GUIDE EXPERT 2026

# Tiering Model Active Directory

Architecture de sécurité en 3 tiers : implémentation, 69 points de contrôle, scripts PowerShell et études de cas

**Ayi NEDJIMI**

**Ayinedjimi Consultants**

www.ayinedjimi-consultants.fr

# Mentions légales



**Site web :** www.ayinedjimi-consultants.fr

**Édition :** Mars 2026

**Contenu :** 20 000+ mots — 69 points de contrôle — Scripts PowerShell inclus

Ce guide est fourni à titre informatif et éducatif. Les scripts et configurations proposés doivent être testés dans un environnement de laboratoire avant tout déploiement en production. L'auteur ne saurait être tenu responsable des dommages résultant de l'application des recommandations de cet ouvrage.

# Table des matières



## ANNEXES



## COMPLÉMENTS

CHAPITRE 1

# Introduction au Tiering Model

## Contexte et Enjeux de la Sécurité Active Directory

Dans le paysage actuel des menaces informatiques, la sécurité des systèmes d'information reposant sur Microsoft Active Directory représente un défi majeur pour les organisations de toutes tailles. Active Directory, en tant que pierre angulaire de l'infrastructure d'identité et d'accès dans la plupart des environnements Windows, constitue une cible de choix pour les cybercriminels et les acteurs malveillants.

Les statistiques récentes en matière de cybersécurité révèlent une tendance inquiétante : plus de 80% des incidents de sécurité majeurs impliquent une compromission de comptes à privilèges élevés. Cette réalité souligne l'importance cruciale d'une approche structurée et méthodique de l'administration sécurisée des environnements Active Directory. Les attaques modernes ne se contentent plus de cibler les périmètres externes des réseaux ; elles exploitent avec sophistication les faiblesses internes, notamment celles liées à la gestion des identités et des accès.

L'administration d'un système d'information est une activité critique qui exige une attention particulière et une rigueur sans faille. Dans le contexte spécifique des environnements Active Directory, cette criticité est amplifiée par le rôle central que joue l'annuaire dans la gestion des authentifications, l'attribution des droits d'accès, et le paramétrage des politiques de sécurité. Une compromission de l'annuaire Active Directory ne se limite pas à un incident isolé : elle peut conduire à une compromission globale de l'ensemble du système d'information.

### Pourquoi un guide spécifique à Active Directory ?

Bien que de nombreux principes généraux de sécurité informatique s'appliquent universellement, Active Directory présente des particularités qui nécessitent une approche adaptée. Les concepts de domaines, de forêts, de relations d'approbation, et les protocoles

d'authentification spécifiques comme NTLM et Kerberos créent un environnement complexe où les bonnes pratiques génériques doivent être complétées par des recommandations spécifiques.

# Qu'est-ce que le Modèle de Tiering ?

Le modèle de tiering, également appelé modèle administratif à niveaux ou modèle de cloisonnement hiérarchique, représente une approche structurée et éprouvée pour sécuriser l'administration des systèmes d'information reposant sur Active Directory. Ce modèle propose une segmentation logique de l'infrastructure informatique en plusieurs niveaux hiérarchiques distincts, communément appelés "tiers", chacun caractérisé par ses propres exigences de sécurité, ses contrôles d'accès spécifiques, et son niveau de sensibilité.

L'objectif principal de cette architecture en tiers est de limiter considérablement les risques associés aux comptes privilégiés, qui constituent traditionnellement la cible prioritaire des cyberattaques sophistiquées. En établissant des barrières logiques strictes entre les différents niveaux d'administration, le modèle vise à contenir les attaques potentielles et à réduire drastiquement l'impact d'une éventuelle intrusion ou compromission.

## La Problématique des Déplacements Latéraux

Dans un environnement Active Directory traditionnel, où le cloisonnement fait défaut, les administrateurs utilisent fréquemment des comptes à privilèges élevés pour effectuer une grande variété de tâches administratives. Cette pratique, bien que pratique d'un point de vue opérationnel, expose l'ensemble du domaine à des risques considérables de compromission. Le scénario d'attaque typique se déroule en plusieurs phases bien documentées :

1. **Compromission initiale :** L'attaquant pénètre initialement le système d'information par des moyens divers : phishing, exploitation de vulnérabilités sur les postes de travail, ingénierie sociale, ou exploitation de services exposés sur Internet.
2. **Établissement d'un point d'ancrage :** Une fois l'accès initial obtenu, généralement sur un poste de travail utilisateur ou un serveur de moindre importance, l'attaquant cherche à maintenir sa présence et à éviter la détection.
3. **Reconnaissance et énumération :** L'attaquant procède alors à une phase de reconnaissance intensive, cartographiant l'environnement Active Directory, identifiant les comptes privilégiés, les serveurs critiques, et les relations de confiance.
4. **Déplacements latéraux :** C'est là que réside le cœur du problème. Dans un environnement mal cloisonné, l'attaquant peut se déplacer de système en système,

collectant au passage des identifiants stockés en mémoire, des tickets Kerberos, et des condensats de mots de passe.

5. **Élévation de privilèges progressive :** À chaque déplacement, l'attaquant tente d'élever ses privilèges, passant d'un compte utilisateur standard à un compte administrateur local, puis à un administrateur de domaine.
6. **Compromission totale :** Finalement, l'attaquant parvient à obtenir le contrôle total de l'annuaire Active Directory, lui permettant de créer des portes dérobées, d'exfiltrer des données sensibles, et d'assurer une persistance à long terme.

Ce cheminement, qui peut dans certains cas prendre seulement quelques heures depuis la compromission initiale jusqu'au contrôle total du domaine, est souvent rendu possible par une absence criante de cloisonnement logique des ressources de l'Active Directory. Le modèle de tiering vise précisément à briser cette chaîne d'attaque en introduisant des barrières strictes entre les différents niveaux de privilèges.

# Les Trois Niveaux du Modèle de Tiering

Le modèle de tiering repose sur une architecture tripartite, organisant les ressources, les comptes, et les systèmes en trois niveaux distincts selon leur sensibilité et leur criticité. Cette organisation hiérarchique permet d'appliquer des contrôles de sécurité proportionnés au niveau de risque associé à chaque tier.

## Tier 0 : Le Cœur de Confiance de l'Organisation

Le Tier 0 représente le niveau de sécurité et de confiance le plus élevé au sein de l'infrastructure. Il constitue littéralement le cœur de confiance de l'organisation, englobant les ressources dont la compromission entraînerait une perte totale de contrôle sur l'ensemble du système d'information.

**Caractéristiques du Tier 0 :**

- Privilèges d'administration maximaux sur l'ensemble de la forêt Active Directory
- Capacité d'octroyer des privilèges sur tous les autres tiers
- Contrôle complet sur toutes les ressources de l'annuaire
- Nombre de ressources volontairement limité pour réduire la surface d'attaque
- Exposition aux menaces minimisée par un cloisonnement strict
- Exigences de sécurité les plus élevées de toute l'infrastructure

**Ressources typiquement catégorisées en Tier 0 :**

- Contrôleurs de domaine Active Directory (tous les DC de la forêt)
- Serveurs de gestion des certificats (autorités de certification PKI/IGC) délivrant des certificats d'authentification pour le Tier 0
- Serveurs de fédération d'identité (ADFS, serveurs de synchronisation cloud)
- Comptes d'administration du domaine (Domain Admins, Enterprise Admins, Schema Admins)
- Postes d'administration dédiés (PAW - Privileged Access Workstations) pour l'administration du Tier 0
- Systèmes de gestion des secrets et des mots de passe privilégiés pour le Tier 0
- Infrastructures de virtualisation hébergeant des ressources Tier 0
- Systèmes de sauvegarde des ressources Tier 0
- Infrastructures de stockage hébergeant des données Tier 0

## Tier 1 : La Confiance dans les Valeurs Métiers

Le Tier 1 représente le niveau intermédiaire du modèle, caractérisé par une grande hétérogénéité. Il englobe les systèmes et ressources qui portent ou traitent les valeurs métiers de l'organisation, sans pour autant avoir un contrôle direct sur l'infrastructure Active Directory elle-même.

**Caractéristiques du Tier 1 :**

- Privilèges d'administration sur les serveurs et applications métier
- Aucun privilège sur le Tier 0
- Contrôle potentiel sur les ressources du Tier 2
- Grande diversité de systèmes et d'applications
- Criticité variable selon les applications hébergées

**Ressources typiquement catégorisées en Tier 1 :**

- Serveurs d'applications métier (ERP, CRM, systèmes de gestion)
- Serveurs de bases de données métier
- Serveurs de messagerie d'entreprise
- Serveurs de gestion de code source et de développement
- Serveurs de fichiers contenant des données métier sensibles
- Équipements critiques de chaîne de production
- Systèmes SCADA et de contrôle industriel

- Serveurs web hébergeant des applications internes critiques
- Comptes d'administration de serveurs et d'applications
- Postes d'administration dédiés pour le Tier 1

### Tier 2 : La Confiance dans les Moyens d'Accès

Le Tier 2 constitue le niveau de base du modèle, englobant principalement les postes de travail des utilisateurs finaux et les moyens d'accès aux ressources métier. Bien qu'il soit considéré comme le moins sensible en termes de privilèges, il représente paradoxalement la surface d'attaque la plus exposée.

**Caractéristiques du Tier 2 :**

- Privilèges limités aux postes de travail utilisateurs
- Aucun privilège sur les Tiers 0 et 1
- Nombre de ressources très important
- Exposition aux menaces maximale (Internet, emails, dispositifs USB)
- Point d'entrée le plus fréquent pour les attaques

**Ressources typiquement catégorisées en Tier 2 :**

- Postes de travail de bureautique des utilisateurs finaux
- Ordinateurs portables professionnels
- Consoles industrielles et terminaux opérateurs
- Équipements de téléphonie IP
- Dispositifs mobiles professionnels (smartphones, tablettes)
- Systèmes de visioconférence
- Comptes utilisateurs standards
- Comptes d'administration locale des postes de travail
- Services de déploiement de postes de travail (SCCM, MDT pour le Tier 2)

## Pourquoi Implémenter le Modèle de Tiering ?

Les motivations pour adopter un modèle de tiering dans un environnement Active Directory sont multiples et s'inscrivent dans une démarche globale de gestion des risques cyber et de conformité réglementaire.

## Réponse à l'Évolution des Menaces

Le paysage des menaces informatiques évolue à une vitesse remarquable. Les attaquants, qu'ils soient des cybercriminels motivés financièrement, des acteurs étatiques, ou des groupes activistes, perfectionnent constamment leurs techniques. Les attaques ciblant spécifiquement Active Directory ont connu une progression significative ces dernières années, avec l'émergence de techniques sophistiquées telles que :

- **Le Pass-the-Hash (PtH) :** Exploitation de condensats de mots de passe NTLM capturés pour s'authentifier sans connaître le mot de passe en clair.
- **Le Pass-the-Ticket (PtT) :** Réutilisation de tickets Kerberos volés pour accéder à des ressources sans authentification supplémentaire.
- **Le Golden Ticket :** Création de tickets Kerberos forgés permettant un accès illimité à toutes les ressources du domaine.
- **Le Silver Ticket :** Création de tickets de service forgés pour accéder à des services spécifiques.
- **Les attaques par DCShadow :** Enregistrement d'un faux contrôleur de domaine pour injecter des modifications malveillantes dans Active Directory.
- **Le Kerberoasting :** Extraction et craquage hors ligne des mots de passe de comptes de service.
- **Les attaques sur les délégations Kerberos :** Exploitation de configurations de délégation faibles pour usurper l'identité d'utilisateurs privilégiés.

Le modèle de tiering, en établissant des barrières strictes entre les différents niveaux de privilèges, limite considérablement l'efficacité de ces techniques d'attaque. Même si un attaquant parvient à compromettre un système de faible privilège (Tier 2), les contrôles mis en place l'empêchent de progresser vers les niveaux supérieurs.

## Conformité Réglementaire et Normative

De nombreuses réglementations et normes en matière de sécurité de l'information exigent une gestion rigoureuse des accès privilégiés. Parmi celles-ci, on peut citer :

- **Le Règlement Général sur la Protection des Données (RGPD) :** Impose des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, incluant la gestion des accès.
- **La norme ISO/IEC 27001 :** Requiert des contrôles sur la gestion des accès privilégiés et la séparation des environnements.
- **Le standard PCI-DSS :** Exige une restriction stricte de l'accès aux données de cartes de paiement par le principe du besoin d'en connaître.

- **Les directives NIS et NIS2 :** Imposent des mesures de sécurité pour les opérateurs de services essentiels.
- **La Loi de Programmation Militaire (LPM) :** Pour les opérateurs d'importance vitale en France.

L'implémentation d'un modèle de tiering facilite grandement la démonstration de conformité avec ces exigences réglementaires en fournissant une structure claire, documentée et auditable pour l'administration sécurisée du système d'information.

### Amélioration de la Visibilité et de l'Auditabilité

Un des bénéfices souvent sous-estimés du modèle de tiering réside dans l'amélioration significative de la visibilité sur les activités administratives. En séparant clairement les rôles et en imposant l'utilisation de comptes dédiés pour chaque niveau, l'organisation gagne en capacité de :

- **Traçabilité :** Identifier précisément qui a effectué quelle action administrative, à quel moment, et depuis quel système.
- **Détection d'anomalies :** Repérer plus facilement les comportements suspects, comme l'utilisation d'un compte Tier 0 sur un système Tier 2.
- **Investigation d'incidents :** Reconstituer le déroulement d'un incident de sécurité avec davantage de précision.
- **Révision des privilèges :** Auditer régulièrement les droits accordés et identifier les sur-privilèges.

### Réduction des Erreurs Humaines

Les erreurs humaines constituent une source importante de vulnérabilités dans les systèmes d'information. Dans un environnement où les administrateurs utilisent quotidiennement des comptes hautement privilégiés pour toutes leurs tâches, le risque d'erreur catastrophique est élevé. Le modèle de tiering, en imposant l'utilisation de comptes à privilèges limités pour les tâches courantes et en réservant les comptes privilégiés à des actions spécifiques, réduit mécaniquement ce risque.

## Les Principes Fondamentaux du Cloisonnement

Le succès de l'implémentation d'un modèle de tiering repose sur le respect rigoureux de plusieurs principes fondamentaux qui constituent le socle de l'architecture de sécurité.

## Le Principe de Moindre Privilège

Le principe de moindre privilège stipule que chaque compte, processus ou système ne doit disposer que des droits strictement nécessaires à l'accomplissement de ses fonctions légitimes. Dans le contexte du modèle de tiering, ce principe se traduit par :

- L'attribution de privilèges spécifiques à chaque tier sans débordement vers les tiers supérieurs
- L'utilisation de comptes standards pour les tâches non administratives
- La délégation fine des droits administratifs selon les besoins réels
- La révision régulière des privilèges pour éliminer les sur-privilèges accumulés

## La Séparation des Tâches (Segregation of Duties)

La séparation des tâches vise à empêcher qu'une seule personne ou un seul compte puisse réaliser seul une action critique. Dans le modèle de tiering, cela se manifeste par :

- La distinction entre les administrateurs des différents tiers
- La séparation entre les fonctions de création et de validation
- L'impossibilité pour un administrateur Tier 2 d'administrer directement le Tier 0
- La nécessité d'approbations multiples pour les changements critiques

## La Défense en Profondeur

La défense en profondeur consiste à implémenter plusieurs couches de sécurité indépendantes, de sorte que la défaillance d'une couche ne compromette pas l'ensemble de la sécurité. Dans le contexte du tiering :

- Contrôles au niveau réseau (segmentation, filtrage)
- Contrôles au niveau système (durcissement, authentification multi-facteurs)
- Contrôles au niveau applicatif (gestion des sessions, journalisation)
- Contrôles au niveau organisationnel (procédures, formations)

## Point d'Attention Critique

**La forêt Active Directory, et non le domaine, constitue la frontière de sécurité pertinente.** Une erreur courante consiste à considérer qu'un cloisonnement entre domaines d'une même forêt offre une sécurité suffisante. En réalité, un administrateur disposant de privilèges élevés

sur un domaine de la forêt peut, dans de nombreux cas, escalader ses privilèges pour obtenir le contrôle de l'ensemble de la forêt. Le périmètre d'application du modèle de tiering doit donc être la forêt entière.

# Prérequis et Conditions de Mise en Œuvre

L'implémentation réussie d'un modèle de tiering nécessite la réunion de plusieurs conditions préalables, tant sur le plan technique qu'organisationnel.

## Prérequis Techniques

- **Niveau fonctionnel Active Directory :** Un niveau fonctionnel de forêt et de domaine Windows Server 2012 R2 minimum est requis pour bénéficier de fonctionnalités essentielles comme les silos d'authentification et le groupe Protected Users.
- **Inventaire exhaustif :** Une cartographie complète de l'infrastructure doit être disponible, incluant tous les serveurs, postes de travail, comptes, groupes, et applications.
- **Outils de gestion :** Déploiement d'outils facilitant la gestion sécurisée, tels que LAPS (Local Administrator Password Solution) pour la gestion des mots de passe administrateurs locaux.
- **Infrastructure de journalisation :** Mise en place d'une solution centralisée de collecte et d'analyse des journaux d'événements.
- **Postes d'administration dédiés :** Disponibilité de machines physiques ou virtuelles dédiées à l'administration, durcies et isolées.

## Prérequis Organisationnels

- **Engagement de la direction :** Le soutien visible et actif de la direction générale est indispensable, car le projet implique des changements significatifs dans les modes de fonctionnement.
- **Ressources humaines :** Allocation de ressources suffisantes en termes de personnel qualifié et de temps disponible pour le projet.
- **Budget :** Financement adéquat pour l'acquisition d'équipements, de licences logicielles, et éventuellement de prestations externes.
- **Formation :** Programme de formation approfondi pour les équipes d'administration sur les principes du modèle et les nouvelles procédures.
- **Communication :** Plan de communication pour expliquer les changements aux différentes parties prenantes et obtenir leur adhésion.

- **Gestion du changement :** Processus structuré pour accompagner la transformation des pratiques et gérer la résistance au changement.

### Évaluation Initiale des Risques

Avant de débuter l'implémentation, il est crucial de réaliser une évaluation approfondie des risques actuels de l'environnement Active Directory. Cette évaluation devrait couvrir :

- L'identification des chemins d'attaque existants vers les ressources critiques
- L'analyse de la dissémination des secrets d'authentification (mots de passe, tickets Kerberos)
- La cartographie des comptes privilégiés et de leurs usages
- L'évaluation de la configuration des relations d'approbation entre domaines et forêts
- La revue des délégations de droits et des groupes privilégiés
- L'analyse des vulnérabilités connues dans la configuration Active Directory

Cette évaluation initiale servira de baseline pour mesurer les progrès réalisés au fur et à mesure de l'implémentation du modèle de tiering.

## Bénéfices Attendus et Retour sur Investissement

L'implémentation d'un modèle de tiering représente un investissement conséquent en termes de temps, de ressources et d'efforts. Il est légitime de s'interroger sur les bénéfices attendus et le retour sur investissement.

### Réduction Mesurable des Risques

Les organisations ayant implémenté un modèle de tiering rapportent une réduction significative de leur exposition aux risques cyber. Les incidents de sécurité impliquant une compromission totale du domaine Active Directory deviennent exceptionnels lorsque le modèle est correctement mis en œuvre et maintenu.

### Limitation de l'Impact des Incidents

Même dans le cas où un incident de sécurité se produit, le cloisonnement strict entre les tiers limite considérablement la propagation de l'attaque. Une compromission du Tier 2 ne conduit plus automatiquement à une compromission totale du système d'information.

### Réduction des Coûts de Remédiation

Le coût de remédiation d'une compromission totale d'un environnement Active Directory peut se chiffrer en millions d'euros pour une organisation de taille moyenne, sans compter les coûts indirects liés à l'interruption d'activité, à l'atteinte à la réputation, et aux implications réglementaires. L'investissement dans un modèle de tiering, bien que significatif, reste généralement très inférieur au coût potentiel d'un incident majeur.

### Amélioration de la Posture de Sécurité Globale

Au-delà de la protection spécifique d'Active Directory, l'implémentation du modèle de tiering s'accompagne généralement d'une amélioration de la posture de sécurité globale de l'organisation : meilleure hygiène en matière de gestion des comptes, amélioration des processus de gestion des changements, renforcement de la culture de sécurité.

