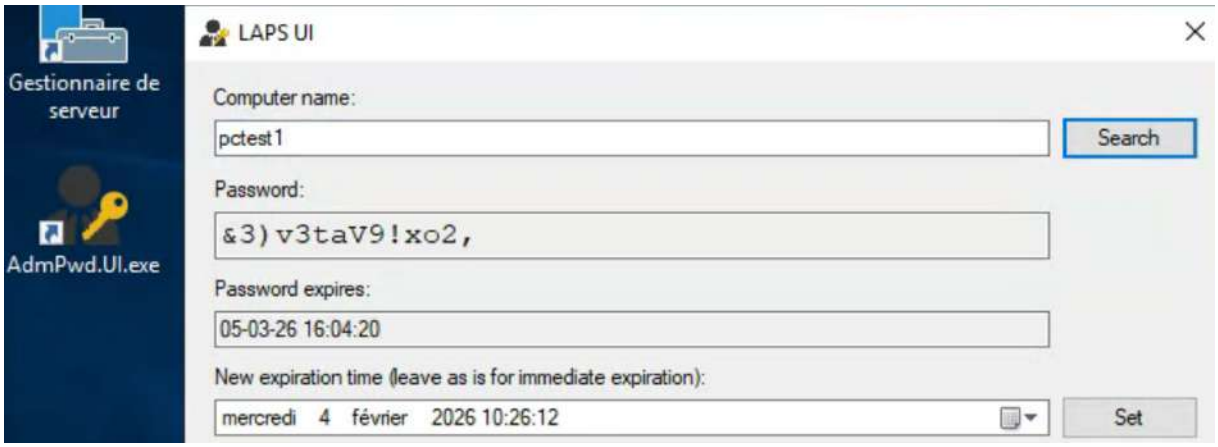
- **Protection contre le Force Brute (Stratégie de verrouillage) :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de verrouillage du compte.
  - **Seuil de verrouillage de comptes :** 5 tentatives d'ouverture de session non valides. (Après 5 échecs, le compte est bloqué).
  - **Durée de verrouillage de comptes :** 30 minutes. (Le compte reste inaccessible pendant cette durée, freinant drastiquement les attaques automatisées).
  - **Réinitialiser le compteur de verrouillages :** 30 minutes.
- **Durcissement de l'interface d'authentification (Modèles d'administration) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Composants Windows > Interface utilisateur d'informations d'identification.
  - **Paramètre :** "Ne pas afficher le bouton Affichage du mot de passe" est **Activé**.
  - *Effet :* Supprime l'icône "œil" dans les champs de mot de passe, empêchant une personne située derrière l'utilisateur de lire le mot de passe en clair.
- **Limitation des sollicitations personnelles (OOBE) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Composants Windows > OOBE.
  - **Paramètre :** "Ne pas lancer l'expérience des paramètres de confidentialité à l'ouverture de session" est **Activé**.
  - *Effet :* Empêche Windows de demander à l'utilisateur de configurer des services cloud ou de géolocalisation personnels lors de l'ouverture de session.

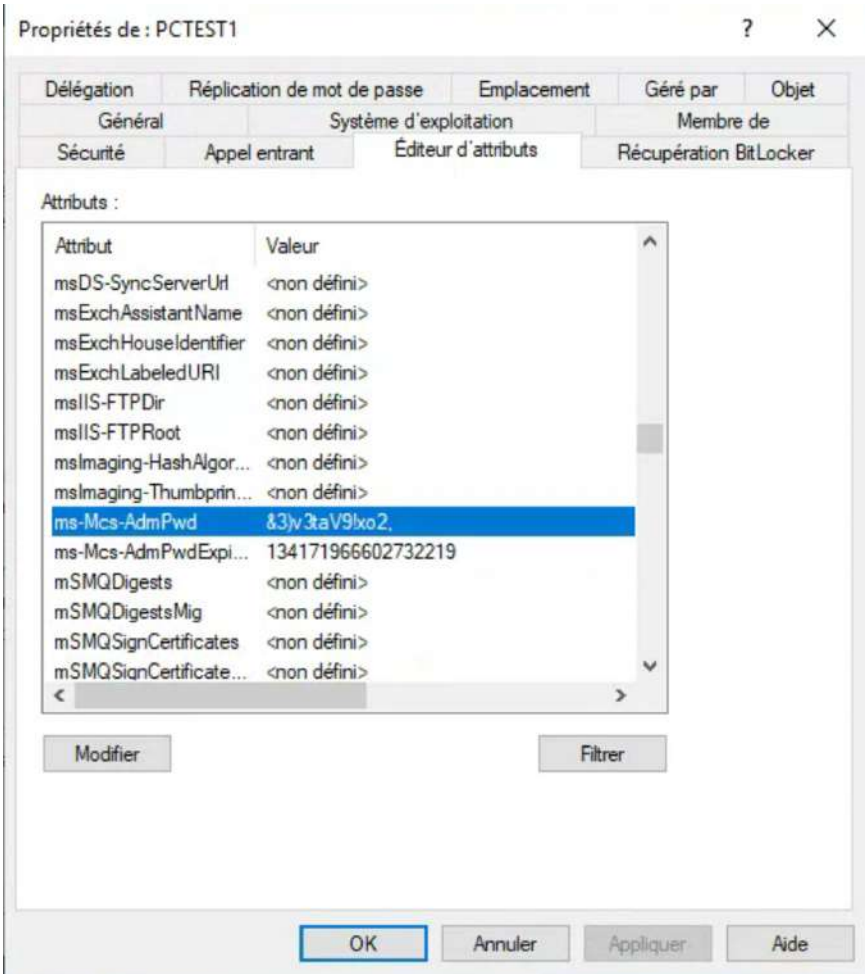
FICHE EXIGENCE : EXG-SEC-PDT21 (LAPS - GESTION ADMIN LOCAL)

1. Objectif de sécurité (Synthèse) L'utilisation d'un mot de passe administrateur local unique sur tout le parc informatique expose le réseau à des attaques par mouvements latéraux (type *Pass-the-Hash*). Si un seul poste est compromis, tous le sont. L'objectif est d'implémenter la solution **LAPS (Local Administrator Password Solution)** pour garantir que chaque ordinateur dispose d'un mot de passe administrateur **unique, complexe et renouvelé automatiquement** tous les 30 jours. Ce secret est stocké de manière sécurisée dans l'Active Directory.

2. Configuration Technique (GPO) L'implémentation a nécessité une phase de préparation de l'environnement Active Directory avant la configuration de la GPO **EXG21-LAPS**.

- **Pré-requis d'infrastructure (Installation) :**
  - Extension du schéma AD pour accueillir les nouveaux attributs (ms-Mcs-AdmPwd).
  - **Intégration des modèles :** Copie manuelle des fichiers de définition de stratégie (.admx, .adml) et des bibliothèques (.dll) dans le magasin central du contrôleur de domaine (\\SYSVOL\...\PolicyDefinitions) pour rendre les paramètres accessibles dans l'éditeur de GPO.
  - **Outils d'administration :** Installation du client lourd AdminPwd.UI.exe sur le poste d'administration pour permettre la récupération des mots de passe en cas de besoin.
- **Déploiement de l'Agent Client (Installation Logicielle) :**
  - *Chemin :* Configuration ordinateur > Paramètres du logiciel > Installation de logiciel.
  - **Package :** Local Administrator Password Solution (Version x64).
  - **Type de déploiement : Attribué**. L'agent MSI est installé automatiquement au redémarrage du poste client, permettant à la machine de dialoguer avec l'AD pour la rotation du mot de passe.
- **Configuration de la Stratégie (Modèles d'administration) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > LAPS.
  - **Enable local admin password management :** Activé (Active la rotation).
  - **Password Settings :** Configuration de la complexité (Majuscules + Minuscules + Chiffres + Spéciaux) et de la durée de vie (30 jours).
  - **Name of administrator account to manage :** Configuré pour cibler le compte administrateur de secours créé spécifiquement (car le compte natif SID-500 est désactivé).


Gestionnaire de serveur
AdmPwd.UI.exe
LAPS UI
Computer name:
pctest1
Search
Password:
&3)v3taV9!xo2,
Password expires:
05-03-26 16:04:20
New expiration time (leave as is for immediate expiration):
mercredi 4 février 2026 10:26:12
Set


Propriétés de : PCTEST1
Délégation
Réplication de mot de passe
Emplacement
Géré par
Objet
Général
Système d'exploitation
Membre de
Sécurité
Appel entrant
Éditeur d'attributs
Récupération BitLocker
Attributs :
Attribut
Valeur
msDS-SyncServerUrl <non défini>
msExchAssistantName <non défini>
msExchHouseIdentifier <non défini>
msExchLabeledURI <non défini>
msIIS-FTPDir <non défini>
msIIS-FTPRoot <non défini>
msImaging-HashAlgor... <non défini>
msImaging-Thumbprin... <non défini>
ms-Mcs-AdmPwd &3)v3taV9!xo2,
ms-Mcs-AdmPwdExpi... 134171966602732219
mSMQDigests <non défini>
mSMQDigestsMig <non défini>
mSMQSignCertificates <non défini>
mSMQSignCertificate... <non défini>
Modifier
Filtrer
OK
Annuler
Appliquer
Aide

FICHE EXIGENCE : EXG-SEC-PDT23 (RESTRICTION DES DROITS UTILISATEURS)

1. Objectif de sécurité (Synthèse) Cette mesure est l'application stricte du **Principe de Moindre Privilège**. Un utilisateur standard ne doit disposer que des droits strictement nécessaires à son travail. L'objectif est double :

- **Empêcher l'élévation de privilèges :** En garantissant qu'aucun utilisateur (hors équipe IT) n'est administrateur de sa machine.
- **Réduire la surface d'attaque "Living off the Land" :** En bloquant l'accès aux outils système (Invite de commande, Éditeur de registre, PowerShell) souvent utilisés par les attaquants pour explorer le réseau ou modifier le système une fois connectés.

2. Configuration Technique (GPO) Le durcissement est centralisé dans la Stratégie de Groupe **EXG23_restriction_droits**. Elle agit sur trois niveaux distincts :

- **Nettoyage du Groupe Administrateurs (Préférences) :**
  - *Chemin :* Configuration ordinateur > Préférences > Paramètres du Panneau de configuration > Utilisateurs et groupes locaux.
  - **Action :** Une stratégie "Mettre à jour" cible le groupe intégré **Administrateurs**.
  - **Configuration stricte :** Les options "Supprimer tous les utilisateurs membres" et "Supprimer tous les groupes de membres" sont cochées.
  - *Effet :* À chaque application de la GPO, Windows vide le groupe Administrateurs de tout compte parasite (utilisateur local, technicien temporaire oublié) et ne réinscrit que le groupe CESIOSTAGE\Admins du domaine.
- **Blocage des Outils Système (Modèles d'administration) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Système.
  - **Désactiver l'accès à l'invite de commandes (CMD) :** Activé. Cela empêche l'utilisateur de lancer cmd.exe.
  - **Empêcher l'accès aux outils de modifications du Registre (Regedit) :** Activé. Empêche l'utilisateur de contourner les restrictions via regedit.exe.
  - *Chemin :* Composants Windows > Windows PowerShell.
  - **Activer l'exécution des scripts :** Désactivé. Cela bloque l'exécution de scripts .ps1 sur le poste.
- **Attribution des Droits Utilisateur (Stratégies Locales) :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateurs.
  - **Restriction massive :** La plupart des privilèges sensibles (Modifier l'heure système, Arrêter le système à distance, Ouvrir une session en tant que service, etc.) ont été redéfinis pour n'inclure que le groupe **Admins du domaine**.
  - Cela empêche un utilisateur standard, même s'il trouvait une faille, d'exécuter des actions réservées au système.

FICHE EXIGENCE : EXG-SEC-PDT37 (DURCISSEMENT KERBEROS & NTLM)

1. Objectif de sécurité (Synthèse) L'authentification dans un domaine Active Directory repose historiquement sur plusieurs protocoles. Certains, comme LM, NTLMv1 ou le chiffrement DES/RC4 pour Kerberos, sont aujourd'hui obsolètes et vulnérables aux attaques par interception (Sniffing) et cassage de mot de passe (Cracking). L'objectif est de forcer l'utilisation exclusive de **Kerberos** avec un chiffrement robuste (AES) et, lorsque le repli est inévitable (pour les vieilles applications), de n'autoriser que **NTLMv2**, tout en interdisant formellement les protocoles faibles.

2. Configuration Technique (GPO) La configuration est appliquée via la Stratégie de Groupe **EXG37-kerberos**. Elle agit sur les options de sécurité locales pour modifier le comportement des fournisseurs de sécurité (SSP).

Les réglages se situent dans : Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité.

- **Durcissement NTLM (Niveau d'authentification) :**
  - **Paramètre :** "Sécurité réseau : niveau d'authentification LAN Manager".
  - **Valeur :** Envoyer uniquement une réponse NTLM version 2. Refuser LM et NTLM.
  - *Explication :* Cela interdit au poste de répondre aux défis d'authentification avec des hachages faibles (LM/NTLMv1), neutralisant ainsi les attaques de type "Pass-the-Hash" basiques sur ces protocoles.
- **Durcissement Kerberos (Types de chiffrement) :**
  - **Paramètre :** "Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos".
  - **Valeurs Désactivées :** DES_CBC_CRC, DES_CBC_MD5, RC4_HMAC_MD5. (Désactivation critique de RC4, souvent ciblé par les attaques "Kerberoasting").
  - **Valeurs Activées :** AES128_HMAC_SHA1, AES256_HMAC_SHA1, Futurs types de chiffrement.
  - *Explication :* Force le client Windows à négocier des tickets Kerberos chiffrés exclusivement en **AES** (Advanced Encryption Standard), le standard actuel de sécurité.
- **Restriction NTLM (Audit) :**
  - Des paramètres d'audit ont été activés ("Auditer le trafic NTLM entrant") pour identifier les applications qui continuent d'utiliser NTLM au lieu de Kerberos, dans le but de les migrer ou de les bloquer à terme.

3.4.3. PERIPHERIQUES ET MATERIEL

FICHE EXIGENCE : EXG-SEC-PDT30 (RESTRICTION USB & SUPPORTS AMOVIBLES)

1. Objectif de sécurité (Synthèse) Les supports amovibles (clés USB, disques externes) représentent un double risque majeur : l'exfiltration massive de données confidentielles et l'introduction de logiciels malveillants (Malware, Ransomware) contournant les défenses périmétriques. Conformément à une approche "Zero Trust", la stratégie appliquée est le **verrouillage par défaut**. L'usage de clés de stockage personnelles est interdit. Seuls les dispositifs cryptographiques indispensables à l'activité notariale (Clé REAL) font l'objet d'une validation spécifique.

2. Configuration Technique (GPO) Le durcissement est appliqué via la Stratégie de Groupe **EXG30-USB**. Contrairement à une approche permissive (liste noire), nous avons opté pour une interdiction radicale des classes de stockage de masse.

- **Chemin :** Configuration ordinateur > Modèles d'administration > Système > Accès au stockage amovible.
- **Blocage des Supports de Stockage :**
  - **Paramètre :** "Toutes les classes de stockage amovible : Refuser tous les accès".
  - **État : Activé**.
  - *Impact Technique :* Ce paramètre coupe l'accès en lecture et en écriture à tout périphérique se déclarant comme "Mass Storage" (Clés USB, Disques durs externes, Téléphones en mode transfert de fichiers).
- **Défense en profondeur (Exécution) :**
  - **Paramètre :** "Disques amovibles : refuser l'accès en exécution".
  - **État : Activé**.
  - *Objectif :* Même si un disque parvenait à être monté (faille pilote), aucun binaire (.exe, .bat) ne pourrait être lancé depuis ce support.

3. Note de Vigilance (Clé REAL) L'application de cette politique stricte nécessite une vérification impérative du fonctionnement de la **Clé REAL** (Dispositif de signature électronique).

- *Analyse technique :* Si la Clé REAL fonctionne uniquement comme une "Carte à puce" (Smart Card), elle ne sera pas impactée par ce blocage de "Stockage".
- *Exception potentielle :* Si la Clé REAL tente de monter un volume de stockage (pour des pilotes ou certificats), elle sera bloquée par la GPO actuelle. Dans ce cas, une dérogation par **ID de Périphérique (Device ID)** devra être configurée pour autoriser uniquement ce matériel spécifique tout en bloquant le reste.

FICHE EXIGENCE : EXG-SEC-PDT31 (VALIDATION PERIPHERIQUES & IMPRIMANTES)

1. Objectif de sécurité (Synthèse) L'installation libre de périphériques ou d'imprimantes par les utilisateurs introduit deux risques majeurs : l'instabilité du système (pilotes incompatibles) et l'infection (pilotes vérolés ou imprimantes malveillantes simulant un serveur légitime). L'objectif est d'interdire l'installation silencieuse ("Plug and Play" complet) pour tout nouveau matériel. L'intervention d'un administrateur doit être techniquement obligatoire pour valider et installer tout pilote ou périphérique non reconnu.

2. Configuration Technique (GPO) Le contrôle est assuré par la Stratégie de Groupe **EXG31-nouveaux-peripherique**. Elle agit sur deux vecteurs : les périphériques physiques (USB/PCI) et les imprimantes réseau.