## Conclusion de l'Introduction

Le modèle de tiering représente une approche éprouvée et robuste pour sécuriser les environnements Active Directory face aux menaces contemporaines. Son implémentation, bien que complexe et exigeante, offre des bénéfices substantiels en termes de réduction des risques et de conformité réglementaire.

Les pages suivantes de ce guide détailleront les aspects conceptuels, méthodologiques et techniques de la mise en œuvre d'un modèle de tiering, en abordant successivement les principes de sécurité fondamentaux, l'implémentation spécifique de chaque tier, et les bonnes pratiques de gestion et de maintenance.

L'approche proposée repose sur une méthodologie itérative et pragmatique, permettant une implémentation progressive tout en obtenant des améliorations de sécurité significatives dès les premières étapes.

CHAPITRE 2

# Concepts et Principes

## Méthodologie de Cloisonnement du Système d'Information

L'implémentation d'un modèle de tiering ne peut se faire de manière spontanée ou anarchique. Elle requiert une méthodologie rigoureuse, structurée et progressive qui tient compte de la réalité opérationnelle de l'organisation. La démarche proposée repose sur un processus itératif d'amélioration continue, permettant d'obtenir des gains de sécurité progressifs tout en minimisant les impacts sur les opérations quotidiennes.

### Une Approche Itérative et Pragmatique

Le cloisonnement d'un système d'information complexe selon le modèle de tiering n'est pas un projet ponctuel avec un début et une fin clairement définis. Il s'agit plutôt d'une démarche d'amélioration continue qui s'inscrit dans la durée. Cette approche itérative présente plusieurs avantages décisifs :

- **Réduction des risques de disruption :** En procédant par étapes progressives, l'organisation évite les changements massifs qui pourraient perturber gravement les opérations métier ou créer des interruptions de service prolongées.
- **Apprentissage progressif :** Chaque itération permet aux équipes d'acquérir de l'expérience, d'identifier les difficultés spécifiques à leur environnement, et d'ajuster leur approche pour les itérations suivantes.
- **Gains rapides :** Dès les premières itérations, focalisées sur les éléments les plus critiques (Tier 0), l'organisation bénéficie d'améliorations significatives de sa posture de sécurité.
- **Adaptation au contexte :** L'approche itérative permet d'adapter continuellement le modèle aux évolutions de l'infrastructure, aux changements organisationnels, et à l'émergence de nouvelles menaces.
- **Gestion facilitée du changement :** Les équipes et les utilisateurs disposent du temps nécessaire pour s'adapter progressivement aux nouvelles contraintes et procédures.

## Les Deux Phases du Cycle Itératif

Chaque itération du processus d'amélioration se décompose en deux phases complémentaires qui doivent être exécutées de manière équilibrée.

### Phase 1 : Étude et Analyse

Cette phase analytique constitue le socle sur lequel reposera l'ensemble des actions de sécurisation. Elle comprend plusieurs activités essentielles :

**Identification des périmètres :**

- Identification exhaustive des ressources constituant le Tier 0 (contrôleurs de domaine, comptes privilégiés, infrastructures support)
- Délimitation précise du périmètre Tier 1 en fonction des valeurs métier de l'organisation
- Classification des postes de travail et moyens d'accès dans le Tier 2
- Identification des zones grises nécessitant une analyse approfondie pour déterminer leur catégorisation

**Analyse des chemins d'attaque :**

- Cartographie des chemins de contrôle existants dans Active Directory à l'aide d'outils spécialisés comme BloodHound
- Identification des comptes disposant de privilèges excessifs ou inappropriés
- Analyse des délégations de droits et des appartenances aux groupes privilégiés
- Évaluation de la dissémination des secrets d'authentification (où les mots de passe et tickets sont-ils stockés et utilisés ?)
- Identification des chemins indirects via les infrastructures de virtualisation, de stockage et de sauvegarde

**Catégorisation détaillée :**

- Attribution d'un niveau de tier à chaque ressource identifiée : serveur, poste de travail, compte utilisateur, groupe de sécurité
- Documentation des justifications pour chaque catégorisation, particulièrement pour les cas ambigus
- Création d'un référentiel de catégorisation qui servira de base pour les décisions futures
- Validation des catégorisations avec les responsables métier et techniques concernés

## Phase 2 : Actions et Implémentation

Sur la base des analyses effectuées dans la première phase, la phase d'actions vise à concrétiser le cloisonnement et à réduire les risques identifiés :

**Application des bonnes pratiques d'architecture :**

- Création d'unités organisationnelles (OU) dédiées pour chaque tier dans Active Directory
- Mise en place de stratégies de groupe (GPO) spécifiques à chaque tier
- Déploiement de postes d'administration dédiés (PAW) pour les tiers sensibles
- Configuration de l'infrastructure réseau pour supporter la segmentation logique

**Réduction de l'exposition :**

- Élimination des comptes et privilèges inutiles
- Réduction du nombre de ressources catégorisées en Tier 0 au strict minimum
- Limitation des interactions entre les différents tiers
- Désactivation des protocoles et services non essentiels

**Durcissement système et logiciel :**

- Application de configurations de sécurité renforcées via les GPO
- Activation des mécanismes de protection natifs (Windows Defender Application Control, Credential Guard, Device Guard)
- Déploiement de solutions de protection des points de terminaison (EDR)
- Mise en œuvre de l'authentification multi-facteurs pour les accès privilégiés

**Délégation fine des droits :**

- Remplacement des privilèges globaux par des délégations ciblées
- Utilisation de Just Enough Administration (JEA) pour PowerShell
- Implémentation de l'accès juste-à-temps (JIT) pour les privilèges temporaires
- Configuration des silos d'authentification pour restreindre l'usage des comptes privilégiés

**Traitement des chemins d'attaque :**

- Suppression des chemins d'attaque non nécessaires identifiés lors de la phase d'analyse
- Mise en place de contrôles compensatoires pour les chemins qui ne peuvent être éliminés
- Documentation et justification des chemins résiduels acceptés

## Pilotage et Gouvernance du Processus

Le succès de la démarche itérative repose sur un pilotage efficace et une gouvernance claire. Les éléments suivants sont essentiels :

- **Sponsor exécutif :** Un membre de la direction générale doit porter le projet et assurer son soutien visible auprès de toutes les parties prenantes.
- **Équipe de pilotage :** Une équipe restreinte disposant d'une vision transverse du système d'information doit être constituée pour piloter la démarche. Cette équipe doit inclure des représentants de la sécurité, des opérations IT, et des métiers.
- **Indicateurs de progression :** Des métriques doivent être définies pour mesurer objectivement les progrès réalisés : nombre de chemins d'attaque critiques éliminés, pourcentage de ressources Tier 0 sécurisées, taux de conformité aux politiques de sécurité, etc.
- **Révision régulière :** Des points de contrôle périodiques doivent être organisés pour évaluer l'avancement, identifier les obstacles, et ajuster le plan d'action si nécessaire.
- **Communication continue :** Une communication transparente et régulière vers l'ensemble des parties prenantes est indispensable pour maintenir l'adhésion et gérer les résistances.

# Périmètre d'Application du Modèle

La définition précise du périmètre d'application du modèle de tiering constitue une étape fondamentale qui conditionnera l'efficacité de l'ensemble de la démarche.

## La Forêt comme Frontière de Sécurité

### Principe Fondamental

Dans Active Directory, la forêt, et non le domaine, constitue la véritable frontière de sécurité. Cette distinction est cruciale et sa méconnaissance est à l'origine de nombreuses failles de sécurité.

Plusieurs raisons techniques expliquent pourquoi la forêt doit être considérée comme le périmètre de sécurité :

- **Les groupes Enterprise Admins et Schema Admins :** Ces groupes, définis au niveau de la forêt, disposent de privilèges qui s'étendent à tous les domaines de la forêt.

- **Le schéma Active Directory :** Il est unique et partagé par tous les domaines de la forêt. Un administrateur capable de modifier le schéma peut potentiellement impacter tous les domaines.
- **Le catalogue global :** Les serveurs de catalogue global répliquent des informations de tous les domaines de la forêt, créant des dépendances de sécurité.
- **Les relations d'approbation transitives :** Par défaut, les domaines au sein d'une même forêt se font mutuellement confiance de manière transitive, créant des chemins de privilèges potentiels.
- **Les partitions de configuration et de schéma :** Ces partitions sont répliquées sur tous les contrôleurs de domaine de la forêt, créant des vecteurs d'attaque potentiels.

## Cas des Environnements Multi-Forêts

Dans les environnements complexes comportant plusieurs forêts Active Directory, la définition du périmètre devient plus délicate et dépend de plusieurs facteurs :

**Relations d'approbation entre forêts :**

- Forêts sans relation d'approbation : Chaque forêt peut être traitée comme un périmètre indépendant
- Forêts avec approbation unidirectionnelle : Le périmètre peut rester distinct si le filtrage SID est activé et si l'approbation est correctement configurée
- Forêts avec approbation bidirectionnelle : Le périmètre de sécurité devrait idéalement englober toutes les forêts interconnectées

**Synchronisation d'identités :**

Si des mécanismes de synchronisation d'identités (comme Microsoft Identity Manager) sont en place entre les forêts, cela crée des dépendances de sécurité qui doivent être prises en compte dans la définition du périmètre.

**Partage de ressources :**

L'existence de ressources partagées entre forêts (serveurs, applications, données) influence la définition du périmètre et peut nécessiter une approche coordonnée du tiering entre les forêts.

# Identification et Catégorisation des Ressources

Le processus d'identification et de catégorisation des ressources constitue le cœur de la phase d'analyse. Il doit être mené avec rigueur et méthode pour garantir l'efficacité du cloisonnement.

## Identification des Valeurs Métier

Avant de pouvoir catégoriser les ressources techniques, il est indispensable d'identifier clairement les valeurs métier de l'organisation. Cette démarche implique :

- **Recensement des missions critiques :** Quelles sont les activités essentielles à la survie et au fonctionnement de l'organisation ?
- **Identification des processus métier :** Quels processus supportent ces missions critiques ?
- **Cartographie des applications et données :** Quelles applications et quelles données sont nécessaires à l'exécution de ces processus ?
- **Analyse d'impact :** Quel serait l'impact d'une indisponibilité, d'une altération ou d'une divulgation de ces ressources ?
- **Priorisation :** Établissement d'une hiérarchie des valeurs métier pour prioriser les efforts de protection

Cette analyse métier, souvent négligée dans les projets purement techniques, est pourtant essentielle pour justifier les investissements de sécurité et obtenir l'adhésion des responsables métier.

## Catégorisation des Objets Active Directory

Une fois les valeurs métier identifiées, tous les objets de l'Active Directory doivent être catégorisés dans l'un des trois tiers. Cette catégorisation concerne :

| Type d'Objet | Critères de Catégorisation | Exemples |
|---|---|---|
| **Comptes utilisateurs** | Privilèges maximum détenus, ressources administrées | Compte Domain Admin → Tier 0<br>Compte admin serveur ERP → Tier 1<br>Compte utilisateur standard → Tier 2 |
| **Comptes d'ordinateurs** | Type de système, rôle dans l'infrastructure | Contrôleur de domaine → Tier 0<br>Serveur de base de données métier → Tier 1<br>Poste de travail utilisateur → Tier 2 |
| **Groupes de sécurité** | Privilèges accordés au groupe, ressources accessibles | Domain Admins → Tier 0<br>Admins serveurs applicatifs → Tier 1<br>Utilisateurs bureautique → Tier 2 |
| **Unités organisationnelles** | Objets contenus et GPO appliquées | OU Tier 0 → contient objets Tier 0<br>OU Serveurs Métier → Tier 1<br>OU Postes Utilisateurs → Tier 2 |

## Principes de Catégorisation

Plusieurs principes guident le processus de catégorisation pour garantir sa cohérence et son efficacité :

### Principe du Maillon le Plus Faible

Lorsqu'un compte possède des privilèges sur plusieurs tiers, il doit être catégorisé au niveau du tier le plus élevé sur lequel il dispose de privilèges. Par exemple, un compte disposant de privilèges administratifs à la fois sur des serveurs Tier 1 et sur un contrôleur de domaine (Tier 0) doit impérativement être catégorisé en Tier 0.

### Principe de la Chaîne de Contrôle

Une ressource doit être catégorisée au même niveau que la ressource la plus sensible qu'elle peut contrôler. Par exemple, un hyperviseur hébergeant des machines virtuelles Tier 0 doit lui-même être catégorisé en Tier 0, car sa compromission permettrait de compromettre les VM qu'il héberge.

### Principe de Conservation des Secrets

Tout système sur lequel des secrets d'authentification d'un tier donné peuvent être stockés, même temporairement, doit être catégorisé au même niveau de tier. Cela concerne notamment la mémoire RAM où les condensats de mots de passe et les tickets Kerberos peuvent résider.

# Gestion des Secrets d'Authentification

La maîtrise de la dissémination des secrets d'authentification constitue l'un des piliers fondamentaux du modèle de tiering. Un secret d'authentification mal contrôlé peut anéantir tous les efforts de cloisonnement.

## Types de Secrets d'Authentification

Dans un environnement Active Directory, plusieurs types de secrets doivent être protégés :

- **Mots de passe en clair :** Rarement stockés mais peuvent transiter lors de certaines authentifications ou être présents temporairement en mémoire
- **Condensats NTLM (hashes) :** Formes dérivées des mots de passe, stockées dans la base SAM locale et dans la base NTDS.dit des contrôleurs de domaine, utilisables pour l'authentification sans connaître le mot de passe original
- **Tickets Kerberos :** Tickets TGT (Ticket-Granting Ticket) et TGS (Ticket-Granting Service) stockés temporairement en mémoire et réutilisables pour accéder aux ressources
- **Clés privées de certificats :** Utilisées pour l'authentification par certificat, souvent stockées dans le magasin de certificats Windows ou sur des cartes à puce
- **Clés SSH :** Dans les environnements hybrides incluant des systèmes Linux, les clés privées SSH peuvent permettre l'accès à des ressources critiques
- **Jetons et clés API :** De plus en plus utilisés pour l'authentification des services et des applications, ils constituent des secrets d'authentification à part entière

## Principe Fondamental de Non-Dissémination

### Règle d'Or

**Aucun secret d'authentification d'un tier ne doit jamais être accessible, saisi, stocké ou traité sur un tier de niveau inférieur.**

Concrètement, cela signifie :

- Un mot de passe Tier 0 ne doit JAMAIS être saisi sur un système Tier 1 ou Tier 2
- Un ticket Kerberos d'un compte Tier 0 ne doit JAMAIS résider en mémoire d'un système Tier 1 ou Tier 2
- Un condensat NTLM d'un compte Tier 0 ne doit JAMAIS être stocké sur un système autre que Tier 0

Le non-respect de ce principe crée un chemin d'attaque direct : si un attaquant compromet un système de niveau inférieur et y trouve des secrets de niveau supérieur, tout le cloisonnement devient inefficace.

## Techniques de Protection des Secrets

Plusieurs techniques et technologies permettent de protéger efficacement les secrets d'authentification :

**LAPS (Local Administrator Password Solution) :**

LAPS est une solution Microsoft gratuite permettant la gestion automatique des mots de passe des comptes administrateurs locaux. Elle offre plusieurs avantages critiques :

- Génération automatique de mots de passe complexes et uniques pour chaque système
- Rotation régulière des mots de passe selon une politique configurable
- Stockage sécurisé des mots de passe dans Active Directory avec contrôle d'accès granulaire
- Élimination du problème des mots de passe administrateurs locaux identiques sur tous les postes
- Journalisation des accès aux mots de passe pour la traçabilité

**Managed Service Accounts (MSA et gMSA) :**

Les comptes de service gérés éliminent le besoin de gérer manuellement les mots de passe des comptes de service :

- Renouvellement automatique des mots de passe sans intervention humaine
- Impossibilité d'utiliser le compte pour une ouverture de session interactive
- Gestion simplifiée des SPN (Service Principal Names)
- Pour les gMSA : possibilité d'utiliser le même compte sur plusieurs serveurs

**Credential Guard :**

Credential Guard est une fonctionnalité de sécurité de Windows qui utilise la virtualisation pour protéger les secrets d'authentification :

- Isolation des secrets dans un environnement virtualisé (VSM - Virtual Secure Mode)
- Protection contre les attaques de type Pass-the-Hash
- Nécessite du matériel supportant la virtualisation et UEFI Secure Boot

**Remote Credential Guard :**

Extension de Credential Guard pour les sessions RDP, protégeant les identifiants lors des connexions à distance :

- Les identifiants ne sont jamais transmis au système distant
- Réduction drastique du risque de vol d'identifiants lors de sessions d'administration distante

## Gestion des Mots de Passe dans les Scripts et GPP

Une source fréquente de fuite de secrets provient du stockage inadéquat de mots de passe dans des emplacements accessibles :

### Dangers des Mots de Passe en Clair

**Scripts dans SYSVOL :**

Le dossier SYSVOL, répliqué sur tous les contrôleurs de domaine et accessible en lecture à tous les utilisateurs authentifiés du domaine, ne doit JAMAIS contenir de scripts incluant des mots de passe, même obfusqués. Un attaquant ayant simplement un compte utilisateur standard peut accéder à ces scripts.

**Group Policy Preferences (GPP) :**

Les versions anciennes de Windows Server permettaient de stocker des mots de passe dans les GPP pour automatiser certaines configurations. Ces mots de passe étaient chiffrés avec une clé AES publiquement documentée par Microsoft, les rendant trivialement déchiffrables. Il est impératif de :

- Installer le correctif KB2962486 qui empêche la création de nouvelles GPP avec mots de passe
- Auditer le SYSVOL pour identifier et supprimer les GPP historiques contenant des mots de passe
- Remplacer ces mots de passe compromis sur tous les systèmes où ils étaient utilisés

# Analyse des Chemins d'Attaque

L'identification et le traitement des chemins d'attaque vers les ressources sensibles constituent un élément central de la démarche de cloisonnement. Un chemin d'attaque représente une séquence de faiblesses ou de relations que peut exploiter un attaquant pour progresser depuis un point d'entrée initial vers une cible privilégiée.

## Outils d'Analyse des Chemins d'Attaque

Plusieurs outils permettent d'identifier automatiquement les chemins d'attaque dans Active Directory :

**BloodHound :**

BloodHound est devenu l'outil de référence pour l'analyse des chemins d'attaque Active Directory. Il fonctionne en deux temps :

- **Collecte de données :** Un collecteur (SharpHound) interroge Active Directory pour recueillir des informations sur les relations entre objets : appartenances aux groupes, délégations, sessions actives, etc.
- **Analyse graphique :** Les données collectées sont importées dans une base de données graphe (Neo4j) permettant d'interroger visuellement les relations et d'identifier les chemins vers les objets sensibles

BloodHound peut identifier des chemins d'attaque complexes impliquant plusieurs sauts et relations qui seraient impossibles à détecter manuellement.

**Purple Knight (anciennement Semperis Directory Services Protector) :**

Cet outil commercial analyse la configuration Active Directory et identifie les vulnérabilités et les écarts par rapport aux bonnes pratiques de sécurité.

**PingCastle :**

Outil gratuit fournissant une évaluation de la sécurité Active Directory avec un focus sur les risques et les indicateurs de santé.

## Types de Chemins d'Attaque Courants

Les chemins d'attaque vers les ressources Tier 0 empruntent généralement l'une des formes suivantes :

- **Appartenances aux groupes privilégiés :** Un compte Tier 2 membre (directement ou indirectement) d'un groupe privilégié Tier 0
- **Délégations de contrôle :** Droits accordés à des comptes de niveau inférieur sur des objets de niveau supérieur (par exemple, droit de réinitialiser le mot de passe d'un compte Tier 0)
- **Sessions administratives :** Un administrateur Tier 0 ouvrant une session sur un système Tier 1 ou Tier 2, exposant ses identifiants
- **Propriété d'objets :** Un compte de niveau inférieur propriétaire d'un objet de niveau supérieur peut modifier ses permissions
- **GPO appliquées :** Une GPO modifiable par un compte de niveau inférieur mais appliquée à des objets de niveau supérieur
- **Relations d'approbation :** Chemins transitifs à travers des relations d'approbation mal configurées
- **Délégations Kerberos :** Comptes configurés avec une délégation non contrainte pouvant usurper l'identité d'autres comptes
- **Accès aux infrastructures support :** Accès administratifs aux hyperviseurs, aux baies de stockage, ou aux systèmes de sauvegarde hébergeant des ressources Tier 0

## Méthodologie de Traitement

Pour chaque chemin d'attaque identifié, une démarche systématique doit être appliquée :

1. **Évaluation du risque :** Quel est la probabilité d'exploitation ? Quel serait l'impact ? Y a-t-il des contrôles compensatoires ?
2. **Identification de solutions :** Quelles actions permettraient d'éliminer ou de réduire ce chemin d'attaque ?
3. **Analyse d'impact :** Quels seraient les impacts opérationnels de ces solutions ?
4. **Décision :** Éliminer le chemin, mettre en place des contrôles compensatoires, ou accepter le risque résiduel de manière documentée et validée
5. **Implémentation :** Déploiement de la solution retenue
6. **Vérification :** Confirmation que le chemin d'attaque a bien été éliminé ou réduit
7. **Documentation :** Consignation de l'analyse, de la décision et des actions dans un registre des risques

### Approche Pragmatique

Il est irréaliste de viser l'élimination de 100% des chemins d'attaque, particulièrement dans les grands environnements complexes. L'objectif est de traiter en priorité les chemins les plus critiques et les plus facilement exploitables, tout en documentant et en justifiant les chemins résiduels acceptés avec des contrôles compensatoires appropriés.

# Infrastructures Support et Chemins Indirects

Une erreur fréquente dans la mise en œuvre du modèle de tiering consiste à se concentrer exclusivement sur les serveurs et les comptes Active Directory, en négligeant les infrastructures support qui constituent pourtant des chemins d'attaque majeurs.

## Infrastructures de Virtualisation

Dans les environnements modernes, la grande majorité des serveurs sont virtualisés. Cette virtualisation crée des dépendances de sécurité critiques :

**Principe de catégorisation :**

Un hyperviseur hébergeant ne serait-ce qu'une seule machine virtuelle Tier 0 doit lui-même être catégorisé en Tier 0. En effet, un attaquant ayant compromis l'hyperviseur peut :

- Accéder à la mémoire des VM hébergées, extrayant les secrets d'authentification
- Modifier les fichiers de configuration ou les disques virtuels des VM
- Créer des snapshots des VM pour une analyse hors ligne
- Intercepter les communications réseau entre les VM

**Conséquences :**

Cette exigence a des implications importantes :

- Les hyperviseurs Tier 0 doivent être administrés uniquement depuis des postes d'administration Tier 0
- Idéalement, les VM Tier 0 devraient être hébergées sur des hyperviseurs dédiés, distincts de ceux hébergeant des VM de niveaux inférieurs
- Si une mutualisation est inévitable, des contrôles compensatoires stricts doivent être mis en place

### Infrastructures de Stockage

Les baies de stockage SAN ou NAS hébergeant des données Tier 0 doivent également être catégorisées en Tier 0 :

- Accès aux LUN ou volumes contenant des disques de VM Tier 0
- Possibilité de créer des snapshots ou des clones du stockage
- Accès potentiel aux données au repos si le chiffrement n'est pas activé

### Systèmes de Sauvegarde

Les systèmes de sauvegarde représentent un chemin d'attaque souvent négligé mais particulièrement dangereux :

- Les sauvegardes contiennent des copies complètes des systèmes, incluant potentiellement des secrets d'authentification
- Les sauvegardes de contrôleurs de domaine contiennent la base NTDS.dit avec tous les condensats de mots de passe
- Un attaquant accédant aux sauvegardes peut restaurer un contrôleur de domaine dans un environnement contrôlé pour extraire les secrets

**Mesures de protection :**

- Catégorisation des systèmes de sauvegarde du Tier 0 en Tier 0
- Chiffrement obligatoire de toutes les sauvegardes
- Contrôle d'accès strict aux médias de sauvegarde et aux clés de chiffrement
- Séparation physique des sauvegardes Tier 0
- Journalisation et surveillance de tous les accès aux sauvegardes Tier 0

## Conclusion du Chapitre

Les concepts et principes présentés dans ce chapitre constituent le socle théorique et méthodologique sur lequel repose l'implémentation pratique du modèle de tiering. La compréhension approfondie de ces concepts est essentielle avant d'aborder les aspects techniques détaillés de l'implémentation de chaque tier.

Les chapitres suivants détailleront l'implémentation concrète du modèle, en commençant par le Tier 0 qui requiert l'attention et les contrôles les plus stricts, puis en abordant les Tiers 1 et 2, et enfin en présentant les bonnes pratiques de gestion et de maintenance pour assurer la pérennité du modèle.

Il est important de garder à l'esprit que le modèle de tiering n'est pas une solution miracle qui élimine tous les risques, mais plutôt un cadre structuré qui, lorsqu'il est correctement implémenté et maintenu, réduit considérablement la surface d'attaque et limite la capacité des attaquants à progresser dans le système d'information.

CHAPITRE 3

# Implémentation Tier 0

### Importance Critique du Tier 0

Le Tier 0 représente le cœur absolu de la sécurité de votre système d'information. Sa compromission entraîne invariablement une compromission totale de l'ensemble de l'infrastructure Active Directory et de toutes les ressources qu'elle protège. L'implémentation rigoureuse des contrôles de sécurité du Tier 0 n'est pas optionnelle : elle constitue la condition sine qua non de l'efficacité de tout le modèle de tiering.

## Principes Fondamentaux du Tier 0

L'implémentation du Tier 0 repose sur plusieurs principes fondamentaux qui doivent guider toutes les décisions architecturales et opérationnelles :

### Minimisation de la Surface d'Attaque

Le premier principe consiste à réduire au strict minimum le nombre de ressources catégorisées en Tier 0. Chaque ressource ajoutée au Tier 0 augmente la complexité de sa gestion et élargit sa surface d'attaque potentielle. Il faut systématiquement se poser la question : cette ressource doit-elle absolument être en Tier 0, ou existe-t-il une alternative permettant de la catégoriser à un niveau inférieur ?

Cette minimisation s'applique à tous les types de ressources :

- **Nombre de contrôleurs de domaine :** Déployer uniquement le nombre nécessaire pour assurer la haute disponibilité et les performances requises, sans surplus.
- **Comptes privilégiés :** Limiter drastiquement le nombre de comptes disposant de privilèges Tier 0. Idéalement, une organisation moyenne ne devrait pas avoir plus de 5 à 10 comptes d'administration de domaine actifs.

- **Groupes privilégiés :** Restreindre l'appartenance aux groupes comme Domain Admins, Enterprise Admins, Schema Admins au strict nécessaire.
- **Applications sur les contrôleurs de domaine :** Les contrôleurs de domaine ne devraient exécuter AUCUNE application autre que les services Active Directory eux-mêmes. Pas de serveur de fichiers, pas de serveur d'impression, pas d'agent de sauvegarde non certifié.
- **Accès physiques :** Limiter drastiquement le nombre de personnes disposant d'un accès physique aux salles hébergeant les ressources Tier 0.

## Isolation Maximale

Le Tier 0 doit être isolé des autres tiers par tous les moyens techniques disponibles. Cette isolation doit être multicouche et redondante :

- **Isolation réseau :** Bien que le filtrage réseau seul soit insuffisant dans un environnement AD, il constitue une couche de défense importante. Les contrôleurs de domaine doivent être dans des segments réseau dédiés avec des règles de pare-feu strictes.
- **Isolation administrative :** Les comptes et systèmes Tier 0 doivent être administrés exclusivement depuis des ressources Tier 0 dédiées.
- **Isolation logique dans Active Directory :** Création d'unités organisationnelles dédiées avec blocage de l'héritage des GPO et contrôles d'accès stricts.
- **Isolation des secrets :** Utilisation de technologies comme Credential Guard pour isoler les secrets d'authentification même au sein des systèmes Tier 0.

## Défense en Profondeur Renforcée

Chaque couche de sécurité doit être considérée comme potentiellement contournable. La défense en profondeur implique de multiplier les couches indépendantes, de sorte que la compromission d'une couche ne suffise pas à compromettre l'ensemble :

- Authentification multi-facteurs obligatoire pour tous les accès Tier 0
- Chiffrement complet des disques sur tous les systèmes Tier 0
- Durcissement système selon les standards de sécurité les plus exigeants
- Surveillance continue avec détection d'anomalies comportementales
- Restriction applicative stricte (liste blanche des exécutables autorisés)
- Journalisation exhaustive de toutes les actions administratives

# Structure Organisationnelle dans Active Directory

La structure organisationnelle est le fondement de l'implémentation technique du Tier 0 dans Active Directory.

## Création de l'Unité Organisationnelle Tier 0

La première étape consiste à créer une structure d'unités organisationnelles dédiée pour héberger tous les objets du Tier 0 :

### Structure Recommandée

```
domain.local
│
└── Tier 0
    ├── Accounts
    │   ├── Users (comptes d'administration Tier 0)
    │   ├── Service Accounts (comptes de service gérés Tier 0)
    │   └── Break Glass (comptes de secours)
    │
    ├── Groups
    │   ├── Administrative (groupes d'administration)
    │   ├── Service (groupes de service)
    │   └── Restricted (groupes à accès restreint)
    │
    ├── Computers
    │   ├── Domain Controllers
    │   ├── PAW (postes d'administration privilégiés)
    │   ├── Certificate Authority
    │   ├── ADFS (si applicable)
    │   └── Identity Sync (serveurs de synchronisation)
    │
    └── Quarantine (objets en cours de catégorisation)
```

**Propriétés cruciales de l'OU Tier 0 :**

- **Blocage de l'héritage GPO :** L'OU Tier 0 principale doit avoir son héritage GPO bloqué pour empêcher l'application de stratégies définies à des niveaux supérieurs et potentiellement contrôlées par des administrateurs de niveau inférieur.
- **Contrôle d'accès restrictif :** Seuls les administrateurs Tier 0 doivent disposer de droits de modification sur l'OU Tier 0 et ses sous-OU. Les droits par défaut accordés à des groupes comme Account Operators ou Server Operators doivent être révoqués.
- **Protection contre la suppression :** Activer la protection contre la suppression accidentelle sur toutes les OU Tier 0.
- **Journalisation avancée :** Activer l'audit SACL (System Access Control List) pour enregistrer toutes les tentatives d'accès et de modification.

## Gestion des Stratégies de Groupe Tier 0

Les stratégies de groupe appliquées au Tier 0 constituent un élément critique de sa sécurité. Leur gestion doit respecter des règles strictes :

### Principes de Gestion des GPO Tier 0

1. **Gestion exclusive :** Seuls les administrateurs Tier 0 peuvent créer, modifier ou lier des GPO s'appliquant au Tier 0.
2. **Stockage dédié :** Idéalement, créer un dossier spécifique dans SYSVOL pour les GPO Tier 0, bien que techniquement SYSVOL reste accessible en lecture à tous les utilisateurs authentifiés.
3. **Contrôle de version :** Maintenir une documentation stricte de toutes les modifications apportées aux GPO Tier 0, idéalement via un système de gestion de versions.
4. **Test systématique :** Toute modification de GPO Tier 0 doit être testée dans un environnement de lab avant déploiement en production.
5. **Séparation des GPO :** Ne JAMAIS utiliser la même GPO pour des objets Tier 0 et des objets de niveau inférieur.

**GPO essentielles pour le Tier 0 :**

- **GPO de durcissement des contrôleurs de domaine :** Désactivation des services inutiles, restriction des protocoles, configuration des pare-feu locaux.
- **GPO de durcissement des PAW :** Restriction applicative, blocage USB, désactivation Internet et email, Credential Guard, Device Guard.
- **GPO de stratégies de mots de passe :** Politique de mots de passe renforcée spécifiquement pour les comptes Tier 0 (longueur minimale 20 caractères, complexité maximale, historique étendu).
- **GPO d'audit et journalisation :** Activation de l'audit avancé pour tous les événements de sécurité critiques.
- **GPO de restrictions de connexion :** Configuration des restrictions sur où et quand les comptes Tier 0 peuvent être utilisés.

# Sécurisation des Contrôleurs de Domaine

Les contrôleurs de domaine sont le cœur battant du Tier 0. Leur sécurisation doit être absolue et sans compromis.

## Durcissement Système des Contrôleurs de Domaine

Le durcissement des contrôleurs de domaine va bien au-delà de l'installation par défaut de Windows Server :

**Configuration réseau sécurisée :**

- Désactivation de IPv6 si non utilisé (ou sécurisation appropriée si utilisé)
- Configuration de SMB signing obligatoire
- Désactivation de SMBv1 (protocole obsolète et vulnérable)
- Configuration LDAP signing et LDAP channel binding
- Activation de l'exigence de Kerberos AES (désactivation de DES et RC4 si possible)

**Configuration des services :**

- Désactivation de tous les services non essentiels
- Désactivation du service Print Spooler (vecteur d'attaque fréquent)
- Configuration stricte des services RPC
- Désactivation de Windows Update automatique (géré manuellement avec test préalable)

**Protection de la base Active Directory :**

- Activation de la protection DIT (Directory Information Tree)
- Chiffrement complet du disque hébergeant NTDS.dit
- Sauvegarde quotidienne avec rétention appropriée
- Vérification régulière de l'intégrité de la base via ntdsutil

## Gestion des Mises à Jour

La gestion des mises à jour sur les contrôleurs de domaine requiert une approche équilibrée entre sécurité et stabilité :

### Processus de Gestion des Correctifs

1. **Veille de sécurité :** Surveillance quotidienne des bulletins de sécurité Microsoft, notamment les correctifs critiques pour Active Directory.
2. **Évaluation de criticité :** Pour chaque correctif, évaluer son importance pour la sécurité versus les risques de régression.
3. **Test en environnement dédié :** Déploiement sur un contrôleur de domaine de test reproduisant l'environnement de production.

4. **Validation fonctionnelle :** Tests approfondis des fonctions critiques : authentification, réplication, groupe policy, DNS.
5. **Déploiement progressif :** Application d'abord sur un seul DC de production, observation pendant 24-48h, puis extension aux autres DC.
6. **Plan de retour arrière :** Sauvegarde complète avant chaque mise à jour et procédure documentée de rollback.
7. **Fenêtre de maintenance :** Planification de fenêtres de maintenance spécifiques, évitant les périodes critiques pour l'entreprise.

**Cas particuliers nécessitant une attention spéciale :**

- Mises à jour de sécurité critiques pour Active Directory (déploiement accéléré après test)
- Correctifs pour les vulnérabilités activement exploitées (évaluation urgente)
- Mises à jour fonctionnelles non sécuritaires (déploiement optionnel après analyse risques/bénéfices)
- Mises à jour de niveau fonctionnel de la forêt ou du domaine (planification extensive, test approfondi)

## Sécurité Physique des Contrôleurs de Domaine

La sécurité physique est souvent négligée mais constitue un point critique :

### Menaces Physiques

Un attaquant ayant un accès physique à un contrôleur de domaine peut :

- Démarrer le serveur sur un média externe pour accéder aux données
- Extraire les disques durs pour une analyse hors ligne
- Effectuer une attaque DMA (Direct Memory Access) pour extraire les secrets de la RAM
- Implanter un dispositif de surveillance matériel (keylogger, sniffer réseau)
- Effectuer un reset du mot de passe du compte DSRM (Directory Services Restore Mode)

**Mesures de protection physique :**

- **Salle serveur sécurisée :** Contrôle d'accès physique strict, vidéosurveillance, journalisation des accès
- **Chiffrement complet des disques :** BitLocker avec TPM et code PIN obligatoire au démarrage
- **BIOS/UEFI sécurisé :** Mot de passe BIOS, désactivation du boot sur USB/CD, Secure Boot activé

- **Protection contre les attaques DMA :** Désactivation des ports non nécessaires, Kernel DMA Protection sur Windows 10/11
- **Détection d'intrusion physique :** Capteurs d'ouverture de châssis, alertes en cas de manipulation
- **Sites distants :** Utilisation de RODC (Read-Only Domain Controllers) pour les sites à sécurité physique limitée

# Comptes et Groupes Privilégiés

La gestion rigoureuse des comptes et groupes privilégiés est au cœur de la sécurité du Tier 0.

## Groupes Privilégiés Natifs

Active Directory intègre plusieurs groupes privilégiés par défaut. Leur gestion doit être particulièrement stricte :

| Groupe | Portée | Privilèges | Recommandation |
|---|---|---|---|
| **Enterprise Admins** | Forêt | Administration complète de tous les domaines de la forêt | Membres : 0 en temps normal. Ajouter temporairement uniquement pour opérations exceptionnelles nécessitant une portée forêt |
| **Domain Admins** | Domaine | Administration complète du domaine, admin local sur tous les systèmes | Membres : 2 à 5 maximum. Comptes utilisés uniquement pour administration DC et AD |
| **Schema Admins** | Forêt | Modification du schéma Active Directory | Membres : 0 en temps normal. Ajout temporaire uniquement pour modifications de schéma planifiées |
| **Administrators** | Domaine | Administration du domaine et des DC | Membres : Uniquement les comptes strictement nécessaires. Revue trimestrielle |
| **Backup Operators** | Domaine | Sauvegarde et restauration de fichiers | Éviter l'utilisation. Utiliser des comptes de service gérés avec délégations fines |
| **Account Operators** | Domaine | Gestion de comptes (hors comptes privilégiés) | Éviter l'utilisation. Utiliser des délégations fines spécifiques |
| **Server Operators** | Domaine | Administration de serveurs | Ne JAMAIS utiliser. Privilèges excessifs et mal délimités |

## Stratégie de Comptes Dédiés

Chaque administrateur Tier 0 doit disposer de plusieurs comptes distincts pour différents usages :

### Exemple de Nomenclature de Comptes

Pour un administrateur nommé Jean Dupont :

- `jean.dupont` - Compte utilisateur standard (Tier 2) pour email, bureautique, navigation
- `jean.dupont-adm1` - Compte d'administration Tier 1 pour serveurs applicatifs
- `jean.dupont-adm0` - Compte d'administration Tier 0 pour DC et infrastructure AD
- `jean.dupont-bg0` - Compte break-glass Tier 0 (secours, usage exceptionnel uniquement)

**Règles d'utilisation strictes :**

- Chaque compte est utilisé UNIQUEMENT pour son tier désigné

- Les mots de passe sont différents entre tous les comptes
- Les comptes Tier 0 ne peuvent JAMAIS se connecter à des systèmes Tier 1 ou Tier 2
- Les comptes privilégiés ne doivent JAMAIS être utilisés pour email ou navigation
- Authentification multi-facteurs obligatoire pour les comptes Tier 0

### Comptes Break-Glass (Bris de Glace)

Les comptes break-glass sont des comptes de secours permettant de reprendre le contrôle de l'Active Directory en cas de situation d'urgence :

**Caractéristiques des comptes break-glass :**

- Membres du groupe Domain Admins ou Administrators
- Mots de passe ultra-complexes (40+ caractères), stockés dans un coffre-fort physique scellé
- Configurés pour ne JAMAIS expirer
- Exclus des politiques de verrouillage de compte
- Alertes immédiates en cas d'utilisation
- Revue mensuelle pour vérifier qu'ils sont toujours fonctionnels (sans les utiliser)
- Procédure documentée et testée annuellement pour leur utilisation

**Situations d'utilisation légitimes :**

- Tous les comptes d'administration normaux sont verrouillés ou compromis
- Problème critique de réplication empêchant l'administration normale
- Corruption de l'annuaire nécessitant une restauration d'urgence
- Défaillance du système MFA bloquant tous les accès privilégiés

## Postes d'Administration Privilégiée (PAW)

Les PAW (Privileged Access Workstations) constituent un élément absolument critique de la sécurité Tier 0. Ils sont les seuls systèmes depuis lesquels l'administration des ressources Tier 0 doit être effectuée.