- **Sécurisation des Imprimantes (Point & Print) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Imprimantes.
  - **Paramètre :** "Restrictions Pointer et imprimer" est **Activé**.
  - **Configuration détaillée :**
    - *Serveurs de confiance :* L'installation sans élévation est restreinte explicitement au serveur d'impression interne SRV-AD.
    - *Invites de sécurité :* Pour tout autre serveur ou nouvelle connexion, les options sont réglées sur **"Afficher l'avertissement et l'invite d'élévation"**.
  - *Effet :* Si un utilisateur tente d'ajouter une imprimante ne venant pas du serveur SRV-AD, Windows bloquera l'installation du pilote et demandera un login/mot de passe Administrateur.
- **Restriction d'Installation de Matériel (Device Guard) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Système > Installation de périphériques > Restrictions d'installation de périphériques.
  - **Paramètre 1 :** "Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie" est **Activé**.
    - *Impact :* Applique une logique de "refus par défaut" pour les nouveaux matériels non explicitement autorisés.
  - **Paramètre 2 :** "Autoriser les administrateurs à passer outre les stratégies de restriction d'installation de périphériques" est **Activé**.
  - *Impact :* Garantit que seuls les membres du groupe Administrateurs peuvent installer un nouveau matériel, validant ainsi physiquement et logiquement l'ajout du périphérique sur le poste.

FICHE EXIGENCE : EXG-SEC-PDT32 (SECURITE DES COMMUNICATIONS PERIPHERIQUES)

1. Objectif de sécurité (Synthèse) Sécuriser l'ensemble des canaux de communication entre le poste de travail et ses périphériques externes.

- **Impression & Scan :** Interdire les flux en clair (RAW 9100, FTP, SMBv1) pour éviter l'interception de documents confidentiels.
- **Connexion locale :** Bloquer les attaques physiques via DMA et restreindre l'usage du Bluetooth aux seuls périphériques d'interface humaine (HID) chiffrés.

2. Configuration Technique (GPO & Registre) La configuration est centralisée dans la GPO **EXG32-secu-com-peripherique**.

- **Déploiement Sécurisé des Imprimantes (Préférences GPO) :**
  - *Chemin :* Configuration ordinateur > Préférences > Paramètres du Panneau de configuration > Imprimantes.
  - **Action :** Création d'une imprimante TCP/IP partagée.
  - **Configuration du port :** Au lieu d'utiliser une IP standard, le chemin d'accès est forcé en **IPPS** (Internet Printing Protocol Secure).
  - **Syntaxe URL :** https://[IP-IMPRIMANTE]/ipp/print (ou le nom de file spécifique).
  - *Impact :* Force le poste client à encapsuler le flux d'impression dans du TLS/SSL (Port 443), rendant le document illisible s'il est capturé sur le réseau.
- **Durcissement du Spouleur (Registre via GPO) :**
  - *Chemin :* Configuration ordinateur > Préférences > Paramètres Windows > Registre.
  - **Clé 1 :** HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RpcAuthnLevelPrivacyEnabled.
    - **Valeur :** 1 (DWORD).
    - *Explication :* Impose le niveau d'authentification RPC "Privacy", qui chiffre les données échangées avec le serveur d'impression.
  - **Clé 2 :** HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RpcOverTcp.
    - **Valeur :** 1 (DWORD).
    - *Explication :* Privilégie TCP pour une meilleure gestion de la sécurité par rapport aux canaux nommés.
- **Protection DMA du Noyau (Modèles d'administration) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Système > Protection DMA du noyau.
  - **Paramètre :** "Stratégie d'énumération pour les appareils externes...".
  - **Valeur :** Bloquer tout (Block All).
  - *Registre associé :* HKLM\SOFTWARE\Policies\Microsoft\Windows\System\DmaGuardEnumerationPolicy = 0.

    - *Objectif :* Interdit l'accès direct à la mémoire RAM pour les périphériques Thunderbolt/USB4 non approuvés au démarrage.
- **Restriction Bluetooth :**
    - *Chemin :* Configuration ordinateur > Modèles d'administration > Composants Windows > Bluetooth.
    - **Paramètre :** "Autoriser uniquement les services Bluetooth spécifiés".
    - **Configuration :** Seuls les UUIDs correspondant aux services Clavier/Souris (HID) et Audio chiffré sont autorisés. Les services de transfert de fichiers (OBEX) sont bloqués.

3. Standards et Protocoles (Architecture) En complément du paramétrage Windows, une politique stricte est appliquée sur les équipements périphériques eux-mêmes :

- **Imprimantes Réseau :**
    - Activation obligatoire du protocole **IPPS** ou "Secure Printing" dans l'interface d'administration web de l'imprimante.
    - Désactivation des protocoles d'administration **SNMP v1 et v2c** (texte clair). Seul **SNMP v3** (avec authentification et chiffrement) est autorisé pour la supervision.
- **Scanners (Flux Entrants) :**
    - La fonction "Scan to Folder" (Numérisation vers dossier réseau) est configurée exclusivement en **SMBv3 avec chiffrement** (SMB Encryption activé sur le serveur de fichiers).
    - Alternative autorisée : **FTPS** (FTP over SSL).
    - Le FTP simple (Port 21 non chiffré) est strictement interdit et bloqué par le pare-feu du poste.

3.4.5. DURCISSEMENT SYSTEME ET RESEAU

FICHE EXIGENCE : EXG-SEC-PDT33 & 35 (CONFIDENTIALITE ET REDUCTION DE SURFACE)

1. Objectif de sécurité (Synthèse) Cette mesure vise deux objectifs complémentaires :

- **Confidentialité (PDT33) :** Windows 10/11 collecte par défaut une grande quantité de données (diagnostics, saisie, localisation) envoyées à Microsoft. L'objectif est de couper ces flux sortants pour garantir qu'aucune donnée d'entreprise ne fuite via la télémétrie.
- **Réduction de la surface d'attaque (PDT35) :** De nombreux services systèmes sont activés par défaut mais inutiles en entreprise (Xbox, P2P, UPnP). Chaque service actif est une porte d'entrée potentielle pour un attaquant (faille, élévation de privilèges). La stratégie est de désactiver tout ce qui n'est pas strictement nécessaire.

2. Configuration Technique (GPO) L'ensemble est configuré dans la Stratégie de Groupe **EXG33-telemetrie,etc**.

- **Désactivation de la Télémétrie (Modèles d'administration) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Composants Windows > Collecte des données et versions d'évaluation.
  - **Autoriser la télémétrie :** Configuré sur **Désactivé** (ou "0 - Sécurité" pour les versions Enterprise).
  - **Paramètres complémentaires désactivés :**
    - "Autoriser le pipeline de données commerciales" : **Désactivé**.
    - "Autoriser le traitement Analyses du bureau" : **Désactivé**.
    - "Autoriser l'envoi du nom de l'appareil dans les données de diagnostic" : **Désactivé**.
    - "Configurer les notifications d'activation de la télémétrie" : **Désactivé** (Pour ne pas solliciter l'utilisateur).
- **Désactivation des Services (Préférences) :**
  - *Chemin :* Configuration ordinateur > Préférences > Paramètres du Panneau de configuration > Services.
  - **Méthode de configuration :** Pour chaque service listé ci-dessous, une règle a été créée avec les propriétés strictes suivantes pour empêcher le service de démarrer, même manuellement :
    - **Action :** Arrêter le service (Stop).
    - **Type de démarrage :** Désactivé (Disabled).
    - **Délai d'attente :** 30 secondes.
  - **Liste des services désactivés (PDT35) :**
    - **Espionnage et Localisation :**
      - lfsvc (Service de géolocalisation).
      - DiagTrack (Expériences des utilisateurs connectés et télémétrie).
      - WerSvc (Service de rapport d'erreurs Windows).

- **Réseau Peer-to-Peer et Découverte (Risque de trafic latéral) :**
  - lltdsvc (Mappage de découverte de topologie).
  - PNRPsvc, p2pimsvc, p2psvc, PNRPAutoReg (Services de protocole de résolution de noms d'homologues).
  - upnphost (Hôte de périphérique UPnP - risque de sécurité élevé).
  - RemoteAccess (Routage et accès distant).
- **Partage et Protocoles Obsolètes :**
  - lanmanserver (Serveur - Partage de fichiers et imprimantes, désactivé sur les postes clients purs).
  - WMPNetworkSvc (Partage réseau du Lecteur Windows Media).
  - RpcLocator (Localisateur RPC - Obsolète).
  - SNMP (Service SNMP - Obsolète et non sécurisé en v1/v2).
- **Fonctionnalités Inutiles / Jeux :**
  - Services Xbox : XboxGipSvc, XblAuthManager, XblGameSave, XboxNetApiSvc.
  - Wisvc (Service Windows Insider).
  - LxssManager (Sous-système Windows pour Linux - WSL).
  - sshd (Serveur OpenSSH - Désactivé pour éviter les backdoors, l'administration se fait via outils dédiés).

FICHE EXIGENCE : EXG-SEC-PDT34 (INTERDICTION MODIFICATIONS SYSTEME)

1. Objectif de sécurité (Synthèse) L'objectif est de verrouiller l'environnement de travail pour garantir qu'un utilisateur standard ne puisse pas altérer la configuration du poste. Cela implique :

- **Protection de l'intégrité :** Empêcher le chargement de pilotes non signés ou la désactivation des outils de sécurité.
- **Verrouillage de l'interface :** Masquer les menus permettant de modifier les comptes utilisateurs (création de backdoor) ou la configuration réseau.
- **Principe de "Kiosque" :** L'utilisateur n'accède qu'aux réglages de confort (Souris, Affichage), tout le reste est masqué.

2. Configuration Technique (GPO) La configuration principale de l'interface est portée par la Stratégie de Groupe **EXG34-modif-user**, appliquée au niveau **Utilisateur**.

- **Restriction du Panneau de Configuration (Liste Blanche) :**
  - *Chemin :* Configuration utilisateur > Modèles d'administration > Panneau de configuration.
  - **Paramètre :** "N'afficher que les éléments du Panneau de configuration spécifiés" est **Activé**.
  - **Configuration :** Une liste stricte d'applets autorisées a été définie. Tout ce qui n'est pas dans cette liste est invisible et inaccessible pour l'utilisateur :
    - Microsoft.Mouse & Microsoft.Keyboard (Périphériques d'entrée).
    - Microsoft.Sound (Volume).
    - Microsoft.Display & Microsoft.Personalization (Affichage et fond d'écran).
    - Microsoft.DevicesAndPrinters (Gestion imprimantes).
    - Microsoft.Language & Microsoft.Region (Paramètres régionaux).
    - Microsoft.NetworkAndSharingCenter (Consultation état réseau uniquement).
    - *Autres outils métier :* SyncCenter, CredentialManager.
- **Verrouillage de l'Application "Paramètres" (Settings App Windows 10/11) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Panneau de configuration.
  - **Paramètre :** "Visibilité de la page de paramètres".
  - **Valeur :** hide:yourinfo;otherusers;family-group.
  - *Effet :* Masque spécifiquement les pages "Vos informations" et "Autres utilisateurs" pour empêcher la modification du compte local ou l'ajout d'utilisateurs "Famille/Invité".

3. Mesures Complémentaires (Architecture de Sécurité) Certains points de l'exigence sont couverts par des mécanismes transverses déjà documentés :

- **Blocage de la console de gestion utilisateurs (lusrmgr.msc) :**

    - Assuré par la **GPO EXG09 (Restrictions Logicielles)**. Une règle de hachage ou de chemin interdit explicitement l'exécution de cette console MMC pour les non-administrateurs.
- **Interdiction de PowerShell :**
    - Assurée par la **GPO EXG23 (Restrictions Droits)** et **EXG09**. L'exécutable powershell.exe est bloqué et l'exécution de scripts (.ps1) est désactivée.
- **Chargement de pilotes :**
    - Le privilège SeLoadDriverPrivilege est retiré aux utilisateurs standards via la restriction des droits (EXG23), rendant techniquement impossible le chargement d'un pilote noyau.

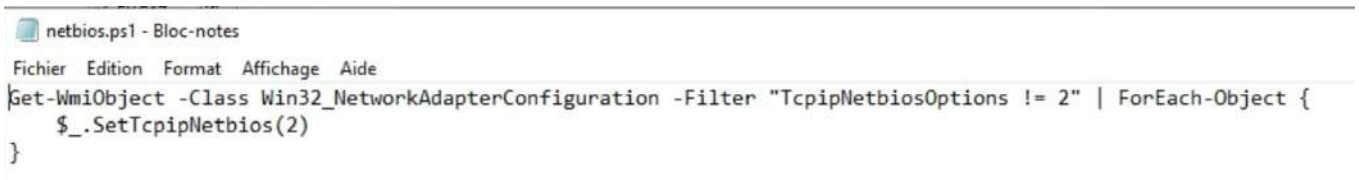
FICHE EXIGENCE : EXG-SEC-PDT36 (SECURISATION PROTOCOLES RESEAU)

1. Objectif de sécurité (Synthèse) Les réseaux Windows conservent par défaut des protocoles hérités (Legacy) pour la compatibilité, mais qui sont aujourd'hui des vecteurs d'attaques critiques :

- **LLMNR & NetBIOS :** Permettent les attaques de type *Poisoning* (via des outils comme Responder) pour intercepter les hachages de mots de passe.
- **SMBv1 :** Vulnérabilité critique exploitée par les ransomwares (type WannaCry).
- **Absence de Signature SMB :** Permet les attaques par relai (SMB Relay) où un attaquant se fait passer pour le serveur.
- **RPC/WinRM non sécurisés :** Permettent l'exécution de code à distance sans chiffrement. L'objectif est de "couper le bruit" sur le réseau en désactivant ces protocoles et en forçant le chiffrement et l'authentification forte pour les communications restantes.

2. Configuration Technique (GPO) La configuration est centralisée dans la Stratégie de Groupe **EXG36-secu-protocole-reseau-client**. Elle utilise une combinaison de scripts, de clés de registre et de modèles d'administration.

- **Désactivation de NetBIOS (Script de Démarrage) :**
  - Contrairement à une simple clé de registre, un script est utilisé pour désactiver NetBIOS sur toutes les interfaces réseaux actives.
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Scripts (démarrage/arrêt) > Démarrage.
  - **Script :** Powershell.
  - **Nom du script :** \\Srv-ad\netlogon\netbios.ps1.
  - *Action du script :* Il itère sur les adaptateurs réseaux et force l'option TcpipNetbiosOptions à 2 (Désactivé).



- **Éradication de SMB v1 (Préférences Registre) :**
  - *Chemin :* Configuration ordinateur > Préférences > Paramètres Windows > Registre.
  - **Clé configurée :** SMB1.
    - **Ruche :** HKEY_LOCAL_MACHINE.
    - **Chemin :** SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters.
    - **Type :** REG_DWORD.
    - **Valeur :** 0.
  - *Effet :* Le pilote SMBv1 est totalement désactivé au niveau du noyau.
- **Désactivation de LLMNR et Sécurisation RPC (Modèles d'administration) :**

    - *Chemin :* Configuration ordinateur > Modèles d'administration > Réseau > Client DNS.
        - **Paramètre :** "Désactiver la résolution de noms multidiffusion" est **Activé**. Cela stoppe les requêtes LLMNR sur le port 5355.
    - *Chemin :* Configuration ordinateur > Modèles d'administration > Système > Appel de procédure distante.
        - **Paramètre :** "Limiter les clients RPC non authentifiés" est **Activé**.
        - **Option :** "Authentifié". Cela rejette toute connexion RPC anonyme.
- **Sécurisation WinRM (Modèles d'administration) :**
    - *Chemin :* Composants Windows > Gestion à distance de Windows (WinRM) > Service WinRM.
    - **Paramètre :** "Autoriser l'authentification de base" est **Désactivé** (Bloque le mot de passe en clair).
    - **Paramètre :** "Autoriser le trafic non chiffré" est **Désactivé**.
- **Signature SMB et Durcissement NTLM (Options de Sécurité) :**
    - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité.
    - **Sécurité réseau : niveau d'authentification LAN Manager :** Envoyer uniquement une réponse NTLM version 2. Refuser LM et NTLM.
    - **Client réseau Microsoft : communications signées numériquement (toujours) :** Activé.
    - **Serveur réseau Microsoft : communications signées numériquement (toujours) :** Activé.
    - *Impact :* Garantit l'intégrité des paquets SMB contre les modifications en transit.

FICHE EXIGENCE : EXG-SEC-PDT61 (ISOLATION INTERNET POSTES D'ADMINISTRATION)

1. Objectif de sécurité (Synthèse) Conformément aux recommandations de l'ANSSI sur la sécurisation de l'administration (PA-022), les postes utilisés pour administrer le Système d'Information (SI) ne doivent jamais être exposés à Internet. L'objectif est de prévenir la compromission des comptes à hauts privilèges. Si un administrateur navigue sur le Web ou consulte ses mails depuis un poste d'administration, il expose le cœur du réseau (Active Directory) à des attaques de type "Drive-by download" ou Phishing. Ce poste doit être considéré comme un "sanctuaire" déconnecté du monde extérieur.

2. Configuration Technique (GPO & Architecture) La sécurisation repose sur une approche en "Défense en Profondeur" combinant cloisonnement réseau et restrictions logicielles via la GPO **EXG61-pas-internet**.

- **Structure Active Directory :**
  - Les postes d'administration ont été isolés dans une Unité d'Organisation (OU) spécifique nommée **PC_ADMIN**. La GPO ne s'applique qu'à ce conteneur pour ne pas impacter les utilisateurs standards.
- **Blocage par Pare-feu (Règles Sortantes) :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows avec sécurité avancée > Règles de trafic sortant.
  - **Règle :** "ANSSI - Blocage Internet et Mail".
  - **Action : Bloquer** la connexion.
  - **Protocoles ciblés :** Une liste exhaustive de ports a été définie pour interdire le Web et la Messagerie :
    - *Web :* 80 (HTTP), 443 (HTTPS), 8080.
    - *Mail :* 25, 465, 587 (SMTP), 110, 993 (POP/IMAP), 143.
  - *Effet :* Le pare-feu local rejette silencieusement toute tentative de sortie vers ces services, quel que soit le logiciel utilisé.
- **Configuration Proxy (Préférences Navigateur) :**
  - *Chemin :* Configuration utilisateur > Préférences > Paramètres du Panneau de configuration > Paramètres Internet.
  - **Paramétrage :** La détection automatique des paramètres est désactivée. Un proxy manuel est défini (ou forcé à une valeur locale) pour empêcher les navigateurs de tenter une résolution directe vers l'extérieur.
- **Cloisonnement Réseau (TCP/IP) :**
  - En complément de la GPO, une mesure architecturale stricte est appliquée : la configuration IP des cartes réseaux des postes d'administration ne comporte **aucune Passerelle par défaut (Default Gateway)**.
  - Cela rend le routage des paquets vers Internet techniquement impossible au niveau de la couche réseau, limitant le poste à son sous-réseau local et aux VLANs d'administration autorisés.