### Principe et Architecture des PAW

Un PAW est un poste de travail durci, dédié exclusivement à l'administration, et isolé de tout vecteur d'attaque courant :

### Caractéristiques Essentielles d'un PAW Tier 0

**Isolation fonctionnelle :**

- AUCUN accès Internet
- AUCUN client de messagerie
- AUCUNE application bureautique (Word, Excel, PDF readers)
- UNIQUEMENT des outils d'administration : RSAT, PowerShell, outils AD, RDP

**Durcissement système :**

- Windows 10/11 Enterprise (jamais Home ou Pro)
- Credential Guard activé
- Device Guard / Application Control (liste blanche stricte des exécutables)
- Virtualization-Based Security (VBS)
- Attack Surface Reduction rules
- Chiffrement BitLocker avec TPM + PIN
- Toutes les mises à jour de sécurité appliquées

**Contrôle d'accès physique :**

- Emplacement physique sécurisé
- Ports USB désactivés (sauf si clé de sécurité MFA requise)
- Lecteurs CD/DVD désactivés
- Boot sur réseau désactivé
- Écran de confidentialité pour éviter le shoulder surfing

**Authentification renforcée :**

- Authentification multi-facteurs obligatoire (carte à puce, clé FIDO2, Windows Hello for Business)
- Pas d'authentification par mot de passe seul
- Délai de verrouillage automatique court (2-3 minutes d'inactivité)

## Déploiement et Gestion des PAW

Le déploiement des PAW doit suivre un processus rigoureux :

1. **Image de référence :** Création d'une image maître durcie, validée par l'équipe sécurité, servant de base à tous les PAW.

2. **Déploiement sécurisé :** Installation dans un environnement contrôlé, jamais connecté au réseau de production avant configuration complète.
3. **Configuration initiale :** Application de toutes les GPO de sécurité, installation des outils d'administration, configuration MFA.
4. **Tests de validation :** Vérification que toutes les restrictions sont effectives et que les outils nécessaires fonctionnent.
5. **Assignation :** Attribution à un administrateur spécifique, avec traçabilité et responsabilité.
6. **Maintenance :** Mises à jour mensuelles de l'image de référence, redéploiement périodique pour éviter la dérive de configuration.

**Nombre de PAW nécessaires :**

- Au minimum : 1 PAW par administrateur Tier 0
- Idéalement : 2 PAW par administrateur (un principal, un de secours)
- Plus : PAW de secours partagés pour situations d'urgence

# Protocoles d'Authentification et Restrictions

La maîtrise des protocoles d'authentification est cruciale pour empêcher les attaques latérales.

## Désactivation de NTLM

NTLM est un protocole d'authentification hérité présentant de nombreuses faiblesses de sécurité, notamment sa vulnérabilité aux attaques Pass-the-Hash. Sa désactivation progressive est fortement recommandée :

### Stratégie de Désactivation NTLM

**Phase 1 - Audit (Durée : 1-2 mois) :**

- Activation de l'audit NTLM via GPO pour identifier toutes les authentifications NTLM
- Collecte et analyse des logs pour identifier les systèmes et applications utilisant encore NTLM
- Création d'un plan de migration vers Kerberos pour chaque utilisation identifiée

**Phase 2 - Migration (Durée : variable selon complexité) :**

- Configuration de SPN (Service Principal Names) pour permettre l'authentification Kerberos
- Mise à jour des applications et scripts pour utiliser Kerberos

- Tests approfondis de chaque migration

**Phase 3 - Restriction Tier 0 :**

- Blocage de NTLM pour les comptes Tier 0 (via groupe Protected Users ou silos d'authentification)
- Configuration des DC pour refuser les authentifications NTLM des comptes Tier 0
- Surveillance des tentatives bloquées

**Phase 4 - Blocage Généralisé (optionnel, selon contexte) :**

- Blocage de NTLM au niveau du domaine pour tous les comptes
- Maintien d'exemptions uniquement pour applications héritées critiques sans alternative

## Groupe Protected Users

Le groupe Protected Users, introduit dans Windows Server 2012 R2, applique automatiquement des restrictions de sécurité renforcées à ses membres :

**Protections automatiques :**

- Impossibilité d'utiliser NTLM, Digest ou CredSSP pour l'authentification
- Impossibilité de pré-authentification Kerberos avec DES ou RC4
- Tickets Kerberos TGT avec durée de vie limitée à 4 heures (non renouvelables)
- Impossibilité de délégation Kerberos (contrainte ou non contrainte)
- Impossibilité de mise en cache des identifiants

**Membres recommandés :**

- Tous les comptes d'administration Tier 0 (sauf comptes de service si incompatibilité)
- Tous les comptes membres de Domain Admins, Enterprise Admins, Schema Admins
- Comptes de service privilégiés (après tests de compatibilité)

**Précautions avant ajout :**

- Vérifier que le niveau fonctionnel du domaine est Windows Server 2012 R2 minimum
- Tester l'impact sur l'authentification des comptes concernés
- S'assurer que les applications supportent ces restrictions
- Ne JAMAIS ajouter le compte Administrator intégré (risque de blocage total en cas de problème)

### Silos d'Authentification

Les silos d'authentification permettent de restreindre précisément où et comment les comptes privilégiés peuvent être utilisés :

Un silo d'authentification définit :

- Quels comptes en font partie
- Sur quels systèmes ces comptes peuvent s'authentifier
- Quels services peuvent utiliser ces comptes
- Les restrictions de délégation Kerberos applicables

**Exemple de configuration Tier 0 :**

- Silo "Tier0-DomainAdmins" contenant tous les comptes Domain Admins
- Authentification autorisée uniquement vers : les contrôleurs de domaine et les PAW Tier 0
- Toute tentative d'authentification vers d'autres systèmes est bloquée et journalisée

## Infrastructures Support du Tier 0

Les infrastructures support hébergeant des ressources Tier 0 doivent elles-mêmes être catégorisées et sécurisées en Tier 0.

### Infrastructure de Virtualisation

Si les contrôleurs de domaine sont virtualisés (configuration de plus en plus courante) :

- **Hyperviseurs dédiés :** Idéalement, les VM Tier 0 doivent être sur des hyperviseurs dédiés, administrés uniquement par des comptes Tier 0 depuis des PAW Tier 0.
- **Isolation réseau :** Les vSwitches et segments réseau hébergeant les VM Tier 0 doivent être isolés.
- **Gestion des snapshots :** Les snapshots de VM Tier 0 contiennent la RAM avec potentiellement des secrets. Leur gestion doit être strictement contrôlée.
- **Accès à la console :** L'accès aux consoles de gestion (vCenter, SCVMM, Hyper-V Manager) doit nécessiter authentification Tier 0 depuis PAW.
- **Sauvegardes des fichiers VM :** Les fichiers VMDK/VHDX doivent être sauvegardés avec chiffrement et accès restreint.

### Autorité de Certification PKI

Les autorités de certification délivrant des certificats utilisables pour l'authentification Tier 0 doivent être catégorisées en Tier 0 :

- CA racine hors ligne, dans un environnement physiquement sécurisé
- CA subordinées pour l'émission de certificats, administrées depuis PAW Tier 0
- Templates de certificats pour authentification Tier 0 avec ACL strictes
- Révocation de certificats processée et surveillée
- Clés privées de la CA protégées par HSM (Hardware Security Module) idéalement

### Serveurs de Synchronisation Cloud

Les serveurs de synchronisation comme Azure AD Connect ou les serveurs ADFS doivent être catégorisés en Tier 0 car leur compromission permet généralement de compromettre le domaine :

- Serveurs dédiés, ne servant AUCUNE autre fonction
- Administration depuis PAW Tier 0 uniquement
- Surveillance accrue des synchronisations et des tentatives d'authentification
- Clés de chiffrement et secrets stockés de manière sécurisée

## Conclusion du Chapitre

L'implémentation du Tier 0 constitue la pierre angulaire de tout le modèle de tiering. Sans un Tier 0 correctement sécurisé et rigoureusement géré, les efforts de sécurisation des autres tiers seront vains. Les principes et pratiques présentés dans ce chapitre ne sont pas optionnels : ils représentent le minimum requis pour protéger efficacement le cœur de confiance de votre système d'information.

Le chapitre suivant abordera l'implémentation des Tiers 1 et 2, qui, bien que moins critiques que le Tier 0, nécessitent également des contrôles de sécurité appropriés pour assurer la protection globale du système d'information.

CHAPITRE 4

# Implémentation Tiers 1 et 2

## Vue d'Ensemble des Tiers 1 et 2

Après avoir sécurisé le Tier 0, qui constitue le cœur de confiance de l'infrastructure Active Directory, il est essentiel de porter son attention sur les Tiers 1 et 2. Ces niveaux, bien que moins critiques que le Tier 0 en termes de privilèges système, revêtent une importance capitale pour la protection des valeurs métier de l'organisation et la prévention des attaques latérales.

La distinction fondamentale entre ces deux tiers réside dans leur fonction et leur niveau d'exposition :

- **Tier 1** englobe les serveurs d'applications métier et les systèmes hébergeant ou traitant les données critiques de l'entreprise. Il représente la confiance dans les valeurs métiers.
- **Tier 2** comprend les postes de travail des utilisateurs et les moyens d'accès aux ressources. Il représente la confiance dans les moyens d'accès, avec la surface d'exposition la plus importante.

L'implémentation de ces deux tiers suit des principes similaires à ceux du Tier 0, mais avec des contraintes opérationnelles généralement plus souples pour maintenir un équilibre entre sécurité et productivité.

## Implémentation du Tier 1

### Identification des Ressources Tier 1

La première étape de l'implémentation du Tier 1 consiste à identifier précisément quelles ressources doivent être catégorisées à ce niveau. Cette identification doit être guidée par l'analyse des valeurs métiers de l'organisation effectuée lors de la phase d'étude.

**Ressources typiquement catégorisées en Tier 1 :**

- **Serveurs d'applications métier :** ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), systèmes de gestion financière, applications RH, outils de BI (Business Intelligence).
- **Serveurs de bases de données métier :** Instances SQL Server, Oracle, PostgreSQL, MySQL hébergeant des données métier critiques.
- **Serveurs de messagerie :** Serveurs Exchange, systèmes de messagerie collaborative.
- **Serveurs de fichiers métier :** Partages réseau contenant des données sensibles ou essentielles aux activités de l'entreprise.
- **Serveurs web applicatifs :** Serveurs IIS, Apache, nginx hébergeant des applications internes critiques.
- **Serveurs de développement et CI/CD :** Serveurs de gestion de code source (GitLab, Azure DevOps), serveurs de compilation et de déploiement continu.
- **Systèmes industriels critiques :** SCADA, superviseurs de production, systèmes de contrôle-commande.
- **Infrastructures de virtualisation Tier 1 :** Hyperviseurs hébergeant les serveurs Tier 1, mais pas de VM Tier 0.
- **Systèmes de sauvegarde des serveurs Tier 1 :** Serveurs et infrastructure de sauvegarde dédiés au Tier 1.

## Cas Particuliers et Décisions de Catégorisation

Certains systèmes peuvent présenter des caractéristiques mixtes nécessitant une analyse approfondie :

- **Serveurs de déploiement (SCCM, WSUS) :** S'ils déploient uniquement sur le Tier 1, ils sont Tier 1. S'ils déploient également sur le Tier 0, ils doivent être catégorisés Tier 0 ou divisés en instances séparées.
- **Serveurs de monitoring :** S'ils supervisent le Tier 0, ils doivent être Tier 0. Sinon, ils peuvent être Tier 1.
- **Serveurs de journalisation (SIEM) :** S'ils collectent et stockent des logs Tier 0, ils doivent être catégorisés Tier 0.
- **Serveurs DNS secondaires :** Si les contrôleurs de domaine hébergent DNS, tout serveur DNS secondaire doit être au minimum Tier 1, voire Tier 0 selon l'architecture.

Le principe directeur reste : **un système doit être catégorisé au niveau du tier le plus élevé qu'il peut influencer ou compromettre.**

## Structure Organisationnelle Tier 1

Comme pour le Tier 0, une structure d'unités organisationnelles dédiée doit être créée pour le Tier 1 :

### Structure OU Recommandée pour le Tier 1

```
domain.local
│
└── Tier 1
    ├── Accounts
    │   ├── Admins (administrateurs serveurs)
    │   ├── Service Accounts (comptes de service)
    │   └── Application Accounts (comptes applicatifs)
    │
    ├── Groups
    │   ├── Administrative
    │   ├── Application Access
    │   └── Service Management
    │
    ├── Servers
    │   ├── Database Servers
    │   ├── Application Servers
    │   ├── File Servers
    │   ├── Web Servers
    │   ├── Mail Servers
    │   └── Development Servers
    │
    └── Management
        ├── PAW (postes d'admin Tier 1)
        └── Jump Servers (bastions d'administration)
```

**Configuration des OU Tier 1 :**

- Blocage de l'héritage des GPO sur l'OU Tier 1 racine
- Contrôle d'accès : seuls les administrateurs Tier 1 et Tier 0 peuvent modifier ces OU
- Délégation de droits spécifiques pour permettre la gestion du Tier 1 sans accès au Tier 0
- Protection contre la suppression accidentelle activée
- Audit des modifications activé

## Comptes d'Administration Tier 1

Les comptes d'administration Tier 1 nécessitent une gestion similaire à celle du Tier 0, mais avec quelques assouplissements pragmatiques :

**Principes de gestion :**

- **Comptes dédiés :** Chaque administrateur dispose d'un compte dédié pour l'administration Tier 1, distinct de son compte utilisateur standard.

- **Séparation stricte :** Les comptes Tier 1 ne peuvent JAMAIS administrer le Tier 0, ni être utilisés pour des activités Tier 2 (bureautique, email).
- **Authentification multi-facteurs recommandée :** Bien que pas toujours obligatoire comme pour le Tier 0, la MFA est fortement recommandée pour les comptes Tier 1.
- **Délégation granulaire :** Plutôt que d'accorder des droits Domain Admins, créer des groupes spécifiques avec des délégations fines (admins serveurs SQL, admins serveurs Exchange, etc.).
- **Principe de moindre privilège :** Un administrateur de bases de données n'a pas besoin de droits sur les serveurs web, et vice versa.

### Exemple de Délégations Tier 1

| Groupe | Périmètre | Droits Accordés |
|---|---|---|
| Tier1-ServerAdmins | OU Tier 1\Servers | Administrateur local sur tous les serveurs Tier 1 |
| Tier1-DatabaseAdmins | Serveurs de bases de données | Administrateur local + droits sysadmin SQL |
| Tier1-ExchangeAdmins | Serveurs Exchange | Organization Management Exchange |
| Tier1-WebAdmins | Serveurs Web | Administrateur local + gestion IIS |

## Postes d'Administration Tier 1

Comme pour le Tier 0, l'administration du Tier 1 doit se faire depuis des postes dédiés. Cependant, les contraintes peuvent être légèrement assouplies pour faciliter les opérations :

**Options pour l'administration Tier 1 :**

1. **PAW Tier 1 dédiés :** Postes durcis similaires aux PAW Tier 0, mais avec accès uniquement au Tier 1. Configuration recommandée pour les environnements les plus sensibles.
2. **Jump Servers / Bastions :** Serveurs Windows Server d'administration centralisés accessibles en RDP depuis le Tier 2, mais d'où part l'administration vers le Tier 1. Solution plus souple que les PAW.
3. **Restricted Admin Workstations (RAW) :** Postes de travail standard mais avec restrictions renforcées lorsque utilisés pour l'administration (Remote Credential Guard, restrictions applicatives).

### Configuration d'un Jump Server Tier 1

**Caractéristiques essentielles :**

- Windows Server 2019 ou ultérieur
- Chiffrement BitLocker
- Accès RDP uniquement depuis le Tier 2, avec MFA requise
- Remote Credential Guard activé pour toutes les connexions sortantes
- Aucun accès Internet direct
- Restriction applicative : uniquement outils d'administration
- Journalisation exhaustive de toutes les sessions
- Session timeout après 30 minutes d'inactivité

**Avantages :**

- Centralisation de l'administration facilitant la surveillance
- Isolation des secrets d'authentification Tier 1 grâce à Remote Credential Guard
- Plus simple à gérer et déployer que des PAW individuels
- Permet l'administration depuis n'importe quel poste Tier 2 avec authentification appropriée

**Inconvénients :**

- Point de défaillance unique si mal configuré
- Nécessite une haute disponibilité (déployer au moins 2 jump servers)
- Ressource partagée nécessitant une gestion rigoureuse des sessions

## Sécurisation des Serveurs Tier 1

Les serveurs Tier 1 doivent être sécurisés selon des standards élevés, bien que généralement moins contraignants que le Tier 0 :

**Durcissement système :**

- Application des baselines de sécurité Microsoft ou CIS (Center for Internet Security)
- Désactivation des services et protocoles non nécessaires
- Restriction des ports ouverts au strict nécessaire
- Configuration du pare-feu Windows avec règles strictes
- Activation de l'audit de sécurité avancé
- Déploiement d'un EDR (Endpoint Detection and Response)

**Gestion des comptes locaux :**

- Déploiement de LAPS sur tous les serveurs Tier 1
- Désactivation du compte administrateur local intégré (si possible selon les applications)
- Pas de partage de mots de passe administrateurs locaux entre serveurs
- Droits de lecture LAPS accordés uniquement aux administrateurs Tier 1

**Gestion des comptes de service :**

- Utilisation systématique de gMSA (Group Managed Service Accounts) pour les services Windows
- Pour les applications ne supportant pas gMSA : mots de passe ultra-complexes, rotation régulière
- Aucun compte de service ne doit être membre de groupes privilégiés Tier 0
- Délégations SPN appropriées pour permettre l'authentification Kerberos

**Restriction des authentifications :**

- Les comptes Tier 1 peuvent s'authentifier sur les serveurs Tier 1 et les PAW/Jump Servers Tier 1
- Les comptes Tier 1 ne peuvent PAS s'authentifier sur le Tier 0 ou le Tier 2
- Les comptes Tier 2 ne peuvent PAS s'authentifier sur les serveurs Tier 1 (sauf utilisateurs applicatifs pour accès aux services, pas administration)
- Configuration via silos d'authentification ou restrictions de connexion dans les propriétés des comptes

## Segmentation Réseau du Tier 1

La segmentation réseau joue un rôle important dans la protection du Tier 1, bien qu'elle ne soit pas suffisante à elle seule :

**Architecture réseau recommandée :**

- **VLAN dédiés :** Les serveurs Tier 1 dans des VLAN séparés du Tier 2
- **Zones DMZ :** Les serveurs accessibles depuis Internet (serveurs web publics) dans une DMZ avec filtrage strict
- **Micro-segmentation :** Séparation des différents types de serveurs (bases de données, applications, web) dans des sous-réseaux distincts

- **Règles de pare-feu :**
  - Autoriser uniquement les flux nécessaires entre Tier 2 et Tier 1 (accès applicatifs, pas RDP)
  - Autoriser les flux d'administration depuis les PAW/Jump Servers Tier 1
  - Bloquer tout flux direct entre Tier 1 et Tier 0 (à l'exception des flux AD nécessaires : Kerberos, LDAP, DNS)
  - Journaliser toutes les tentatives de connexion bloquées

# Implémentation du Tier 2

## Caractéristiques du Tier 2

Le Tier 2 présente des caractéristiques particulières qui influencent son implémentation :

- **Volume important :** Généralement le tier contenant le plus de ressources (tous les postes utilisateurs)
- **Exposition maximale :** Surface d'attaque la plus large (Internet, email, périphériques USB, ingénierie sociale)
- **Hétérogénéité :** Grande variété de matériels, systèmes d'exploitation, et usages
- **Contraintes de productivité :** Les restrictions de sécurité ne doivent pas entraver excessivement le travail des utilisateurs
- **Point d'entrée principal des attaques :** C'est souvent par le Tier 2 que commencent les compromissions

## Structure Organisationnelle Tier 2

### Structure OU Tier 2

```
domain.local
│
└── Tier 2
    ├── Users
    │   ├── Standard Users
    │   ├── VIP Users (dirigeants, RH, finance)
    │   └── External Contractors
    │
    ├── Workstations
    │   ├── Desktops
    │   ├── Laptops
    │   └── Kiosks
    │
    ├── Mobile Devices
    │   ├── Smartphones
```

```
│   └── Tablets
│
├── Groups
│   ├── Access Control
│   └── Software Deployment
│
└── Service Accounts
    └── Tier2 Support Services
```

## Sécurisation des Postes de Travail

La sécurisation des postes de travail Tier 2 vise à réduire le risque de compromission initiale et à limiter les possibilités de mouvement latéral en cas d'infection :

**Configuration de sécurité de base :**

- **Chiffrement des disques :** BitLocker activé sur tous les postes, particulièrement les portables
- **Antivirus / EDR :** Déploiement d'une solution de protection moderne avec détection comportementale
- **Pare-feu activé :** Configuration du pare-feu Windows avec règles appropriées
- **Mises à jour automatiques :** Windows Update configuré pour installer automatiquement les mises à jour critiques et de sécurité
- **Désactivation des comptes administrateurs locaux :** Les utilisateurs ne doivent PAS avoir de droits administrateurs locaux
- **LAPS :** Déploiement de LAPS pour gérer les mots de passe administrateurs locaux
- **AppLocker ou WDAC :** Restriction applicative pour bloquer l'exécution de logiciels non autorisés

**Protection contre les vecteurs d'attaque courants :**

- **Protection email :**
  - Filtrage anti-spam et anti-malware
  - Blocage des types de pièces jointes dangereuses (.exe, .scr, .vbs, .js, macros Office)
  - Formation régulière des utilisateurs au phishing
  - Simulations de phishing pour maintenir la vigilance
- **Protection web :**
  - Proxy web avec filtrage de contenu
  - Blocage des sites malveillants connus
  - Scan des téléchargements
  - Isolation des navigateurs (sandbox) pour les sites non approuvés

- **Contrôle USB :**
  - Blocage par défaut des périphériques USB non autorisés
  - Liste blanche de périphériques approuvés si nécessaire
  - Scan automatique de tout périphérique USB connecté
- **Protection contre les macros :**
  - Désactivation par défaut des macros Office
  - Si macros nécessaires : restriction aux fichiers signés de sources approuvées

## Gestion des Accès Privilégiés Locaux

Un défi majeur du Tier 2 est la gestion des besoins ponctuels en privilèges administratifs locaux :

**Problématique :**

Certaines actions légitimes nécessitent temporairement des droits administratifs locaux (installation de logiciels spécifiques, modification de configuration, dépannage). Accorder de manière permanente ces droits créerait un risque de sécurité majeur.