3.4.6 SECURITE LOGICIELLE ET PROTECTION

FICHE EXIGENCE : EXG-SEC-PDT38 (PROTECTION ELAM - ANTIMALWARE AU DEMARRAGE)

1. Objectif de sécurité (Synthèse) Les rootkits et bootkits sont des malwares sophistiqués qui s'installent au niveau du noyau (Kernel) ou des pilotes de démarrage, souvent avant même que l'antivirus ne soit actif, ce qui les rend invisibles. L'objectif de la fonctionnalité **ELAM (Early Launch Anti-Malware)** est de modifier l'ordre de démarrage de Windows pour que le pilote de l'antivirus (Microsoft Defender) soit chargé **en premier**. Il peut ainsi analyser et valider tous les autres pilotes avant leur exécution, bloquant toute tentative d'infection de bas niveau.

2. Configuration Technique (GPO) La configuration est centralisée dans la Stratégie de Groupe **EXG38-ELAM**. Elle utilise à la fois les modèles d'administration pour la politique et les préférences de registre pour le renforcement.

- **Configuration de la Stratégie (Modèles d'administration) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Système > Logiciel anti-programme malveillant à lancement anticipé.
  - **Paramètre :** "Stratégie d'initialisation des pilotes de démarrage" est **Activé**.
  - **Politique retenue :** Bons, inconnus et mauvais mais critiques.
  - *Justification technique :* Ce réglage autorise le chargement des pilotes signés (Bons) et ceux non classifiés (Inconnus), mais bloque les pilotes identifiés comme "Mauvais" (Malveillants), sauf si leur absence empêche totalement le démarrage du système (Critiques). Cela offre un équilibre entre sécurité maximale et disponibilité du poste (évite les écrans bleus en cas de faux positif critique).
- **Renforcement par Registre (Préférences) :**
  - Afin de garantir l'application de cette politique même si le service de stratégie de groupe a un délai, la valeur est forcée directement dans le registre.
  - *Chemin :* Configuration ordinateur > Préférences > Paramètres Windows > Registre.
  - **Clé configurée :** DriverLoadPolicy.
    - **Ruche :** HKEY_LOCAL_MACHINE
    - **Chemin :** SOFTWARE\Policies\Microsoft\Windows\System
    - **Valeur :** 0x3 (3) (Correspond à l'option "Bons, inconnus et critiques").

FICHE EXIGENCE : EXG-SEC-PDT41 (CHIFFREMENT BITLOCKER & TPM)

1. Objectif de sécurité (Synthèse) Le vol physique d'un ordinateur portable ou d'un disque dur est un risque majeur de fuite de données. L'objectif est de chiffrer l'intégralité du disque système (Full Disk Encryption) pour rendre les données illisibles sans la clé de déchiffrement. Cette clé est protégée par la puce de sécurité matérielle **TPM (Trusted Platform Module)** du poste. De plus, pour éviter toute perte de données en cas d'oubli du code PIN ou de panne, les clés de recouvrement doivent être automatiquement sauvegardées et centralisées dans l'Active Directory, sans que l'utilisateur puisse s'y opposer.

2. Configuration Technique (GPO) La configuration est pilotée par la Stratégie de Groupe **EXG41-Bitlocker&TPM**, située dans Configuration ordinateur > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker.

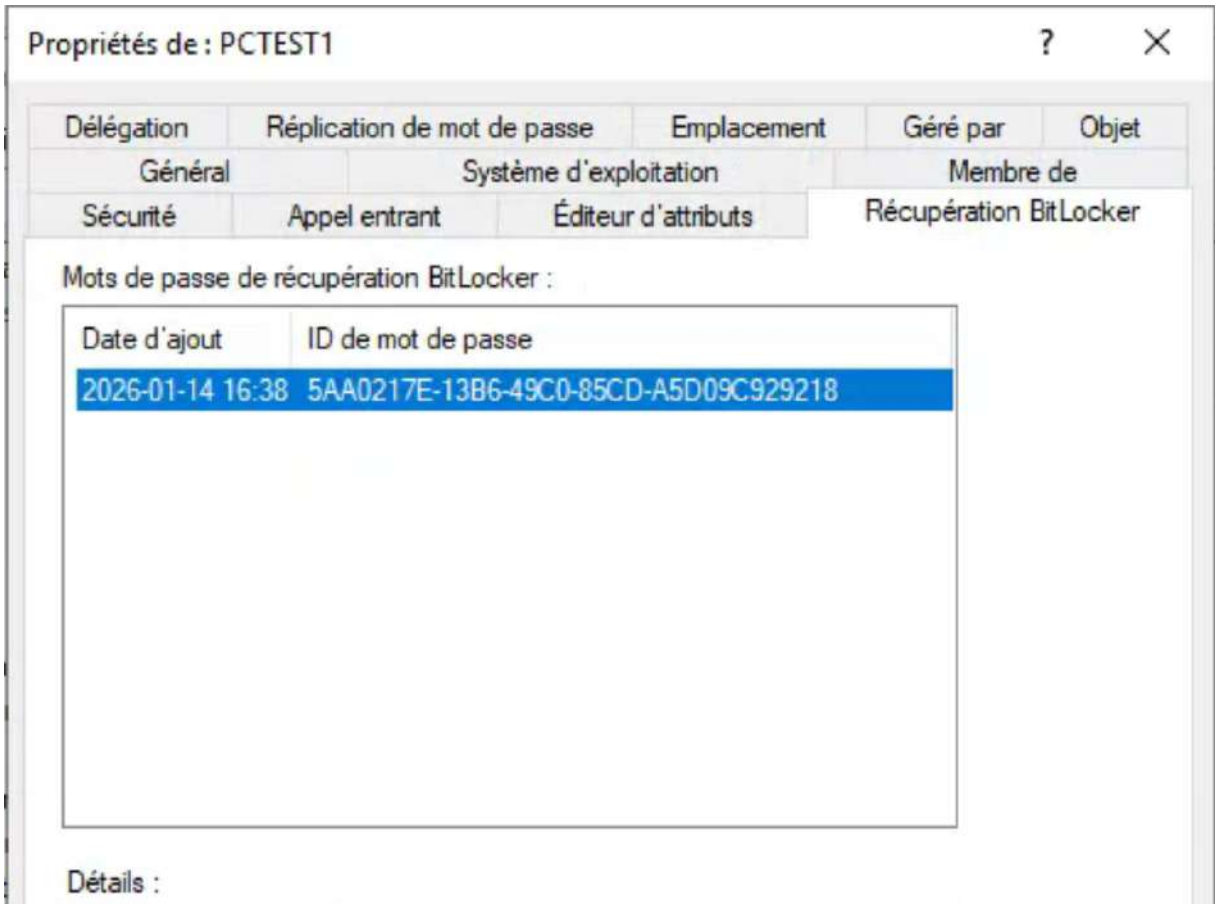
- **Algorithme de Chiffrement (Robustesse) :**
  - **Paramètre :** "Choisir la méthode et la puissance de chiffrement des lecteurs (Windows 10...)".
  - **Configuration :** L'algorithme **XTS-AES 128 bits** a été sélectionné pour tous les types de lecteurs (Système, Données fixes, Amovibles). Cet algorithme offre le meilleur compromis performance/sécurité pour les SSD modernes.
- **Sauvegarde Active Directory (Recouvrement) :**
  - **Paramètre :** "Enregistrer les informations de récupération BitLocker dans les services de domaine Active Directory".
  - **Configuration :** L'option **"Exiger la sauvegarde BitLocker vers les services de domaine Active Directory"** est activée.
  - *Sécurité critique :* Si le poste ne parvient pas à contacter le Contrôleur de Domaine pour déposer sa clé, le chiffrement ne se lance pas (Fail-safe).
- **Authentification au Démarrage (Lecteurs du système d'exploitation) :**
  - **Paramètre :** "Exiger une authentification supplémentaire au démarrage".
  - **Configuration :**
    - **TPM :** Autorisé (Utilisé par défaut pour déverrouiller le disque de manière transparente si le poste n'a pas été modifié).
    - **Code PIN :** Autorisé (Permet d'ajouter une couche "Ce que je sais" en plus du TPM).
    - *Note :* L'option "Autoriser BitLocker sans un module de plateforme sécurisée compatible" est cochée pour permettre le chiffrement (via mot de passe/clé USB) sur les quelques postes dépourvus de puce TPM.