**Solutions :**

1. **Élévation juste-à-temps :** Utilisation de solutions permettant l'élévation temporaire et contrôlée des privilèges (Microsoft Application Virtualization, solutions tierces comme CyberArk Endpoint Privilege Manager).
2. **Comptes d'administration locale dédiés :** Pour le support technique, utilisation de comptes d'administration locale gérés par LAPS, utilisés uniquement par le personnel autorisé.
3. **Groupes restreints :** Configuration de groupes Active Directory dont l'appartenance accorde des droits administratifs locaux, mais avec surveillance stricte.
4. **Catalogue applicatif :** Mise à disposition d'un catalogue d'applications pré-approuvées installables en self-service sans privilèges.

## Segmentation des Postes Utilisateurs

Tous les postes Tier 2 n'ont pas le même niveau de risque. Une segmentation peut être pertinente :

**Catégories de postes Tier 2 :**

- **Postes VIP :** Postes des dirigeants, du département financier, des RH. Nécessitent une protection renforcée (surveillance accrue, restrictions plus strictes).

- **Postes standards :** Postes de bureautique classiques. Configuration de sécurité standard.
- **Postes de développement :** Nécessitent souvent plus de souplesse (installation d'outils, accès à des ressources variées). Peuvent justifier une isolation dans un sous-réseau spécifique avec surveillance accrue.
- **Kiosques et postes partagés :** Postes utilisés par plusieurs personnes (salles de réunion, espaces communs). Configuration verrouillée, session invité, nettoyage automatique.
- **Postes de prestataires externes :** Isolation maximale, accès restreint au strict nécessaire, surveillance intensive.

### Gestion des Dispositifs Mobiles

Les smartphones et tablettes professionnels constituent une catégorie particulière au sein du Tier 2 :

**Solution MDM (Mobile Device Management) :**

- Déploiement d'une solution MDM (Microsoft Intune, VMware Workspace ONE, etc.)
- Politiques de conformité : chiffrement obligatoire, code PIN, mise à jour système
- Conteneurisation des applications et données professionnelles
- Effacement à distance en cas de perte ou vol
- Blocage de l'appareil si non conforme (jailbreak détecté, etc.)

**Principes de sécurité :**

- Séparation des données personnelles et professionnelles
- Accès email professionnel uniquement via conteneur sécurisé
- Restriction des applications autorisées à accéder aux données professionnelles
- Pas de stockage de documents sensibles hors conteneur professionnel

## Relations entre les Tiers

### Flux Autorisés et Interdits

Le cloisonnement entre les tiers repose sur un contrôle strict des flux d'authentification et d'administration :

### Matrice des Flux d'Administration Autorisés

| De \ Vers | Tier 0 | Tier 1 | Tier 2 |
|---|---|---|---|
| **Tier 0** | ✓ Administration Tier 0 | ✓ Administration Tier 1 possible mais déconseillée | ✗ Interdit |
| **Tier 1** | ✗ Strictement interdit | ✓ Administration Tier 1 | ✗ Interdit (sauf via Jump Server avec Remote Credential Guard) |
| **Tier 2** | ✗ Strictement interdit | ✗ Strictement interdit | ✓ Support Tier 2 |

**Légende :**

- ✓ : Flux autorisé
- ✗ : Flux interdit et bloqué techniquement

**Flux applicatifs (distinct de l'administration) :**

- Tier 2 → Tier 1 : ✓ Accès aux applications métier depuis les postes utilisateurs (HTTP, bases de données, etc.)
- Tier 1 → Tier 0 : ✓ Authentification AD, requêtes DNS, mise à jour via WSUS hébergé sur DC
- Tier 2 → Tier 0 : ✓ Authentification AD, requêtes DNS (flux strictement nécessaires)

## Gestion des Exceptions

Dans les environnements complexes, des exceptions peuvent être nécessaires. Leur gestion doit être rigoureuse :

1. **Documentation :** Toute exception doit être documentée avec justification métier/technique
2. **Validation :** Approbation formelle par l'équipe sécurité et le management
3. **Compensation :** Mise en place de contrôles compensatoires (surveillance accrue, restrictions additionnelles)
4. **Revue régulière :** Réévaluation trimestrielle pour vérifier si l'exception est toujours nécessaire
5. **Plan de sortie :** Définition d'un plan pour éliminer l'exception à terme

## Surveillance et Détection

La surveillance continue des Tiers 1 et 2 est essentielle pour détecter les tentatives de compromission et les violations de cloisonnement :

**Événements critiques à surveiller :**

- Tentatives d'authentification de comptes Tier 0 depuis Tier 1 ou Tier 2
- Tentatives d'authentification de comptes Tier 1 depuis Tier 2
- Modifications des appartenances aux groupes privilégiés
- Créations de comptes de service avec privilèges élevés
- Échecs d'authentification répétés (attaques par force brute)
- Utilisation d'outils d'administration depuis des postes non autorisés
- Activations de comptes break-glass
- Modifications de GPO
- Installation de logiciels non approuvés
- Communications vers des IP ou domaines suspects

**Infrastructure de surveillance :**

- Centralisation des logs dans un SIEM
- Rétention des logs : minimum 1 an pour Tier 0, 6 mois pour Tiers 1 et 2
- Corrélation automatique pour détecter les chaînes d'attaque
- Alertes en temps réel pour les événements critiques
- Tableaux de bord pour la supervision
- Rapports hebdomadaires et mensuels sur les événements de sécurité

## Formation et Sensibilisation

Le facteur humain reste le maillon le plus faible de la chaîne de sécurité. La formation est cruciale pour tous les niveaux :

**Formation des administrateurs :**

- Formation initiale approfondie sur le modèle de tiering et les procédures
- Formation spécifique aux outils (PAW, Jump Servers, LAPS, etc.)
- Sensibilisation aux techniques d'attaque (Pass-the-Hash, Golden Ticket, etc.)

- Recyclage annuel obligatoire
- Simulation d'incidents pour tester la préparation

**Sensibilisation des utilisateurs Tier 2 :**

- Formation sécurité initiale lors de l'intégration
- Campagnes de sensibilisation régulières (email, affiches, intranet)
- Simulations de phishing trimestrielles
- Formation spécifique pour les utilisateurs VIP (ciblés prioritairement par les attaquants)
- Procédures claires pour signaler les incidents suspects

## Conclusion du Chapitre

L'implémentation des Tiers 1 et 2 complète le modèle de tiering en protégeant les valeurs métiers de l'organisation (Tier 1) et en réduisant les risques d'entrée par les postes utilisateurs (Tier 2). Bien que moins critiques que le Tier 0, ces deux niveaux nécessitent une attention soutenue et des contrôles de sécurité appropriés pour assurer l'efficacité globale du cloisonnement.

Le chapitre suivant abordera les aspects de gestion, de maintenance et les bonnes pratiques pour assurer la pérennité et l'efficacité du modèle de tiering dans la durée.

CHAPITRE 5

# Gestion et Maintenance

## Maintien en Condition de Sécurité

L'implémentation initiale du modèle de tiering n'est que le début du voyage. Le maintien de son efficacité dans la durée exige une vigilance constante, des processus rigoureux et une adaptation continue aux évolutions du système d'information et du paysage des menaces. Le Maintien en Condition de Sécurité (MCS) du modèle de tiering représente un investissement continu sans lequel tous les efforts initiaux se dégraderont rapidement.

### Gestion des Changements dans un Environnement Cloisonné

L'un des défis majeurs du maintien du tiering réside dans la gestion des changements. Tout changement dans le système d'information peut potentiellement impacter le cloisonnement et doit donc être évalué soigneusement :

**Processus de gestion des changements adapté au tiering :**

1. **Demande de changement :** Toute demande de changement (ajout de serveur, modification de configuration, déploiement d'application) doit inclure une analyse d'impact sur le tiering.
2. **Évaluation de tier :** Pour chaque nouvelle ressource, détermination du tier approprié selon les critères établis. Question clé : cette ressource peut-elle influencer ou compromettre des ressources d'un tier supérieur ?
3. **Analyse des chemins d'attaque :** Vérification que le changement n'introduit pas de nouveaux chemins d'attaque vers les tiers supérieurs.
4. **Validation sécurité :** Tout changement impactant le Tier 0 doit être validé par l'équipe de sécurité. Les changements Tier 1 et 2 peuvent suivre un processus de validation allégé.
5. **Documentation :** Mise à jour de l'inventaire des ressources et de leur catégorisation. Mise à jour des diagrammes d'architecture si nécessaire.
6. **Mise en œuvre :** Application du changement avec les contrôles de sécurité appropriés au tier concerné.

7. **Vérification post-changement :** Confirmation que les contrôles de cloisonnement restent effectifs après le changement.

### Dérive de Configuration - Le Danger Silencieux

La dérive de configuration représente une menace insidieuse pour le modèle de tiering. Au fil du temps, sans vigilance constante, le cloisonnement se dégrade progressivement :

- Des exceptions temporaires deviennent permanentes
- Des comptes créés pour un besoin ponctuel restent actifs
- Des privilèges accordés "juste pour cette fois" ne sont jamais révoqués
- Des ressources changent de rôle sans être recatégorisées
- Des GPO sont modifiées sans validation appropriée

**Mesures de prévention :**

- Audits de configuration trimestriels
- Détection automatique des écarts (Configuration drift detection)
- Révision systématique des exceptions tous les 3 mois
- Redéploiement périodique des systèmes depuis des images de référence
- Alertes automatiques en cas de modification non autorisée

## Gestion du Cycle de Vie des Comptes

Les comptes privilégiés ont un cycle de vie qui doit être géré rigoureusement du début à la fin :

**Création de compte :**

- Demande formelle avec justification métier
- Validation par le management et l'équipe sécurité pour les comptes Tier 0 et Tier 1
- Attribution d'un tier approprié dès la création
- Nomenclature respectant les standards établis
- Configuration initiale selon les templates de sécurité du tier
- Formation obligatoire de l'utilisateur avant remise des identifiants
- Enregistrement dans l'inventaire des comptes privilégiés

**Maintenance du compte :**

- Révision trimestrielle de tous les comptes privilégiés
- Vérification que le compte est toujours nécessaire
- Confirmation que les privilèges accordés sont toujours appropriés

- Contrôle de la dernière utilisation (comptes dormants à désactiver)
- Rotation des mots de passe selon la politique établie
- Audit des activités réalisées avec le compte

**Désactivation et suppression :**

- Désactivation immédiate lors du départ d'un collaborateur
- Désactivation des comptes inutilisés depuis plus de 90 jours (Tier 2) ou 60 jours (Tiers 0 et 1)
- Période d'attente de 30 jours entre désactivation et suppression définitive
- Archivage des logs d'activité avant suppression
- Retrait de toutes les appartenances aux groupes
- Suppression de l'entrée dans l'inventaire

## Gestion des Mises à Jour et Correctifs

La gestion des mises à jour dans un environnement cloisonné nécessite une approche structurée différenciée par tier :

### Stratégie de Patching par Tier

**Tier 0 - Approche Ultra-Prudente :**

- Jamais de mises à jour automatiques
- Test obligatoire en environnement de laboratoire reproduisant le Tier 0
- Fenêtre de maintenance planifiée mensuelle (sauf urgences sécuritaires)
- Déploiement progressif : un DC de test, puis un DC de production, puis généralisation
- Validation fonctionnelle approfondie entre chaque étape
- Plan de retour arrière testé et documenté
- Sauvegarde complète avant chaque mise à jour
- Délai de 7 à 14 jours après publication Microsoft pour observer les retours de la communauté
- Exception pour les CVE critiques activement exploitées : déploiement accéléré après test minimal

**Tier 1 - Approche Équilibrée :**

- Test en environnement pré-production
- Fenêtre de maintenance mensuelle planifiée
- Déploiement par vagues : serveurs non critiques d'abord, puis critiques

- Possibilité de mises à jour automatiques pour les correctifs mineurs, selon criticité des applications
- Délai de 3 à 7 jours après publication pour les mises à jour non critiques
- Déploiement rapide (24-48h) pour les correctifs critiques

**Tier 2 - Approche Automatisée :**

- Mises à jour automatiques Windows Update activées pour les correctifs critiques et de sécurité
- Déploiement par groupes pilotes puis généralisation
- Reporting automatique des échecs de mise à jour
- Intervention manuelle uniquement en cas de problème signalé

## Audits et Contrôles Réguliers

Des audits réguliers sont essentiels pour vérifier que le modèle de tiering reste effectif et conforme aux objectifs de sécurité :

**Types d'audits à réaliser :**

| Type d'Audit | Fréquence | Objectifs | Outils |
|---|---|---|---|
| **Audit des chemins d'attaque** | Trimestriel | Identifier les chemins d'attaque vers Tier 0 | BloodHound, Purple Knight |
| **Audit des appartenances aux groupes privilégiés** | Mensuel | Vérifier que seuls les comptes autorisés sont membres | Scripts PowerShell AD, reporting SIEM |
| **Audit de configuration PAW/Jump Servers** | Mensuel | Vérifier l'absence de dérive de configuration | Desired State Configuration (DSC), Intune |
| **Audit des authentifications inter-tiers** | Hebdomadaire | Détecter les violations de cloisonnement | Requêtes SIEM, analyse des logs AD |
| **Audit de vulnérabilités** | Mensuel (Tier 0), Trimestriel (Tiers 1-2) | Identifier les vulnérabilités système et applicatives | Scanners de vulnérabilités (Nessus, Qualys, etc.) |
| **Pentest de l'AD** | Annuel | Test en conditions réelles par attaquants simulés | Équipe Red Team interne ou prestataire externe |
| **Audit de conformité** | Annuel | Vérifier la conformité aux politiques et aux référentiels | Audit manuel, checklists de conformité |

**Gestion des constats d'audit :**

1. **Identification :** Documentation précise de chaque non-conformité ou faiblesse identifiée
2. **Classification :** Évaluation de la criticité (critique/haute/moyenne/basse)
3. **Priorisation :** Classement par risque et par facilité de remédiation
4. **Plan d'action :** Définition des actions correctives avec responsables et échéances
5. **Suivi :** Tracking régulier de l'avancement de la remédiation
6. **Vérification :** Confirmation de l'efficacité de la correction
7. **Clôture :** Documentation et archivage une fois résolu

# Gestion des Incidents de Sécurité

Malgré toutes les précautions, des incidents de sécurité peuvent survenir. Une préparation adéquate et des procédures claires sont essentielles pour limiter leur impact.

## Détection Précoce des Incidents

La détection rapide est cruciale pour limiter l'impact d'une compromission. Le modèle de tiering facilite la détection en définissant clairement ce qui est normal et anormal :

**Indicateurs de compromission à surveiller :**

- **Authentifications anormales :**
  - Compte Tier 0 s'authentifiant depuis un système Tier 1 ou Tier 2
  - Authentifications en dehors des heures habituelles
  - Authentifications depuis des localisations géographiques inhabituelles
  - Authentifications multiples simultanées depuis différents systèmes
- **Modifications de configuration suspectes :**
  - Ajout de membre dans un groupe privilégié
  - Création de compte avec privilèges élevés
  - Modification de GPO sensibles
  - Changement de mot de passe de compte privilégié en dehors des plages autorisées
  - Désactivation de mécanismes de sécurité (antivirus, pare-feu, journalisation)
- **Activités malveillantes :**
  - Utilisation d'outils de pentest (Mimikatz, BloodHound, PsExec)
  - Tentatives de dump de la base NTDS.dit
  - Énumération AD intensive
  - Tentatives d'exploitation de vulnérabilités connues
  - Communications vers des serveurs de C2 (Command & Control) connus

### Scénarios d'Incidents Critiques

**Scénario 1 : Compromission suspectée d'un compte Tier 0**

Détection : Authentification d'un compte Domain Admin depuis un poste Tier 2 non autorisé

Actions immédiates :

1. Désactiver le compte compromis

2. Réinitialiser le mot de passe du compte
3. Révoquer tous les tickets Kerberos du compte (via krbtgt reset si nécessaire)
4. Analyser les actions réalisées avec le compte
5. Rechercher des portes dérobées créées (comptes cachés, scheduled tasks)
6. Déconnecter le système source du réseau pour analyse forensique

**Scénario 2 : Détection d'outils d'attaque sur un PAW Tier 0**

Détection : EDR alerte sur la présence de Mimikatz sur un PAW

Actions immédiates :

1. Isoler immédiatement le PAW du réseau
2. Désactiver tous les comptes s'étant authentifiés depuis ce PAW
3. Changement d'urgence du mot de passe krbtgt (Golden Ticket mitigation)
4. Analyse forensique du PAW
5. Vérification de tous les autres PAW
6. Revue des logs pour identifier l'origine de la compromission

**Scénario 3 : Ransomware sur le Tier 2 tentant de se propager**

Détection : EDR détecte un ransomware sur plusieurs postes Tier 2

Actions immédiates :

1. Isolation des postes infectés
2. Blocage réseau des hashes/IOC du ransomware
3. Vérification que le ransomware n'a PAS atteint Tier 1 ou Tier 0
4. Restauration depuis sauvegardes saines
5. Analyse de la méthode d'infection initiale
6. Correction de la faille exploitée

## Procédures de Réponse aux Incidents

Une procédure de réponse aux incidents adaptée au modèle de tiering doit être documentée et testée régulièrement :

**Phases de réponse :**

1. **Préparation :**
    - Équipe de réponse aux incidents constituée et formée

- Procédures documentées et accessibles
- Kits d'outils forensiques prêts
- Contacts d'urgence (management, équipes techniques, prestataires, autorités)
- Sauvegardes testées et restaurables

2. **Détection et Analyse :**
   - Détection de l'incident via SIEM, EDR, ou signalement utilisateur
   - Classification de l'incident (tier impacté, type d'attaque, sévérité)
   - Activation de l'équipe de réponse appropriée
   - Analyse initiale pour comprendre la portée
3. **Confinement :**
   - Isolation des systèmes compromis
   - Blocage de la propagation (réseau, identifiants, malwares)
   - Préservation des preuves pour analyse forensique
   - Communication aux parties prenantes selon protocole établi
4. **Éradication :**
   - Suppression de la menace (malwares, accès non autorisés, comptes pirates)
   - Correction des vulnérabilités exploitées
   - Changement de tous les identifiants potentiellement compromis
   - Vérification de l'absence de persistance
5. **Récupération :**
   - Restauration des systèmes depuis sauvegardes saines ou rebuild complet
   - Validation de l'intégrité avant remise en service
   - Surveillance renforcée post-incident
   - Retour progressif à la normale
6. **Retour d'Expérience :**
   - Documentation complète de l'incident
   - Analyse des causes profondes
   - Identification des améliorations nécessaires
   - Mise à jour des procédures
   - Formation des équipes sur les leçons apprises

## Plan de Continuité et de Reprise après Sinistre

Le modèle de tiering doit être pris en compte dans les plans de continuité et de reprise :

**Considérations spécifiques au tiering :**

- **Priorité de restauration :** Tier 0 en priorité absolue, puis Tier 1, puis Tier 2
- **Sites de secours :** Le site de backup doit respecter le même niveau de cloisonnement
- **Procédures de restauration :** Restauration par tier pour maintenir le cloisonnement
- **Comptes de secours :** Les comptes break-glass doivent être fonctionnels même en cas de sinistre majeur
- **Documentation hors ligne :** Procédures accessibles même si l'AD est indisponible

# Évolution et Amélioration Continue

Le modèle de tiering n'est pas statique. Il doit évoluer pour s'adapter aux changements organisationnels, technologiques et aux nouvelles menaces.

## Veille Technologique et Sécuritaire

Une veille active est indispensable pour maintenir la pertinence du modèle :

**Domaines de veille :**

- **Nouvelles menaces contre Active Directory :** Nouvelles techniques d'attaque, outils, vulnérabilités découvertes
- **Évolutions technologiques :** Nouvelles versions de Windows Server, nouvelles fonctionnalités AD
- **Bonnes pratiques :** Publications Microsoft, recommandations de l'industrie, retours d'expérience d'autres organisations
- **Outils de sécurité :** Nouveaux outils de détection, d'analyse, de durcissement
- **Évolutions réglementaires :** Nouvelles exigences de conformité impactant l'AD

**Sources de veille recommandées :**

- Microsoft Security Response Center (MSRC)
- Microsoft Security Blog
- National Vulnerability Database (NVD)
- CERT/CSIRT nationaux
- Conférences de sécurité (Black Hat, DEF CON, RSA Conference)
- Communautés spécialisées (Reddit r/sysadmin, r/netsec, forums Microsoft)
- Prestataires de Threat Intelligence

## Adaptations aux Nouvelles Technologies

L'intégration de nouvelles technologies peut nécessiter des adaptations du modèle :

**Cloud Hybride et Azure AD :**

- Catégorisation des serveurs de synchronisation (Azure AD Connect) : généralement Tier 0
- Gestion des identités hybrides : comptes cloud-only vs synchronisés
- Conditional Access comme extension du cloisonnement
- Privileged Identity Management (PIM) pour l'élévation juste-à-temps
- Protection des comptes admin cloud avec MFA et accès conditionnel

**Conteneurisation et Orchestration :**

- Catégorisation des plateformes d'orchestration (Kubernetes, OpenShift)
- Gestion des identités dans les environnements conteneurisés
- Intégration AD avec les registries de conteneurs

**Infrastructure as Code (IaC) :**

- Protection des repositories contenant l'IaC (Tier 0 si déployant sur Tier 0)
- Gestion des secrets dans les pipelines CI/CD
- Validation de sécurité dans les processus de déploiement automatisé

**Zéro Trust et Microsegmentation :**

- Le tiering comme fondation d'une architecture Zero Trust
- Microsegmentation réseau basée sur les tiers
- Vérification continue de l'identité et du contexte

## Indicateurs de Performance et de Maturité

Pour piloter l'amélioration continue, des indicateurs doivent être définis et suivis :

**Indicateurs de sécurité (KSI - Key Security Indicators) :**

| Indicateur | Méthode de Mesure | Objectif | Fréquence |
|---|---|---|---|
| Nombre de chemins d'attaque critiques vers Tier 0 | BloodHound / analyse AD | 0 (zéro) | Mensuel |
| Nombre de violations de cloisonnement détectées | Alertes SIEM | 0 (zéro) | Continu |
| Pourcentage de systèmes à jour | Reporting patches | > 95% | Hebdomadaire |
| Temps moyen de détection d'incident | SOC metrics | < 1 heure | Mensuel |
| Temps moyen de réponse à incident | SOC metrics | < 4 heures | Mensuel |
| Nombre de comptes privilégiés actifs | Requêtes AD | Minimiser | Mensuel |
| Pourcentage de conformité aux baselines de sécurité | Scans de conformité | > 98% | Mensuel |

**Modèle de maturité du tiering :**

1. **Niveau 1 - Initial :** Aucun cloisonnement, administration ad-hoc, privilèges non contrôlés
2. **Niveau 2 - Basique :** Catégorisation des ressources effectuée, séparation partielle des comptes admin
3. **Niveau 3 - Défini :** Modèle de tiering documenté et communiqué, PAW déployés pour Tier 0, restrictions techniques partielles
4. **Niveau 4 - Géré :** Cloisonnement techniquement appliqué, détection automatisée des violations, processus de gestion établis
5. **Niveau 5 - Optimisé :** Amélioration continue, automation poussée, métriques suivies, adaptation proactive aux menaces

# Automatisation et Orchestration

L'automatisation est un levier puissant pour maintenir la cohérence du modèle de tiering et réduire le risque d'erreur humaine. Une stratégie d'automatisation bien pensée permet non seulement de gagner en efficacité opérationnelle mais également d'améliorer la sécurité en garantissant l'application uniforme des politiques.

## Automatisation de la Gestion des Comptes

La gestion manuelle des comptes privilégiés est source d'erreurs et d'oublis. L'automatisation apporte cohérence et traçabilité :

**Provisionnement automatisé :**

- **Workflow de demande :** Interface web ou système de ticketing pour les demandes de compte privilégié avec validation automatique selon le niveau de tier demandé
- **Création standardisée :** Scripts PowerShell ou Terraform appliquant systématiquement les bonnes configurations selon le tier
- **Nomenclature automatique :** Génération automatique des noms de compte selon les conventions établies
- **Attribution automatique de groupes :** Appartenance aux groupes déterminée automatiquement selon le rôle et le tier
- **Notification :** Envoi automatique des informations de compte à l'utilisateur et aux responsables

**Gestion du cycle de vie :**

- **Désactivation automatique :** Scripts planifiés détectant les comptes inactifs depuis X jours et les désactivant automatiquement avec notification
- **Révision périodique automatisée :** Génération de rapports listant les comptes nécessitant une révision avec envoi aux managers pour validation
- **Rotation des mots de passe :** Changement automatique des mots de passe de service accounts via gMSA ou solutions PAM
- **Expiration temporaire :** Comptes temporaires avec date d'expiration automatique pré-configurée

## Infrastructure as Code pour le Tiering

L'approche Infrastructure as Code (IaC) permet de documenter et de versionner la configuration du tiering tout en facilitant son déploiement reproductible :

**Configuration des PAW via DSC ou Intune :**

- Définition de l'état désiré des PAW dans des fichiers de configuration versionnés
- Application automatique et continue de la configuration
- Détection et correction automatique des dérives de configuration
- Rapports de conformité automatiques

**Déploiement de serveurs par tier :**

- Templates de déploiement (ARM, Terraform, Ansible) par tier avec les configurations de sécurité appropriées
- Application automatique des GPO, des règles de pare-feu, des configurations réseau selon le tier
- Tests automatisés de conformité post-déploiement
- Documentation auto-générée à partir du code d'infrastructure

**Gestion des GPO et politiques :**

- Versionnement des GPO dans Git
- Processus de validation (peer review) avant application
- Déploiement par étapes : test, pré-production, production
- Rollback automatique en cas de détection de problème

### Pipeline CI/CD pour l'Infrastructure de Tiering

**Étapes d'un pipeline typique :**

1. **Code :** Développeur/administrateur modifie une configuration (GPO, DSC, script)
2. **Commit :** Changement committé dans Git avec description
3. **Validation automatique :** Tests de syntaxe, linting, vérification de conformité aux standards
4. **Revue :** Pull request avec approbation requise d'un pair (obligatoire pour Tier 0)
5. **Test en lab :** Déploiement automatique dans un environnement de test isolé
6. **Tests fonctionnels :** Batterie de tests automatisés vérifiant que la configuration ne casse rien
7. **Tests de sécurité :** Scans de sécurité, vérification qu'aucun chemin d'attaque n'est introduit
8. **Approbation déploiement :** Validation manuelle finale pour Tier 0, automatique pour Tier 2
9. **Déploiement production :** Application progressive de la configuration
10. **Surveillance post-déploiement :** Monitoring renforcé pendant 24-48h

## Automatisation de la Surveillance et de la Détection

La détection automatisée des anomalies et des violations du tiering est essentielle pour réagir rapidement :

**Règles de détection SIEM :**

- **Authentifications inter-tiers :** Alerte immédiate si un compte Tier 0 s'authentifie sur un système Tier 1 ou 2
- **Modifications de groupes privilégiés :** Alerte sur tout ajout/retrait dans Domain Admins, Enterprise Admins, etc.
- **Création de compte privilégié :** Notification sur création de tout nouveau compte avec privilèges élevés
- **Activité suspecte :** Détection de patterns d'attaque connus (Pass-the-Hash, Golden Ticket, etc.)
- **Échecs d'authentification répétés :** Tentatives de bruteforce sur comptes privilégiés

**Scripts de surveillance continue :**

- Scripts PowerShell planifiés quotidiennement pour auditer la configuration AD
- Vérification automatique de la conformité aux baselines de sécurité
- Détection de nouveaux chemins d'attaque via BloodHound en mode automatisé
- Inventaire automatique et comparaison avec l'inventaire de référence
- Génération automatique de rapports de conformité hebdomadaires

## Orchestration de la Réponse aux Incidents

L'orchestration automatisée peut accélérer considérablement la réponse aux incidents critiques :

**SOAR (Security Orchestration, Automation and Response) :**

- **Playbooks automatisés :** Séquences d'actions pré-définies déclenchées automatiquement selon le type d'incident
- **Enrichissement automatique :** Collecte automatique d'informations contextuelles sur l'incident (historique du compte, systèmes impactés, etc.)
- **Confinement automatisé :** Désactivation de compte, isolation réseau, blocage d'IP selon le niveau de criticité
- **Escalade intelligente :** Notification des bonnes personnes selon le type et la sévérité de l'incident
- **Documentation automatique :** Journalisation de toutes les actions de réponse pour analyse post-incident

**Exemple de playbook automatisé - Compte Tier 0 compromis :**

1. Détection : SIEM détecte authentification suspecte d'un compte Domain Admin

2. Enrichissement : Collecte automatique de l'historique des authentifications, actions récentes du compte, systèmes accédés
3. Évaluation : Scoring automatique de la criticité selon des critères prédéfinis
4. Confinement : Si criticité élevée, désactivation automatique immédiate du compte
5. Notification : Alerte SMS/appel au responsable sécurité et au manager IT
6. Investigation : Création automatique d'un ticket avec toutes les informations collectées
7. Collecte forensique : Lancement automatique de scripts de collecte sur les systèmes impactés
8. Documentation : Génération d'un rapport initial en quelques secondes

# Aspects Légaux et Réglementaires

Le modèle de tiering s'inscrit dans un contexte légal et réglementaire qui peut à la fois motiver sa mise en œuvre et en contraindre certains aspects.

## Conformité RGPD et Protection des Données

Le Règlement Général sur la Protection des Données (RGPD) impose des obligations qui trouvent des réponses dans le tiering :

**Obligations RGPD adressées par le tiering :**

- **Sécurité des données personnelles (Art. 32) :** Le cloisonnement et la protection renforcée du Tier 0 contribuent directement à la sécurité des systèmes traitant des données personnelles
- **Limitation d'accès :** Le principe du moindre privilège appliqué dans le tiering limite l'accès aux données personnelles aux seules personnes autorisées
- **Traçabilité :** La journalisation renforcée permise par le tiering facilite la démonstration de la conformité et l'investigation en cas d'incident
- **Notification de violation :** La détection automatisée facilite le respect du délai de 72h pour notifier une violation
- **Privacy by design :** L'intégration de la sécurité dès la conception des systèmes via le tiering répond à cette exigence

**Documentation à maintenir pour la conformité :**

- Registre des traitements incluant les mesures de sécurité (mention du tiering)
- Analyse d'impact (PIA) pour les traitements à risque élevé
- Documentation des mesures techniques et organisationnelles

- Logs de tous les accès aux données personnelles sensibles
- Procédures de réponse aux violations de données

## Conformité Sectorielle

Selon le secteur d'activité, des réglementations spécifiques peuvent s'appliquer :

**Secteur Financier :**

- **Directive NIS2 :** Entités essentielles et importantes doivent mettre en œuvre des mesures de cybersécurité appropriées (le tiering en fait partie)
- **DORA (Digital Operational Resilience Act) :** Exigences de résilience opérationnelle numérique pour les entités financières de l'UE
- **PCI-DSS :** Pour le traitement de données de cartes bancaires, exigences de segmentation et de contrôle d'accès alignées avec le tiering
- **ACPR en France :** Attentes fortes sur la sécurité de l'infrastructure informatique

**Secteur Santé :**

- **Certification HDS (France) :** Exigences de sécurité pour l'hébergement de données de santé
- **HIPAA (États-Unis) :** Règles de sécurité et de confidentialité pour les données de santé
- **Référentiel de sécurité des systèmes d'information hospitaliers**

**Opérateurs d'Importance Vitale (OIV) :**

- Obligations spécifiques de sécurité des systèmes d'information d'importance vitale (SIIV)
- Contrôles périodiques de sécurité obligatoires
- Déclaration des incidents de sécurité significatifs

### Responsabilité en Cas de Compromission

L'absence de mise en œuvre de mesures de sécurité reconnues comme l'état de l'art (dont le tiering fait partie pour Active Directory) peut engager la responsabilité de l'organisation et de ses dirigeants :

- **Sanctions CNIL :** Jusqu'à 4% du chiffre d'affaires annuel mondial ou 20M€ en cas de non-conformité RGPD
- **Responsabilité civile :** Actions en justice de clients, partenaires, ou employés victimes de la compromission
- **Responsabilité pénale :** Dans certains cas graves, engagement de la responsabilité pénale des dirigeants

- **Sanctions sectorielles :** Retraits d'agrément, interdictions d'exercer selon le secteur

La mise en œuvre documentée d'un modèle de tiering constitue une preuve de diligence raisonnable en matière de sécurité.

### Obligations de Notification et de Transparence

En cas d'incident de sécurité, diverses obligations de notification s'appliquent :

**Notification aux autorités :**

- **CNIL (RGPD) :** Notification sous 72h en cas de violation de données personnelles présentant un risque pour les personnes
- **Autorité sectorielle (NIS, OIV) :** Notification des incidents significatifs aux autorités de régulation
- **Notification aux personnes concernées :** Si le risque pour les personnes est élevé, notification directe obligatoire

**Le tiering facilite la conformité à ces obligations :**

- Détection plus rapide grâce à la surveillance renforcée
- Évaluation facilitée de la portée de l'incident (quels tiers sont impactés ?)
- Documentation des mesures de sécurité en place (atténuant potentiellement les sanctions)
- Limitation de l'impact (confinement par tier)

## Études de Cas et Retours d'Expérience

L'analyse de cas réels d'implémentation et d'incidents permet de tirer des enseignements précieux pour votre propre démarche.

### Cas 1 : Grande Entreprise Industrielle (12 000 utilisateurs)

**Contexte :**

- Groupe industriel international avec 30 sites de production
- Environnement AD complexe avec multiples domaines et forêts
- Récente compromission via ransomware ayant paralysé la production pendant 5 jours
- Coût de l'incident : 15M€ (arrêt production + remédiation + image)

**Démarche d'implémentation :**

1. **Phase 1 (3 mois) :** Audit complet de l'AD avec BloodHound, identification de 147 chemins d'attaque critiques vers les Domain Admins
2. **Phase 2 (4 mois) :** Catégorisation de toutes les ressources (2 500 serveurs, 350 applications métier) et définition claire du Tier 0
3. **Phase 3 (6 mois) :** Déploiement du Tier 0 : création de comptes dédiés, déploiement de 15 PAW, durcissement de 24 DC, mise en place LAPS
4. **Phase 4 (8 mois) :** Déploiement Tier 1 avec Jump Servers dans chaque site majeur
5. **Phase 5 (6 mois) :** Tier 2 et finalisation avec MDM généralisé
6. **Durée totale :** 27 mois du lancement à la finalisation

**Défis rencontrés :**

- **Résistance culturelle :** Forte opposition initiale des équipes IT habituées à travailler avec des comptes admin tout-puissants. Résolu par formation intensive et accompagnement personnalisé.
- **Applications legacy :** 12 applications critiques nécessitant des privilèges élevés. Solution : conteneurisation dans des environnements dédiés Tier 1 isolés.
- **Multi-sites :** Complexité de déployer et maintenir la cohérence sur 30 sites. Solution : équipes locales formées + automatisation poussée + audits trimestriels.
- **Coûts :** Dépassement budgétaire de 30% par rapport au plan initial (budget final : 1,8M€ vs 1,4M€ prévu)

**Résultats après 18 mois d'opération :**

- Chemins d'attaque critiques vers Tier 0 : 0 (versus 147 initialement)
- Détection d'une tentative de compromission en 15 minutes vs plusieurs jours avant
- Temps de remédiation d'incident divisé par 4
- Conformité réglementaire validée par audit externe
- ROI positif dès la 2ème année (coûts évités > investissement)

## Cas 2 : PME du Secteur Tertiaire (200 utilisateurs)

**Contexte :**

- Entreprise de services avec 200 employés répartis sur 3 sites
- Budget IT limité, équipe IT de 3 personnes
- Environnement simple : 1 forêt, 1 domaine, 4 DC
- Motivation : exigence client pour certification ISO 27001

**Approche pragmatique adoptée :**

- **Simplification :** Modèle à 2 tiers uniquement (Tier 0 strict + "reste")
- **Priorisation :** Focus sur la protection du Tier 0, approche allégée pour le reste
- **Outils gratuits :** LAPS, GPO, scripts PowerShell custom, pas de SIEM commercial (utilisation de Graylog open source)
- **Pas de PAW dédiés :** Utilisation de Jump Server unique avec RDP restrictive
- **Formation interne :** Auto-formation via documentation Microsoft, pas de consultant externe

**Budget et ressources :**

- Investissement initial : 45K€ (principalement matériel : Jump Server, serveurs logs)
- Coût récurrent : 15K€/an (outils, audit annuel externe)
- Temps de déploiement : 6 mois à temps partiel

**Résultats :**

- Certification ISO 27001 obtenue
- Gain de crédibilité auprès des clients
- Posture de sécurité significativement améliorée avec moyens limités
- Démonstration qu'un tiering adapté est possible même pour les PME

## Cas 3 : Incident Majeur Évité Grâce au Tiering

**Scénario :**

Grande institution financière (25 000 utilisateurs) avec tiering mature en place depuis 3 ans.

**Déroulé de l'attaque :**

1. **J-0, 14h30 :** Email de phishing ciblé sur un directeur financier. Clic sur lien malveillant.
2. **J-0, 14h35 :** Malware s'installe sur le poste Tier 2 du directeur. EDR détecte et alerte mais malware polymorphe non encore bloqué.
3. **J-0, 15h00 :** Attaquant établit Command & Control, commence reconnaissance réseau.
4. **J-0, 16h30 :** Attaquant tente élévation de privilèges locale, réussit à obtenir admin local (malgré restriction UAC).
5. **J-0, 17h00 :** Tentative de mouvement latéral vers un serveur Tier 1 de gestion financière. **BLOQUÉ** : pas de chemin d'administration depuis Tier 2 vers Tier 1.