3. Mise en œuvre Opérationnelle (Procédure) L'application de la GPO prépare le terrain mais le chiffrement nécessite des actions spécifiques :

- **Pré-requis Serveur (Infrastructure) :**
  - Installation de la fonctionnalité **"Outils de chiffrement de lecteur BitLocker"** (BitLocker Drive Encryption Administration Utilities) sur le

serveur AD. Cela ajoute l'onglet "Récupération BitLocker" dans la console "Utilisateurs et ordinateurs AD", permettant aux admins de retrouver les clés de secours.

- **Activation sur le Poste (Déploiement) :**
  - Une fois la GPO descendue, l'activation initiale se fait manuellement (ou par script) : **Clic droit sur le disque C: > Activer BitLocker**.
  - Le système vérifie alors la conformité avec la GPO, sauvegarde la clé dans l'AD, et lance le chiffrement en arrière-plan.



FICHE EXIGENCE : EXG-SEC-PDT42 (CONTROLE D'APPLICATION APPLOCKER)

1. Objectif de sécurité (Synthèse) AppLocker est l'évolution moderne des stratégies de restriction logicielle (SRP). Son objectif est d'appliquer un contrôle strict en "Liste Blanche" sur les exécutables, les scripts et les installateurs. Concrètement, un utilisateur standard ne doit pouvoir lancer que des applications situées dans les répertoires protégés du système (Program Files, Windows). Tout exécutable situé dans un profil utilisateur (Téléchargements, AppData, Temp) — lieux de prédilection des virus et ransomwares — est bloqué par défaut. Les administrateurs conservent une liberté totale pour la maintenance.

2. Configuration Technique (GPO) La configuration est portée par la Stratégie de Groupe **EXG42_Applocker** et se décompose en deux volets indissociables : l'activation du service moteur et la définition des règles.

- **Pré-requis Système (Service Identité) :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Services système.
  - **Service : Identité de l'application** (AppIDSvc).
  - **Mode de démarrage :** Configuré sur **Automatique**.
  - *Explication :* Ce service est responsable de la vérification des signatures numériques et des chemins d'accès à chaque lancement de programme. S'il est arrêté, AppLocker est inopérant.
- **Définition des Règles AppLocker :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de contrôle de l'application > AppLocker.
  - **Mode d'application :** Configuré sur **"Appliquer les règles"** (Enforce) pour les règles de l'exécutable. (Le mode "Audit uniquement" est désactivé pour garantir le blocage effectif).
- **Détail des Règles (Règles de l'exécutable) :** Les règles par défaut ont été générées pour créer la "Liste Blanche" système :
  - **Autoriser - Tout le monde - %PROGRAMFILES%* :** Permet l'exécution de tous les logiciels installés légitimement dans les dossiers Programmes.
  - **Autoriser - Tout le monde - %WINDIR%* :** Permet le fonctionnement du système d'exploitation Windows.
  - **Autoriser - Administrateurs - * :** Accorde le droit d'exécution complet (sans restriction de chemin) aux membres du groupe Administrateurs pour la maintenance.
  - *Sécurité par défaut :* Tout ce qui ne correspond pas à ces trois règles (ex: un .exe sur le Bureau ou dans C:\Temp) est implicitement bloqué.

FICHE EXIGENCE : EXG-SEC-PDT43 & 45 (CONTROLE DE COMPTE UTILISATEUR - UAC)

1. Objectif de sécurité (Synthèse) Le Contrôle de Compte Utilisateur (UAC) est une barrière fondamentale qui empêche les applications d'obtenir des droits administratifs silencieusement.

- **Protection locale (PDT43) :** L'objectif est de garantir que toute élévation de privilèges (installation de logiciel, modification système) nécessite une interaction humaine explicite sur un "Bureau Sécurisé" isolé des autres processus. Pour un utilisateur standard, cela impose la saisie d'un mot de passe administrateur.
- **Protection distante (PDT45) :** L'objectif est de bloquer les attaques de mouvement latéral (Pass-the-Hash) utilisant des comptes locaux. En restreignant l'UAC à distance, on empêche un compte administrateur local compromis sur un poste d'exécuter des commandes administratives à travers le réseau sur un autre poste.

2. Configuration Technique (GPO) La configuration est répartie sur deux Stratégies de Groupe distinctes pour la gestion locale et le verrouillage distant.

- **Configuration UAC Locale (GPO : EXG43-UAC)**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité.
  - **Paramètres clés configurés :**
    - **Mode Approbation Administrateur :** "Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation..." est **Activé**. (Force même les admins à approuver les actions).
    - **Bureau Sécurisé :** "Passer au Bureau sécurisé lors d'une demande d'élévation" est **Activé**. (Grise l'écran et empêche les malwares de cliquer sur "Oui" à la place de l'utilisateur).
    - **Comportement (Utilisateurs Standard) :** Configuré sur **"Demande d'informations d'identification"**. (L'utilisateur doit saisir un login/mdp admin pour élever ses droits).
    - **Comportement (Administrateurs) :** Configuré sur **"Demande de consentement"**. (Un clic de validation est requis, empêchant les élévations silencieuses en arrière-plan).
- **Restriction UAC Distante (GPO : EXG45-UACdistant)**
  - Cette configuration se fait via le Registre car il n'existe pas d'ADMX natif pour ce réglage précis de sécurité (LocalAccountTokenFilterPolicy).
  - *Chemin :* Configuration ordinateur > Préférences > Paramètres Windows > Registre.
  - **Clé configurée :** LocalAccountTokenFilterPolicy.
    - **Ruche :** HKEY_LOCAL_MACHINE
    - **Chemin :** SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

        - **Type :** REG_DWORD
        - **Valeur :** 0
    - *Explication technique :* La valeur 0 active le filtrage des jetons d'accès distants. Concrètement, si un administrateur local tente d'accéder au poste via le réseau (ex: \\PC\C$), ses droits d'administration sont retirés ("stripped") par l'UAC distant, bloquant l'accès.

FICHE EXIGENCE : EXG-SEC-PDT47 (PROTECTIONS AVANCEES & DURCISSEMENT)

1. Objectif de sécurité (Synthèse) Cette exigence vise à activer les couches de "Défense en Profondeur" modernes pour pallier les limites des antivirus classiques.

- **Protection des Identités (Credential Guard) :** Isoler les secrets (Hash NTLM, Tickets Kerberos) dans une bulle virtuelle inaccessible même pour un administrateur local, bloquant le vol de mots de passe de la mémoire (LSASS).
- **Protection Mémoire (Exploit Guard) :** Empêcher l'exploitation de failles logicielles via des techniques comme l'ASLR ou le DEP (Prévention de l'exécution des données).
- **Protection Applicative (Office & SmartScreen) :** Bloquer les macros malveillantes venant d'Internet et interdire l'exécution de logiciels à la réputation inconnue ou indésirable (PUA).

2. Configuration Technique (GPO) L'ensemble de ces mesures est regroupé dans la Stratégie de Groupe **EXG47-protections-avancées**.

- **Sécurité basée sur la virtualisation (Device Guard / VBS) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Système > Device Guard.
  - **Paramètre :** "Activer la sécurité basée sur la virtualisation" est **Activé**.
  - **Configuration :**
    - Niveau de sécurité de plateforme : **Démarrage sécurisé (Secure Boot)**.
    - Configuration Credential Guard : **Activé avec le verrouillage UEFI** (Assure que la sécurité ne peut pas être désactivée à distance par un malware modifiant le registre).
- **Exploit Guard & DEP (Protection contre les exploits) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Composants Windows > Windows Defender Exploit Guard > Exploit Protection.
  - **Paramètre :** "Utiliser un ensemble commun de paramètres Exploit Protection".
  - **Fichier de configuration :** \\SRV-AD\netlogon\Settings.xml.
  - *Note technique :* Ce fichier XML, généré depuis un "PC de référence" sain, contient les règles fines de protection mémoire (DEP, ASLR) pour le système et les applications critiques.