6. **J-0, 17h15 :** Tentative de dump des credentials en mémoire. Récupération de hash du compte utilisateur standard du directeur uniquement (aucun compte admin ne s'était authentifié sur ce poste Tier 2).
7. **J-0, 18h00 :** Tentative Pass-the-Hash avec le compte standard vers serveurs. **BLOQUÉ** : compte standard n'a pas d'accès admin aux serveurs.
8. **J-0, 18h30 :** SIEM corrèle les alertes EDR + tentatives de mouvement latéral. Génération d'alerte haute criticité.
9. **J-0, 19h00 :** SOC analyse l'alerte, confirme la compromission, lance la procédure de réponse à incident.
10. **J-0, 19h30 :** Isolation du poste compromis, désactivation du compte utilisateur, reset du mot de passe.
11. **J+1 :** Analyse forensique, éradication du malware, remise en service du poste reconfiguré à partir d'une image saine.

**Analyse post-incident :**

- **Impact réel :** Compromission d'un poste Tier 2 uniquement. Aucune donnée métier sensible exfiltrée. Coût total : ~50K€ (investigation + remédiation).
- **Impact potentiel sans tiering :** L'attaquant aurait pu compromettre les serveurs métier (Tier 1), potentiellement l'AD (Tier 0), exfiltrer massivement des données financières sensibles. Coût estimé : 10M€ - 50M€ (incident majeur avec arrêt d'activité, sanctions réglementaires, atteinte à la réputation).
- **Facteurs de succès :**
  - Cloisonnement strict empêchant le mouvement latéral
  - Absence de credentials privilégiés sur le poste compromis
  - Détection automatisée via SIEM des comportements anormaux
  - Procédures de réponse claires et testées

**Conclusion du RSSI :** "Sans le modèle de tiering, cette attaque aurait pu paralyser notre institution pendant des semaines. Le tiering nous a sauvés. L'investissement de 2,5M€ sur 3 ans a permis d'éviter une catastrophe à plusieurs dizaines de millions."

## Considérations Organisationnelles et Humaines

Le succès du modèle de tiering dépend autant des aspects humains et organisationnels que des aspects techniques.

## Gouvernance et Responsabilités

Une structure de gouvernance claire est essentielle :

**Comité de pilotage tiering :**

- Composition : RSSI, DSI, représentants métiers clés, responsables d'exploitation
- Missions : orientation stratégique, arbitrage sur les exceptions, validation du budget, suivi des indicateurs
- Fréquence : trimestrielle, ou mensuelle en phase de déploiement

**Rôles et responsabilités :**

- **Propriétaire du modèle de tiering :** Responsable global de la sécurité du modèle, généralement le RSSI ou équivalent
- **Gestionnaire Tier 0 :** Responsable opérationnel du Tier 0, gestion au quotidien
- **Gestionnaire Tier 1 :** Responsable de la sécurité et de la gestion du Tier 1
- **Gestionnaire Tier 2 :** Responsable des postes de travail et de leur sécurité
- **Administrateurs par tier :** Équipes techniques opérant sur chaque tier
- **Équipe sécurité :** Surveillance, détection, réponse aux incidents
- **Auditeurs internes :** Vérification de la conformité et de l'efficacité

## Gestion du Changement Culturel

L'implémentation du tiering représente un changement culturel majeur pour les équipes IT :

**Résistances au changement attendues :**

- **"C'est trop contraignant" :** Les administrateurs habitués à utiliser des comptes hautement privilégiés pour tout peuvent percevoir le tiering comme un frein
- **"On n'a jamais eu de problème avant" :** Sous-estimation des risques par manque de visibilité sur les menaces réelles
- **"Ça va ralentir notre travail" :** Perception que la sécurité s'oppose à l'efficacité opérationnelle
- **"C'est trop complexe" :** Difficulté à comprendre tous les aspects du modèle

**Stratégies pour faciliter l'adhésion :**

1. **Communication transparente :** Expliquer le pourquoi (risques réels, incidents vécus par d'autres organisations) avant le comment
2. **Implication précoce :** Impliquer les équipes techniques dès la phase de conception pour recueillir leur feedback

3. **Approche progressive :** Démarrer par le Tier 0, montrer les bénéfices, puis étendre
4. **Formation adaptée :** Formation pratique centrée sur les nouveaux workflows, pas juste de la théorie
5. **Support renforcé :** Hotline, documentation accessible, période d'accompagnement
6. **Valorisation :** Reconnaissance et valorisation des équipes participant activement au déploiement
7. **Quick wins :** Identifier et communiquer sur des bénéfices rapides et visibles

## Formation Continue

Un programme de formation structuré est indispensable à tous les niveaux :

**Programme de formation administrateurs :**

- **Formation initiale (2-3 jours) :**
  - Principes du tiering et justification
  - Architecture détaillée de l'implémentation dans l'organisation
  - Procédures opérationnelles quotidiennes
  - Utilisation des PAW / Jump Servers
  - Gestion des comptes privilégiés
  - Réponse aux incidents
  - Travaux pratiques en environnement de lab
- **Recyclage annuel (1 journée) :**
  - Rappels des fondamentaux
  - Nouveautés et évolutions du modèle
  - Retours d'expérience de l'année
  - Nouvelles menaces et contre-mesures
- **Formation spécialisée (selon rôle) :**
  - Formation approfondie pour les administrateurs Tier 0
  - Formation forensique pour l'équipe de réponse aux incidents
  - Formation audit pour les auditeurs

**Sensibilisation utilisateurs finaux :**

- Module e-learning obligatoire lors de l'onboarding
- Campagnes trimestrielles sur des thèmes spécifiques (phishing, mots de passe, ingénierie sociale)
- Communications ciblées lors d'incidents médiatisés dans le secteur

- Procédure claire pour signaler un incident suspect

# Aspects Économiques

La mise en œuvre et le maintien d'un modèle de tiering représentent un investissement qu'il convient d'évaluer et de justifier.

## Coûts d'Implémentation

Les coûts directs et indirects à anticiper :

**Coûts initiaux :**

- **Matériel :** PAW, Jump Servers, serveurs additionnels pour séparer les tiers (100K€ - 500K€ selon taille)
- **Licences logicielles :** Outils de surveillance, EDR, SIEM (50K€ - 300K€/an)
- **Prestations :** Audit initial, accompagnement au déploiement (100K€ - 500K€)
- **Formation :** Formation des équipes (20K€ - 100K€)

**Coûts récurrents :**

- **Personnel :** Temps additionnel de gestion (estimation 0.5 à 2 ETP selon taille)
- **Licences :** Renouvellement annuel des outils
- **Audits :** Audits réguliers de conformité et pentests (30K€ - 150K€/an)
- **Formation :** Formation continue (10K€ - 50K€/an)

## Retour sur Investissement

Le ROI du tiering se mesure principalement par les coûts évités :

**Coûts d'une compromission majeure de l'AD :**

- **Remédiation technique :** Rebuild complet de l'AD : 500K€ - 5M€
- **Interruption d'activité :** Plusieurs jours à plusieurs semaines : 1M€ - 50M€ selon secteur
- **Perte de données :** Données non récupérables ou exfiltrées : variable
- **Atteinte à la réputation :** Impact long terme difficile à quantifier : potentiellement > 10M€
- **Sanctions réglementaires :** RGPD, sectorielles : jusqu'à 4% du CA
- **Actions en justice :** Clients, partenaires, actionnaires : très variable

**Calcul simplifié du ROI :**

ROI = (Coût évité d'une compromission × Probabilité de compromission) - Coût du tiering

Exemple pour une organisation moyenne :

- Coût estimé d'une compromission totale AD : 5M€
- Probabilité sur 5 ans sans tiering : 30%
- Probabilité sur 5 ans avec tiering : 5%
- Coût du tiering sur 5 ans : 800K€
- ROI = (5M€ × 25%) - 800K€ = **450K€ de gain net**

Au-delà de ces calculs, les bénéfices intangibles incluent :

- Confiance accrue des clients et partenaires
- Facilitation de la conformité réglementaire
- Amélioration de la posture de sécurité globale
- Réduction de la prime d'assurance cyber

# Cas Particuliers et Environnements Spécifiques

## PME et Petites Structures

Le modèle de tiering peut sembler dimensionné pour les grandes entreprises, mais il est adaptable aux PME :

**Adaptations pour PME :**

- **Simplification :** Fusion Tier 1 et Tier 2 en un seul tier "non-Tier 0" dans les très petites structures
- **Mutualisation :** Un Jump Server unique servant à la fois Tier 0 et Tier 1 (avec restrictions strictes)
- **Approche cloud :** Utilisation de services cloud managés pour réduire la complexité (Azure AD, Intune)
- **Priorisation :** Focus sur la protection du Tier 0, approche allégée pour les autres tiers
- **Outils gratuits :** Utilisation d'outils open source ou gratuits (LAPS, Windows Defender, audit scripts PowerShell)

### Configuration Minimale Viable pour PME

Pour une PME de 50-200 personnes :

- 2 contrôleurs de domaine (Tier 0)
- Comptes admin dédiés pour les 2-3 administrateurs
- 1 Jump Server pour l'administration
- LAPS sur tous les postes et serveurs
- Groupe Protected Users pour les comptes admin
- GPO de durcissement basiques
- Journalisation centralisée minimaliste (Graylog, ELK gratuit)
- Audit trimestriel manuel avec scripts PowerShell

Investissement : 50K€ - 100K€ initial, 20K€ - 40K€/an récurrent

## Environnements Multi-Sites et Internationaux

Les grandes organisations multi-sites doivent adapter le modèle à leur géographie :

**Considérations :**

- **Contrôleurs de domaine distribués :** DC Tier 0 dans chaque région principale
- **RODC pour sites distants :** Utilisation de Read-Only Domain Controllers dans les sites à sécurité physique limitée
- **Réplication AD :** Optimisation de la topologie de réplication entre sites
- **Équipes locales :** Formation et habilitation d'administrateurs locaux avec délégations géographiques
- **Fuseaux horaires :** Organisation de la couverture H24 pour la surveillance et la réponse aux incidents
- **Réglementations locales :** Conformité avec les réglementations de chaque pays (localisation des données, etc.)

## Secteurs Régulés

Certains secteurs présentent des contraintes spécifiques :

**Santé (hôpitaux, cliniques) :**

- Disponibilité 24/7 critique : procédures d'urgence documentées
- Systèmes médicaux souvent obsolètes : isolation renforcée
- Données de santé hautement sensibles : chiffrement renforcé

- Conformité HDS (Hébergement de Données de Santé) en France

**Finance (banques, assurances) :**

- Exigences réglementaires strictes (PCI-DSS, DORA)
- Ségrégation stricte front-office / back-office
- Audits externes fréquents
- Sécurité maximale pour les systèmes de paiement

**Industrie (OIV, SEVESO) :**

- Systèmes industriels critiques (SCADA) en Tier 1
- Air gap entre IT et OT (Operational Technology) souvent requis
- Disponibilité critique pour la production
- Conformité IEC 62443 pour cybersécurité industrielle

# Conclusion Générale

Le modèle de tiering représente une approche structurée, éprouvée et efficace pour sécuriser les environnements Active Directory contre les menaces contemporaines. Sa mise en œuvre, bien qu'exigeante, offre des bénéfices substantiels en termes de réduction des risques et de conformité réglementaire.

**Points clés à retenir :**

1. **Le Tier 0 est sacré :** Sa protection absolue est non négociable. Tout compromis sur le Tier 0 anéantit l'ensemble du modèle.
2. **Le cloisonnement est multidimensionnel :** Il ne repose pas uniquement sur la segmentation réseau mais sur une combinaison de contrôles techniques, organisationnels et humains.
3. **La démarche est itérative :** L'implémentation parfaite immédiate est illusoire. Progresser par itérations en priorisant le Tier 0 est l'approche pragmatique.
4. **La maintenance est continue :** Le tiering n'est pas un projet ponctuel mais un état opérationnel permanent nécessitant vigilance et adaptation continues.
5. **L'humain est central :** La technologie seule ne suffit pas. Formation, sensibilisation et adhésion des équipes sont déterminantes.
6. **L'adaptation est nécessaire :** Chaque organisation doit adapter le modèle à son contexte spécifique, sa taille, son secteur d'activité.
7. **La mesure est essentielle :** Des indicateurs clairs permettent de piloter l'amélioration et de démontrer la valeur du modèle.

## Prochaines Étapes pour Votre Organisation

Si vous envisagez de déployer ou d'améliorer un modèle de tiering :

1. **Évaluation initiale :** Réalisez un audit de votre environnement AD actuel pour identifier les risques et les chemins d'attaque existants
2. **Obtention du support :** Présentez le projet à la direction avec une analyse risques/bénéfices adaptée à votre contexte
3. **Définition du périmètre :** Identifiez clairement quelles ressources constituent votre Tier 0
4. **Plan de déploiement :** Établissez une feuille de route réaliste et progressive
5. **Pilote :** Démarrez par un périmètre restreint pour valider l'approche
6. **Déploiement :** Généralisation progressive en commençant par le Tier 0
7. **Opérationnalisation :** Mise en place des processus de maintien en condition de sécurité
8. **Amélioration continue :** Mesure, analyse, ajustement régulier du modèle

## Pour Aller Plus Loin

**Ressources complémentaires :**

- Documentation Microsoft sur le modèle de tiering et l'Enterprise Access Model
- Guides de durcissement Active Directory (CIS Benchmarks, STIGs)
- Outils d'analyse : BloodHound, PingCastle, Purple Knight
- Communautés de pratique : forums, groupes d'utilisateurs, conférences
- Formation certifiante : GIAC GCWN, Microsoft Certified: Security Operations Analyst Associate

**Le mot de la fin :**

La sécurité de votre Active Directory n'est pas un luxe mais une nécessité dans le contexte actuel des menaces cyber. Le modèle de tiering, s'il est correctement implémenté et maintenu, transforme votre annuaire d'un point de faiblesse critique en un bastion résilient. L'investissement en vaut largement la chandelle au regard des enjeux.

La route est longue, parfois difficile, mais le jeu en vaut la chandelle. La sécurité de votre organisation et la confiance de vos parties prenantes en dépendent.

Bonne mise en œuvre du modèle de tiering !

ANNEXE A

# Checklist — 69 Points de Contrôle

> Comment utiliser cette checklist ?Cette checklist vous accompagne tout au long de votre projet de déploiement du modèle de tiering. Cochez les éléments au fur et à mesure de leur réalisation pour suivre votre progression. Les éléments sont organisés par phase chronologique et par priorité.

## Phase 1 : Préparation et Audit Initial (Mois 1-3)

- **Obtenir le soutien et l'engagement de la direction générale** — Présenter le projet, les risques adressés, le budget et le planning au CODIR/COMEX
- **Constituer l'équipe projet** — Chef de projet, experts sécurité, administrateurs systèmes, représentants métiers
- **Réaliser un audit de sécurité Active Directory complet** — Utiliser BloodHound, PingCastle ou Purple Knight pour identifier les chemins d'attaque
- **Établir l'inventaire exhaustif des ressources** — Tous les serveurs, postes de travail, comptes, groupes privilégiés, applications
- **Catégoriser toutes les ressources par tier** — Déterminer quel tier pour chaque ressource selon sa criticité
- **Identifier et documenter les ressources Tier 0** — DC, serveurs PKI, systèmes de backup AD, serveurs d'administration, etc.
- **Définir la politique et la nomenclature des comptes** — Convention de nommage pour les comptes admin (ex: T0-Admin-NomPrenom)
- **Élaborer le plan de déploiement détaillé** — Planning, ressources, budgets, jalons, risques, plan de communication
- **Budgéter le projet (matériel, licences, prestations, formation)** — PAW, Jump Servers, solutions SIEM/EDR, prestations d'audit, formation

- **Mettre en place un environnement de lab/test** — Reproduire l'environnement de production pour tester les configurations

# Phase 2 : Implémentation du Tier 0 (Mois 4-9)

## A. Structure Active Directory

- **Créer l'OU dédiée Tier 0 dans AD** — Organiser les objets Tier 0 dans une structure OU dédiée et protégée
- **Durcir les contrôleurs de domaine** — Appliquer les baselines de sécurité Microsoft, désactiver services inutiles
- **Vérifier le niveau fonctionnel de la forêt et des domaines** — Minimum Windows Server 2012 R2 pour Protected Users et silos d'authentification

## B. Comptes et Groupes Privilégiés

- **Créer les comptes administrateurs Tier 0 dédiés** — Un compte dédié par administrateur, nomenclature cohérente
- **Ajouter les comptes admin Tier 0 au groupe Protected Users** — Protection renforcée contre le vol de credentials
- **Nettoyer les groupes privilégiés (Domain Admins, Enterprise Admins)** — Retirer tous les comptes inutiles, viser zéro membre permanent
- **Créer et configurer les comptes break-glass** — 2 comptes d'urgence avec mots de passe complexes en coffre-fort physique
- **Interdire la connexion interactive sur les serveurs pour les comptes de service** — Utiliser gMSA ou MSA, interdire logon interactif via GPO

## C. PAW (Privileged Access Workstations)

- **Acquérir et déployer les PAW Tier 0** — Postes dédiés, durcis, jamais utilisés pour autre chose que l'admin Tier 0
- **Appliquer la baseline de sécurité PAW** — GPO restrictives, AppLocker/WDAC, Credential Guard, Device Guard
- **Déployer EDR sur tous les PAW** — Solution de détection et réponse aux menaces sur endpoints
- **Configurer Credential Guard et Remote Credential Guard** — Protection matérielle des credentials contre le vol

- **Restreindre les connexions aux PAW Tier 0** — Seuls les comptes admin Tier 0 peuvent se connecter aux PAW Tier 0

## D. Authentification et Protocoles

- **Désactiver NTLM pour le Tier 0 (Kerberos uniquement)** — Configurer via GPO, auditer avant application
- **Déployer l'authentification multi-facteurs (MFA) pour Tier 0** — Smartcard, Windows Hello for Business, ou autre MFA forte
- **Configurer les silos d'authentification pour Tier 0** — Restreindre où les comptes Tier 0 peuvent s'authentifier
- **Implémenter les politiques d'authentification** — Contrôles d'accès dynamiques basés sur le contexte

## E. Segmentation et Réseau

- **Créer un VLAN dédié pour le Tier 0** — Isolation réseau physique/logique des ressources Tier 0
- **Configurer les règles de firewall inter-tiers** — Bloquer tout flux non autorisé depuis Tier 1/2 vers Tier 0
- **Implémenter le principe du moindre privilège réseau** — Autoriser uniquement les flux nécessaires, bloquer le reste par défaut

## F. Gestion des Mots de Passe et Secrets

- **Déployer LAPS (Local Administrator Password Solution)** — Gestion automatisée des mots de passe admin locaux sur tous les systèmes
- **Appliquer une politique de mots de passe renforcée Tier 0** — Longueur minimale 15+ caractères, complexité élevée, rotation régulière
- **Déployer une solution PAM (Privileged Access Management)** — Coffre-fort pour secrets, élévation just-in-time, enregistrement sessions

## G. Surveillance et Journalisation

- **Activer l'audit avancé sur tous les objets Tier 0** — Auditer tous les changements, connexions, élévations de privilèges
- **Déployer/configurer une solution SIEM** — Centralisation et analyse des logs, alertes temps réel

- **Créer les règles de détection spécifiques Tier 0** — Alertes sur connexions inter-tiers, modifications groupes privilégiés, etc.
- **Configurer la rétention longue durée des logs Tier 0** — Minimum 1 an, idéalement 2-3 ans pour investigation et conformité

### H. Documentation et Formation

- **Documenter l'architecture Tier 0** — Diagrammes réseau, liste ressources, comptes, GPO, procédures
- **Rédiger les procédures d'administration Tier 0** — Mode opératoire pour toutes les tâches courantes et d'urgence
- **Former les administrateurs Tier 0** — Formation théorique et pratique sur le modèle, les outils, les procédures

## Phase 3 : Implémentation du Tier 1 (Mois 10-15)

- **Créer l'OU dédiée Tier 1 dans AD** — Structure organisationnelle pour les ressources Tier 1
- **Créer les comptes administrateurs Tier 1** — Comptes dédiés pour l'administration des serveurs applicatifs
- **Déployer les Jump Servers Tier 1** — Bastions d'administration pour accéder aux serveurs Tier 1
- **Appliquer les GPO de durcissement Tier 1** — Politiques de sécurité adaptées au niveau Tier 1
- **Déployer LAPS sur tous les serveurs Tier 1** — Gestion automatisée des mots de passe admin locaux
- **Segmenter le réseau Tier 1 (VLAN dédié)** — Isolation réseau des serveurs applicatifs
- **Configurer les restrictions d'authentification Tier 1** — Empêcher les comptes Tier 1 de s'authentifier sur Tier 0
- **Déployer EDR sur tous les serveurs Tier 1** — Protection des serveurs applicatifs
- **Configurer la surveillance SIEM pour Tier 1** — Collecte logs, alertes sur activités suspectes
- **Former les administrateurs Tier 1** — Procédures d'administration via Jump Servers