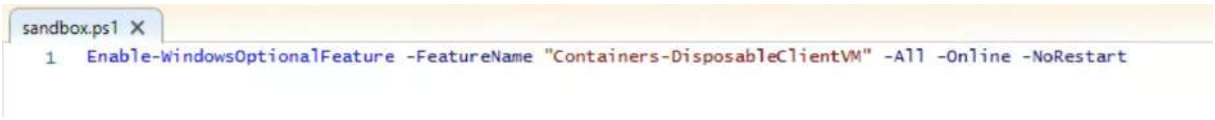

Settings.xml - Bloc-notes

Fichier Edition Format Affichage Aide

```
<?xml version="1.0" encoding="UTF-8"?>
<MitigationPolicy>
  <AppConfig Executable="ExtExport.exe">
    <ASLR ForceRelocateImages="true" RequireInfo="false" />
  </AppConfig>
  <AppConfig Executable="ie4uinit.exe">
    <ASLR ForceRelocateImages="true" RequireInfo="false" />
  </AppConfig>
  <AppConfig Executable="ieinstal.exe">
    <ASLR ForceRelocateImages="true" RequireInfo="false" />
  </AppConfig>
  <AppConfig Executable="ielowutil.exe">
    <ASLR ForceRelocateImages="true" RequireInfo="false" />
  </AppConfig>
  <AppConfig Executable="ieUnatt.exe">
    <ASLR ForceRelocateImages="true" RequireInfo="false" />
  </AppConfig>
  <AppConfig Executable="iexplore.exe">
    <ASLR ForceRelocateImages="true" RequireInfo="false" />
  </AppConfig>
  <AppConfig Executable="mscorsvw.exe">
    <ExtensionPoints DisableExtensionPoints="true" />
  </AppConfig>
  <AppConfig Executable="msfeedssync.exe">
    <ASLR ForceRelocateImages="true" RequireInfo="false" />
  </AppConfig>
  <AppConfig Executable="mshta.exe">
    <ASLR ForceRelocateImages="true" RequireInfo="false" />
  </AppConfig>
 <AppConfig Executable="msfeedssync.exe">
   <ASLR ForceRelocateImages="true" RequireInfo="false" />
 </AppConfig>
 <AppConfig Executable="mshta.exe">
   <ASLR ForceRelocateImages="true" RequireInfo="false" />
 </AppConfig>
 <AppConfig Executable="MsSense.exe">
   <StrictHandle Enable="true" />
   <SEHOP Enable="true" TelemetryOnly="false" />
 </AppConfig>
 <AppConfig Executable="ngen.exe">
   <ExtensionPoints DisableExtensionPoints="true" />
 </AppConfig>
 <AppConfig Executable="ngentask.exe">
   <ExtensionPoints DisableExtensionPoints="true" />
 </AppConfig>
 <AppConfig Executable="PresentationHost.exe">
   <DEP Enable="true" EmulateAtlThunks="false" />
   <ASLR ForceRelocateImages="true" RequireInfo="false" BottomUp="true" HighEntropy="true" />
   <SEHOP Enable="true" TelemetryOnly="false" />
   <Heap TerminateOnError="true" />
 </AppConfig>
 <AppConfig Executable="runtimebroker.exe">
   <ExtensionPoints DisableExtensionPoints="true" />
 </AppConfig>
 <AppConfig Executable="SystemSettings.exe">
   <ExtensionPoints DisableExtensionPoints="true" />
 </AppConfig>
</MitigationPolicy>
```

- **SmartScreen & PUA (Réputation) :**
  - *Chemin :* Composants Windows > Antivirus Windows Defender.
  - **PUA :** "Configurer la détection pour les applications potentiellement indésirables" est **Activé** (Bloquer).

    - *Chemin :* Composants Windows > Windows Defender SmartScreen > Explorateur.
    - **SmartScreen :** "Configurer Windows Defender SmartScreen" est **Activé** en mode **"Avertir et empêcher tout contournement"**, interdisant à l'utilisateur de forcer l'exécution d'un fichier dangereux.
- **Durcissement Microsoft Office (Macros & Mode Protégé) :**
    - *Pré-requis :* Importation des modèles ADMX/ADML d'Office dans le Magasin Central (\\SYSVOL\...\PolicyDefinitions).
    - *Chemin :* Configuration utilisateur > Modèles d'administration > Microsoft Office 2016 > Paramètres de sécurité.
    - **Macros :** "Block all internet macros" (Bloquer toutes les macros Internet) est **Activé**.
    - **Mode Protégé :** Plusieurs paramètres forcent l'ouverture en "Vue Protégée" (Sandbox Office) pour les fichiers venant d'Internet, d'Outlook ou ayant échoué à la validation.
- **Bac à Sable (Windows Sandbox) :**
    - Un script de démarrage PowerShell **sandbox.ps1** est configuré pour activer la fonctionnalité Windows Sandbox sur les postes compatibles, permettant aux utilisateurs de tester des fichiers suspects dans un environnement jetable et isolé.



3.4.7. JOURNALISATION ET SURVEILLANCE

FICHE EXIGENCE : EXG-SEC-PDT49 (CENTRALISATION DES JOURNAUX - WEF)

1. Objectif de sécurité (Synthèse) L'analyse post-mortem d'un incident de sécurité nécessite d'avoir accès aux logs même si le poste de travail a été compromis, effacé ou chiffré par un ransomware. L'objectif est de mettre en place une architecture de **Collecte d'Événements Windows (WEF)**. Les postes de travail (Clients) agissent comme des "abonnés" qui poussent automatiquement leurs journaux de sécurité vers un serveur central (Point de Collecte / WEC), garantissant ainsi l'archivage et la conformité aux exigences légales (CNIL) et d'investigation.

2. Configuration Technique (GPO) L'architecture repose sur la Stratégie de Groupe **EXG49-PointDeCollecte** qui configure le client WinRM et l'abonnement.

- **Configuration du Gestionnaire d'Abonnement (Subscription Manager) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Composants Windows > Transfert d'événements.
  - **Paramètre :** "Configurer le Gestionnaire d'abonnements cible".
  - **Valeur (SubscriptionManagers) :** Server=http://SRV-AD.cesiostage.fr:5985/wsman/SubscriptionManager/WEC,Refresh=60
  - *Analyse technique :* Le poste est instruit de contacter le serveur SRV-AD sur le port **5985** toutes les **60 secondes** pour vérifier s'il y a des événements à transférer.
- **Permissions Locales (Groupes Restreints) :**
  - Pour que le service de transfert puisse lire les journaux de sécurité, il doit avoir les droits appropriés.
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Groupes restreints.
  - **Configuration :** Le compte système **Network Service** (Service Réseau) a été ajouté au groupe local **Lecteurs des journaux d'événements** (Event Log Readers). Sans cette action, le transfert échouerait silencieusement (Accès refusé).
- **Ouverture de Flux (Service WinRM) :**
  - *Chemin :* Configuration ordinateur > Modèles d'administration > Composants Windows > Gestion à distance de Windows (WinRM) > Service WinRM.
  - **Paramètre :** "Autoriser la gestion de serveurs à distance via WinRM".
  - **Filtres IPv4/IPv6 :** Configuré sur * (Autorise l'écoute sur toutes les IP locales pour capter les requêtes du serveur de collecte).

3. Note Technique : Corrélation avec WinRM (EXG36) Une attention particulière a été portée à la cohabitation avec le durcissement WinRM (Exigence EXG36).

- *Contrainte :* Bien que EXG36 impose le chiffrement, le protocole de collecte d'événements natif fonctionne ici via **HTTP (Port 5985)**.

- *Justification de sécurité :* Ce flux n'est pas "en clair" au sens strict. L'authentification et l'intégrité des paquets sont assurées par l'encapsulation **Kerberos** du domaine. L'usage de HTTPS (Port 5986) aurait nécessité le déploiement de certificats serveurs sur chaque poste client, complexité jugée non nécessaire au regard du niveau de sécurité fourni par Kerberos en réseau interne.

FICHE EXIGENCE : EXG-SEC-PDT52 (TAILLE ET RETENTION LOCALE)

1. Objectif Éviter la perte d'événements par écrasement (rotation) avant qu'ils n'aient pu être collectés par le serveur central, notamment en cas de coupure réseau ou de génération massive de logs (attaque par brute force).

2. Configuration Technique (GPO : EXG52-journal-de-securite)

- *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Journal des événements.
- **Taille maximale du journal de sécurité :** 409 600 Kilo-octets (soit **400 Mo**).
- Cette taille conséquente permet de conserver un historique local de plusieurs semaines/mois selon l'activité, agissant comme tampon de sécurité.

FICHE EXIGENCE : EXG-SEC-PDT50 (AUDIT AVANCE ET JOURNALISATION)

1. Objectif de sécurité (Synthèse) La journalisation par défaut de Windows est insuffisante pour comprendre une cyberattaque moderne.

- **Traçabilité des commandes :** Savoir qu'un processus cmd.exe s'est lancé ne suffit pas ; il faut connaître les *arguments* (ex: powershell -enc ...) pour identifier la charge malveillante.
- **Détection des menaces :** L'audit PowerShell (Script Block) permet de démasquer les scripts obfusqués exécutés en mémoire.
- **Hygiène Réseau :** L'audit NTLM est l'étape indispensable avant de pouvoir désactiver ce protocole (EXG37), permettant d'identifier quelles applications l'utilisent encore.

2. Configuration Technique (GPO) La configuration est centralisée dans la Stratégie de Groupe **EXG50-Journalisation**.

- **Audit des Processus et Lignes de Commande (Système & Audit) :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Configuration avancée de l'audit > Suivi détaillé.
  - **Auditer la création du processus :** Configuré sur **Succès**. (Génère l'événement ID 4688).
  - *Chemin :* Modèles d'administration > Système > Audit de création de processus.
  - **Paramètre :** "Inclure une ligne de commande dans les événements de création de processus" est **Activé**.
  - *Effet :* Les journaux de sécurité afficheront désormais la commande exacte tapée par l'attaquant ou l'utilisateur.
- **Journalisation PowerShell (Modèles d'administration & Registre) :**
  - *Chemin :* Composants Windows > Windows PowerShell.
  - **Transcription :** "Activer la transcription PowerShell" est **Activé**.
    - *Répertoire de sortie :* C:\Windows\Logs\PowerShell. (Note : Ce dossier contient des logs textes lisibles de toute session PS).
  - **Script Block Logging (Via Registre) :**
    - *Clé :* HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging -> EnableScriptBlockLogging = 1.
    - *Effet :* Enregistre le code PowerShell déchiffré/désobfusqué tel qu'il est exécuté par le moteur, contournant les tentatives de dissimulation.
- **Audit NTLM (Options de sécurité) :**
  - *Chemin :* Paramètres de sécurité > Stratégies locales > Options de sécurité.
  - **Restreindre NTLM : Auditer le trafic NTLM entrant :** Activer l'audit pour tous les comptes.
  - **Restreindre NTLM : Trafic NTLM sortant vers des serveurs distants :** Auditer tout.

    - *Objectif :* Peupler le journal "Microsoft-Windows-NTLM/Operational" pour identifier les flux à migrer vers Kerberos.
- **Journalisation Application Guard (Préférences Registre) :**
    - Comme il n'y a pas d'ADMX standard, une clé de registre a été poussée.
    - *Chemin :* HKLM\SOFTWARE\Policies\Microsoft\AppHVSI.
    - **Valeur :** AuditApplicationGuard (DWORD) = 1.

3. Note Technique (Hashes Antivirus) Concernant la note sur la "journalisation des hash des charges malveillantes" :

- Cette fonctionnalité est nativement prise en charge par Microsoft Defender Antivirus (Event ID 1116/1117 dans le journal *Microsoft-Windows-Windows Defender/Operational*).
- L'activation de l'audit de création de processus (configurée ci-dessus) est le pré-requis pour corréler un processus avec une alerte antivirus. Pour aller plus loin (hachage de *tous* les exécutables lancés, même sains), l'installation de l'outil **Sysmon** (System Monitor) serait nécessaire, car Windows ne le fait pas nativement par GPO simple.

FICHE EXIGENCE : EXG-SEC-PDT62 (SECURITE ACTIVE DIRECTORY & ANTI-RECONNAISSANCE)

1. Objectif de sécurité (Synthèse) Cette exigence vise à briser la chaîne d'attaque classique : "Compromission d'un poste -> Reconnaissance -> Mouvement Latéral -> Compromission du Domaine".

- **Protection des Admin du Domaine (Tiering) :** Un administrateur de domaine (Tier 0) ne doit **jamais** exposer ses identifiants sur un poste de travail standard (Tier 2). Si un poste est vérolé, l'attaquant ne doit pas pouvoir récupérer un ticket Kerberos ou un hash d'administrateur suprême.
- **Anti-Reconnaissance (NetCease) :** Empêcher un attaquant (ou un malware type *BloodHound/SharpHound*) de cartographier le réseau en demandant au poste "Qui est connecté ici ?".
- **Intégrité des flux :** Garantir que les GPO ne sont pas modifiées en vol et que les échanges avec le Contrôleur de Domaine (DC) sont chiffrés.

2. Configuration Technique (GPO) La configuration est portée par la Stratégie de Groupe **EXG62-ComSecu-controleur-domaine**.

- **Cloisonnement des Administrateurs (Stratégies Locales) :**
  - *Chemin :* Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur.
  - **Interdictions explicites :** Le groupe CESIOSTAGE\Admins du domaine a été ajouté aux politiques suivantes pour leur interdire toute connexion sur le poste :
    - "Interdire l'ouverture de session en tant que service".
    - "Interdire l'ouverture de session en tant que tâche".
    - "Interdire l'ouverture de session par les services Terminal Server" (RDP).
  - *Architecture RDP :* L'accès RDP est réservé au groupe BUILTIN\Utilisateurs du Bureau à distance et au compte de service dédié, conformément à la note d'utiliser des comptes d'administration spécifiques et non ceux du domaine.
- **Sécurisation des Flux DC (Options de Sécurité) :**
  - *Chemin :* Paramètres de sécurité > Stratégies locales > Options de sécurité.
  - **Membre de domaine :** "Chiffrer ou signer numériquement les données des canaux sécurisés (toujours)" est **Activé**.
  - **Sécurité réseau :** "Conditions requises pour la signature de client LDAP" est sur **Exiger la signature**. Cela empêche les attaques Man-in-the-Middle sur les requêtes LDAP vers l'AD.
- **Anti-Reconnaissance / NetCease (Registre) :**

    - Pour bloquer l'énumération de session (BloodHound), les permissions sur le service NetSessionEnum ont été durcies via le Registre (Méthode NetCease).
    - *Chemin :* Configuration ordinateur > Préférences > Paramètres Windows > Registre.
    - **Clé :** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity.
    - **Valeur :** SrvsvcSessionInfo.
    - **Contenu :** Une chaîne binaire complexe (SDDL) qui retire les droits de lecture aux utilisateurs authentifiés standards, rendant le poste "furtif" aux scans de sessions.
- **Application des GPO (Modèles d'administration) :**
    - *Chemin :* Configuration ordinateur > Modèles d'administration > Système > Stratégie de groupe.
    - **Intervalle d'actualisation pour les ordinateurs :** Configuré à **90 minutes** (avec un décalage aléatoire de 0 à 30 minutes).
    - Cela garantit que même si un attaquant modifie un paramètre localement (et qu'il a réussi à contourner les protections), la GPO viendra écraser sa modification et rétablir la conformité automatiquement sous 1h30.

4. CONCLUSION ET REMERCIEMENTS

La mise en œuvre des exigences de sécurité (EXG-SEC-PDT) sur le parc informatique a permis de transformer le poste de travail, souvent considéré comme le maillon faible du Système d'Information, en un premier rempart robuste contre les cybermenaces.

L'approche adoptée ne s'est pas limitée à une simple application de règles, mais a suivi une stratégie de **Défense en Profondeur** cohérente, alignée sur les recommandations de l'ANSSI et les standards actuels (Microsoft Security Baselines).

1. UNE POSTURE DE SECURITE TRANSFORMEE

Le durcissement opéré via les Stratégies de Groupe (GPO) assure désormais une couverture complète des vecteurs d'attaque :

- **Réduction de la Surface d'Attaque (ASR) :** En désactivant les services superflus, les protocoles obsolètes (SMBv1, NetBIOS, LLMNR) et la télémétrie, nous avons drastiquement limité les portes d'entrée potentielles et l'exposition du système.
- **Maîtrise de l'Exécution :** Grâce à **AppLocker** et au contrôle des macros Office, le poste applique un principe de "Liste Blanche". Seules les applications légitimes et validées peuvent s'exécuter, neutralisant de facto la majorité des ransomwares et malwares opportunistes.
- **Protection de l'Identité :** La mise en place de **LAPS**, le durcissement de Kerberos/NTLM et l'isolation des administrateurs (Tiering Model) brisent les chaînes d'attaque visant l'Active Directory (Pass-the-Hash, Golden Ticket).
- **Intégrité des Données :** Le chiffrement **BitLocker** couplé au verrouillage des ports USB garantit la confidentialité des données, même en cas de vol physique du matériel.

2. VISIBILITE ET REACTIVITE

La sécurité n'est pas un état statique, mais un processus continu. L'architecture de journalisation centralisée (**WEF**) mise en place permet désormais de :

- Conserver une trace légale des événements (conformité CNIL).
- Détecter les tentatives d'intrusion (audit PowerShell, audit de processus) avant qu'elles ne causent des dommages irréversibles.

3. PERSPECTIVES ET MAINTIEN EN CONDITION DE SECURITE (MCS)

Si le niveau de sécurité technique atteint est élevé, la pérennité de ce dispositif repose sur deux piliers futurs :

- **Le cycle de vie :** Les règles GPO (notamment AppLocker et Exploit Guard) devront être maintenues pour s'adapter aux nouvelles applications métiers et aux mises à jour de Windows 10/11.

- **La vigilance humaine :** Bien que le système soit durci, l'ingénierie sociale reste un vecteur de menace. La sensibilisation des utilisateurs doit accompagner ces mesures techniques pour garantir une efficacité maximale.

En conclusion, ce projet de sécurisation permet à l'organisation de passer d'une posture réactive à une posture **proactive**, garantissant un environnement de travail fiable, résilient et conforme aux exigences de sécurité modernes.

REMERCIEMENTS

Merci à CESIO pour leur accueil, merci à Sylvain PAQUET , à William ANGLES , Julien GOUINAUD et à Malik VUILLEMOT pour leur soutient tout au long de l'avancée de ce stage et projet.

Je remercie également l'équipe du groupe ALTHIOS à Saint-James (50) pour son accompagnement.

5. SOURCES

- https://cyber.gouv.fr/publications?field_type_de_publication_target_id%5B934%5D=934
- https://www.cnil.fr/fr/securite-securiser-les-postes-de-travail
- https://learn.microsoft.com/en-us/windows/security/
- https://www.cisecurity.org/cis-benchmarks
- https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe
- https://cyber.gouv.fr/sites/default/files/document/anssi-guide-reconditionnement_ordinateurs_bureau_portables_v1-0.pdf
- https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-si
- https://www.it-connect.fr/
- https://gemini.google.com/