## Phase 4 : Implémentation du Tier 2 (Mois 16-21)

- **Créer l'OU dédiée Tier 2 dans AD** — Structure pour les postes de travail
- **Déployer une solution MDM (Intune ou équivalent)** — Gestion et sécurisation des postes de travail
- **Déployer LAPS sur tous les postes Tier 2** — Gestion des mots de passe admin locaux
- **Appliquer les baselines de sécurité Tier 2** — GPO de durcissement pour postes utilisateurs
- **Déployer EDR/Antivirus sur tous les postes Tier 2** — Protection endpoint obligatoire
- **Configurer les restrictions pour empêcher admin sur Tier 0/1** — Les comptes utilisateurs ne peuvent administrer que Tier 2
- **Implémenter le contrôle d'applications (AppLocker/WDAC)** — Whitelist des applications autorisées
- **Configurer la surveillance SIEM pour Tier 2** — Collecte logs essentiels, détection anomalies
- **Sensibiliser les utilisateurs finaux** — Formation sécurité, phishing, bonnes pratiques

## Phase 5 : Maintien en Condition de Sécurité (Continu)

- **Mettre en place les audits trimestriels avec BloodHound** — Vérifier qu'aucun chemin d'attaque vers Tier 0 n'existe
- **Établir un processus de gestion des changements** — Validation impact tiering pour tout changement
- **Planifier les revues mensuelles des comptes privilégiés** — Vérifier nécessité et activité de chaque compte
- **Déployer un processus de gestion des mises à jour par tier** — Tier 0: ultra-prudent, Tier 2: automatisé
- **Réaliser des pentests annuels ciblés AD** — Red team pour tester l'efficacité du tiering
- **Former annuellement les équipes (recyclage)** — Mise à jour compétences, nouvelles menaces
- **Suivre les indicateurs de performance (KPI)** — Chemins d'attaque, violations, temps détection, conformité
- **Mettre à jour la documentation régulièrement** — Maintenir à jour schémas, procédures, inventaires

- **Effectuer une veille technologique et sécuritaire** — Nouvelles menaces AD, nouvelles contre-mesures, évolutions Microsoft
- **Tester régulièrement les procédures de réponse à incident** — Exercices de crise, simulation compromission Tier 0

## Prérequis Techniques et Organisationnels

| Catégorie | Prérequis | Priorité |
|---|---|---|
| **Infrastructure** | Niveau fonctionnel AD: Windows Server 2012 R2 minimum | Critique |
| **Infrastructure** | Contrôleurs de domaine à jour (patches sécurité) | Critique |
| **Matériel** | PAW dédiés pour administrateurs Tier 0 (1 par admin) | Critique |
| **Matériel** | Jump Servers pour Tier 1 (2+ pour redondance) | Haute |
| **Logiciel** | Solution SIEM (Splunk, Elastic, Sentinel, etc.) | Critique |
| **Logiciel** | Solution EDR (Defender ATP, CrowdStrike, etc.) | Critique |
| **Logiciel** | LAPS (Local Administrator Password Solution) | Critique |
| **Logiciel** | Solution MDM (Intune, SCCM, Workspace ONE) | Haute |
| **Logiciel** | Solution PAM optionnelle (CyberArk, Thycotic, etc.) | Moyenne |
| **Ressources Humaines** | Chef de projet dédié (0.5-1 ETP) | Critique |
| **Ressources Humaines** | Experts sécurité disponibles (1-2 personnes) | Critique |
| **Ressources Humaines** | Disponibilité équipes admin (formation, mise en œuvre) | Haute |
| **Budget** | 100K€ - 500K€ pour PME (50-500 utilisateurs) | Critique |
| **Budget** | 500K€ - 2M€ pour ETI/GE (500+ utilisateurs) | Critique |
| **Organisationnel** | Soutien direction générale explicite | Critique |
| **Organisationnel** | Acceptation changement par les équipes IT | Haute |

Points d'Attention CritiquesNe jamais utiliser un compte Tier 0 sur un système Tier 1 ou 2- Cela annule le cloisonnementPrivilégier une approche progressive- Commencer par Tier 0, valider, puis étendreTester en lab avant production- Éviter les surprises en productionNe pas sous-estimer la résistance au changement- Communication et formation sont essentiellesPrévoir un plan B pour chaque étape critique- Rollback doit être possible

Critères de Succès du ProjetZéro chemin d'attaque critique vers le Tier 0 (validé par BloodHound)100% des comptes admin utilisent des comptes dédiés par tier100% des connexions admin Tier 0 se font via PAW uniquementDétection automatisée de toute tentative de violation inter-tiersConformité >98% aux baselines de sécurité par tierTemps moyen de détection d'incident <1hZéro incident de compromission totale AD post-tiering

ANNEXE B

# FAQ

## Questions Générales

### Q : Qu'est-ce que le modèle de tiering et pourquoi est-il important ?

Le modèle de tiering est une approche de sécurité qui segmente les ressources IT en trois niveaux hiérarchiques basés sur leur criticité :

- **Tier 0 :** Active Directory et ressources critiques
- **Tier 1 :** Serveurs applicatifs et d'infrastructure
- **Tier 2 :** Postes de travail utilisateurs

**Importance :** Il empêche la propagation latérale des attaques. Sans tiering, un attaquant compromettant un simple poste utilisateur peut facilement escalader ses privilèges jusqu'à devenir Domain Admin.

💡 **Bon à savoir :** Le tiering réduit de 70-90% la probabilité qu'une compromission Tier 2 atteigne le Tier 0.

### Q : Combien de temps faut-il pour implémenter le tiering complet ?

La durée varie selon la taille et la complexité de l'environnement :

- **PME (< 500 utilisateurs) :** 3-6 mois
- **Entreprise moyenne (500-2000 utilisateurs) :** 6-12 mois
- **Grande entreprise (> 2000 utilisateurs) :** 12-24 mois

⚠️ **Important :** Ne cherchez pas la perfection dès le début ! Une approche itérative avec sécurisation du Tier 0 en priorité (2-3 mois) apporte déjà 80% des bénéfices.

### Q : Quel est le coût d'implémentation du tiering ?

> Le coût varie significativement selon l'échelle :
>
> - **Licences logicielles :** La plupart des fonctionnalités sont incluses dans Windows Server et Windows 10/11 Enterprise (déjà possédés généralement)
> - **Matériel PAW :** 1000-2000€ par PAW × nombre d'admins Tier 0
> - **SIEM/EDR :** Variable selon la solution (gratuit avec Windows Defender ou 50-100€/endpoint/an pour solutions commerciales)
> - **Consulting/Formation :** 20 000-100 000€ selon taille
> - **Temps interne :** 0.5-2 ETP pendant la durée du projet
>
> 💰 **ROI :** Le coût d'une compromission AD majeure est estimé entre 500 000€ et 5 000 000€. Le tiering se rembourse dès qu'il évite un seul incident majeur.

### Q : Peut-on implémenter le tiering progressivement ou faut-il tout faire d'un coup ?

> **Réponse :** L'approche progressive est non seulement possible, mais fortement recommandée !
>
> **Ordre recommandé :**
>
> 1. **Phase 1 (priorité absolue) :** Sécuriser le Tier 0
>    - Identifier et isoler les ressources Tier 0
>    - Déployer des PAW pour admins Tier 0
>    - Activer Protected Users et LAPS
>    - Bloquer NTLM pour comptes Tier 0
> 2. **Phase 2 :** Implémenter Tier 1 (serveurs)
> 3. **Phase 3 :** Renforcer Tier 2 (postes)
> 4. **Phase 4 :** Optimisation et amélioration continue
>
> ✅ **Avantage :** Gains de sécurité progressifs, risque de disruption minimisé, apprentissage au fur et à mesure.

## Questions sur le Tier 0

### Q : Combien de PAW Tier 0 faut-il déployer ?

> **Règle de base :** 1 PAW par administrateur Tier 0, minimum 2 PAW au total.

**Calcul recommandé :**

- 1 PAW par admin Tier 0 actif
- +1-2 PAW de secours partagés
- +1 PAW pour les comptes break-glass

**Exemple :** Pour 4 administrateurs Tier 0 → 4 PAW + 2 secours = 6 PAW au total

**Alternative :** Si le budget PAW est limité, commencer avec des Jump Servers Tier 0 (1-2 serveurs Windows durcis) puis migrer vers des PAW.

### Q : Peut-on virtualiser les PAW ou doivent-ils être physiques ?

**Recommandation :** PAW physiques pour Tier 0, virtualisation acceptable pour Tier 1.

**Pourquoi physique pour Tier 0 ?**

- Évite la dépendance à l'hyperviseur (qui doit lui-même être Tier 0)
- Meilleur isolement (pas de VM escape possible)
- Simplicité de la gestion des droits

**Exception :** Si l'hyperviseur est déjà catégorisé Tier 0 et strictement sécurisé, la virtualisation est acceptable.

⚠️ **Attention :** Ne JAMAIS virtualiser des PAW Tier 0 sur un hyperviseur géré depuis le Tier 1 ou 2 !

### Q : Que faire si un administrateur Tier 0 a besoin d'accéder à Internet ?

**Solution :** Utiliser deux postes distincts ou une architecture multi-session.

**Option 1 (Recommandée) :** Deux postes physiques séparés

- PC standard (Tier 2) pour email, Internet, bureautique
- PAW Tier 0 dédié pour administration AD uniquement

**Option 2 :** Architecture "Local Admin on Secure Host"

- Un seul PC physique
- VM locale pour navigation Internet (Tier 2)
- Système hôte = PAW Tier 0

❌ **JAMAIS :** Naviguer sur Internet ou consulter emails depuis un PAW Tier 0 !

### Q : Faut-il vraiment bloquer NTLM pour le Tier 0 ?

**Oui, c'est fortement recommandé !** NTLM est vulnérable aux attaques Pass-the-Hash.

**Approche progressive :**

1. Activer l'audit NTLM pour identifier les usages (1-2 mois)
2. Migrer ces usages vers Kerberos (configuration SPN)
3. Bloquer NTLM pour comptes Tier 0 via Protected Users
4. Surveiller les tentatives bloquées

✅ **Bénéfice :** Blocage NTLM élimine la majorité des techniques de mouvement latéral utilisées par les attaquants.

## Questions sur le Tier 1

### Q : Jump Server vs PAW pour administrer le Tier 1 : quelle différence ?

**Jump Server :**

- Serveur Windows centralisé accessible en RDP
- Partagé entre plusieurs administrateurs
- Plus simple à déployer et gérer
- Nécessite Remote Credential Guard
- Coût : 1-2 serveurs pour toute l'équipe

**PAW Tier 1 :**

- Poste dédié par administrateur
- Meilleur isolement
- Plus complexe à gérer
- Coût : 1 poste × nombre d'admins

💡 **Recommandation :** Jump Servers pour Tier 1 (bon compromis coût/sécurité), PAW réservés au Tier 0.

### Q : Comment catégoriser un serveur qui héberge à la fois des apps Tier 1 et Tier 2 ?

**Règle :** Catégoriser au niveau le plus élevé = Tier 1 dans ce cas.

**Mieux encore :** Éviter cette situation !

- Séparer les applications sur des serveurs distincts
- Ou virtualiser pour isoler chaque tier

⚠️ **Problème :** Un serveur multi-tier nécessite des comptes admin Tier 1, mais est accessible depuis Tier 2, créant un chemin d'attaque potentiel.

# Questions sur le Tier 2

### Q : LAPS est-il vraiment nécessaire si on a déjà des mots de passe complexes ?

> **Oui, absolument !** LAPS résout un problème différent.
>
> **Le problème :** Même avec un mot de passe complexe "Admin@2024!", si ce mot de passe est identique sur 500 postes, un attaquant qui compromet un poste peut utiliser Pass-the-Hash pour accéder aux 499 autres.
>
> **Solution LAPS :**
>
> - Mot de passe unique par machine
> - Rotation automatique régulière
> - Stocker sécurisé dans AD
>
> ✅ **Impact :** LAPS bloque 80% des mouvements latéraux dans le Tier 2.

### Q : Faut-il segmenter le Tier 2 (postes VIP, développeurs, etc.) ?

> **Recommandé pour certaines populations :**
>
> - **Postes VIP/Direction :** Cibles de choix pour le phishing, surveillance accrue
> - **Postes développeurs :** Besoins spécifiques (admin local parfois), risque élevé
> - **Postes finance/RH :** Accès à données sensibles
>
> **Segmentation via :**
>
> - OU dédiées dans AD
> - GPO spécifiques
> - Sous-réseaux distincts si budget permet
> - Surveillance EDR renforcée

# Questions d'Implémentation

### Q : Par où commencer concrètement ?

> **Plan d'action premiers 30 jours :**
>
> 1. **Semaine 1 :** Audit de l'existant
>    - Exécuter BloodHound pour identifier chemins d'attaque
>    - Lister tous les comptes privilégiés

    - Identifier les ressources Tier 0
2. **Semaine 2 :** Quick wins Tier 0
    - Réduire membership de Domain Admins au strict minimum
    - Activer l'audit avancé sur les DC
    - Créer comptes break-glass
3. **Semaine 3-4 :** Premiers contrôles
    - Déployer LAPS
    - Créer premier PAW Tier 0 (ou Jump Server)
    - Ajouter comptes Tier 0 à Protected Users

📋 **Ressource :** Consultez notre Checklist de Déploiement pour le plan complet !

### Q : Comment gérer la résistance au changement des équipes ?

**Stratégies éprouvées :**

1. **Sponsorship exécutif :** Obtenir le soutien visible de la direction
2. **Communication claire :** Expliquer le "pourquoi" (protection contre ransomware, etc.)
3. **Formation :** Former les admins aux nouvelles pratiques
4. **Progression douce :** Commencer avec les admins volontaires
5. **Montrer les bénéfices :** Démonstration d'attaque bloquée grâce au tiering

⚠️ **Erreur fréquente :** Imposer le changement sans explication ni formation = échec garanti !

### Q : Peut-on faire le tiering sans budget dédié ?

**Oui ! Beaucoup est possible avec les outils natifs Windows.**

**Gratuit ou presque :**

- Protected Users (natif AD)
- LAPS (gratuit Microsoft)
- Silos d'authentification (natif Windows Server)
- Credential Guard (natif Windows 10/11 Enterprise)
- GPO pour durcissement (natif)
- Windows Defender (antivirus natif, mode EDR basique)

**Investissements recommandés si budget :**

- PAW hardware (2-3 machines : 5000€)
- EDR commercial (meilleure détection)

- SIEM (pour grandes organisations)

💡 **Astuce :** Commencer avec 100% gratuit, puis investir progressivement selon les besoins identifiés.

## Questions sur les Outils

### Q : BloodHound est-il un outil d'attaquant ou de défenseur ?

**Les deux !** BloodHound est un outil à double usage (dual-use).

**Usage défensif (recommandé) :**

- Identifier les chemins d'attaque avant les attaquants
- Prioriser les actions de sécurisation
- Valider l'efficacité du tiering
- Audit régulier de la posture de sécurité

**Précautions :**

- Exécuter SharpHound avec un compte dédié
- Stocker les résultats de manière sécurisée
- Ne pas laisser BloodHound accessible à tous

📊 **Fréquence :** Exécuter BloodHound tous les trimestres pour suivre l'évolution des chemins d'attaque.

### Q : Quel SIEM choisir pour le monitoring du tiering ?

**Options selon la taille :**

**PME (< 500 endpoints) :**

- Microsoft Sentinel (cloud, coût par volume de logs)
- Elastic Stack (gratuit, self-hosted)
- Graylog (gratuit, plus simple qu'Elastic)

**Entreprise moyenne :**

- Splunk (puissant mais cher)
- Microsoft Sentinel
- IBM QRadar

**Grande entreprise :**

- Splunk Enterprise

- IBM QRadar
- LogRhythm

💡 **Conseil :** Pour le tiering, l'important est d'avoir des règles de détection pour violations inter-tiers, peu importe le SIEM choisi.

# Dépannage

### Q : Les comptes du groupe Protected Users ne peuvent plus s'authentifier, que faire ?

**Causes fréquentes :**

1. **Tickets Kerberos expirés (4h max)**
   - Solution : Re-authentification régulière automatique
   - Les sessions restent actives, seule la durée du TGT est limitée
2. **Application ne supporte pas Kerberos**
   - Solution : Configurer SPN pour l'application
   - Ou sortir le compte de service de Protected Users temporairement
3. **Niveau fonctionnel domaine insuffisant**
   - Vérifier : Windows Server 2012 R2 minimum requis
   - Upgrader le niveau fonctionnel si nécessaire

⚠️ **Ne PAS ajouter à Protected Users :** Compte Administrator intégré, comptes de service critiques sans test préalable

### Q : LAPS ne fonctionne pas, comment diagnostiquer ?

**Checklist de diagnostic :**

1. **Schéma AD étendu ?**
   - Vérifier attributs ms-Mcs-AdmPwd présents
   - Commande : `Get-ADObject "CN=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=domain,DC=com"`
2. **Droits sur l'OU ?**
   - Les ordinateurs doivent pouvoir écrire leur mot de passe
   - Commande: `Set-AdmPwdComputerSelfPermission -OrgUnit "OU=Computers"`
3. **GPO appliquée ?**
   - Vérifier sur le poste : `gpresult /h report.html`
   - Chercher "AdmPwd" dans le rapport

4. **Extension CSE installée ?**
    - Client LAPS installé sur les postes ?
    - Vérifier : `Get-WindowsCapability -Online | Where-Object Name -like '*LAPS*'`

### Q : Comment savoir si mon tiering est vraiment efficace ?

**Tests de validation :**

1. **Test BloodHound :**
    - Aucun chemin de Tier 2 vers Tier 0 ne doit exister
    - Query: "Shortest path from Tier 2 users to Domain Admins"
2. **Test d'authentification :**
    - Essayer de logon avec compte Tier 0 sur poste Tier 2 → Doit échouer
    - Vérifier les silos d'authentification fonctionnent
3. **Test SIEM :**
    - Simuler une violation (compte test Tier 0 sur Tier 2)
    - Alerte doit se déclencher en < 5 minutes
4. **Purple Team Exercise :**
    - Simuler une attaque complète
    - Vérifier que le tiering bloque la progression

📊 **KPI à suivre :** Nombre de chemins d'attaque (objectif: 0 depuis Tier 2 vers Tier 0), temps de détection violations, % conformité checklist

ANNEXE C

# Études de Cas

Découvrez comment différentes organisations ont implémenté avec succès le modèle de tiering.

Les études de cas suivantes sont basées sur des déploiements réels (noms et détails modifiés pour la confidentialité). Elles illustrent les défis rencontrés, les solutions apportées et les résultats obtenus.

## Cas #1: PME Manufacturing

350 employés | 400 endpoints | Secteur: Industrie | Durée: 5 mois

### Contexte

Entreprise de fabrication de composants électroniques avec un site de production principal et deux sites commerciaux. L'infrastructure IT était gérée par une équipe de 3 personnes.

**Problématique initiale:** Suite à une tentative de ransomware bloquée de justesse, la direction a décidé de renforcer la sécurité de l'Active Directory qui contenait des comptes avec des privilèges excessifs non contrôlés.

### État Initial

23Comptes Domain Admins0PAW déployés100%MDP admin identiques47Chemins d'attaque vers DA

## Déroulement du Projet

Mois 1: Audit et PréparationExécution de BloodHound qui révèle 47 chemins d'attaque différents permettant à un utilisateur standard de devenir Domain Admin. Identification de 23 comptes dans le groupe Domain Admins, dont 8 comptes de service et 5 comptes inactifs depuis plus d'un an.Mois 2: Quick Wins Tier 0Nettoyage du groupe Domain Admins (passage de 23 à 5 membres). Création de 2 comptes break-glass. Activation de l'audit avancé sur les contrôleurs de domaine. Déploiement LAPS sur 100% des serveurs et postes.Mois 3: Déploiement PAWAcquisition et déploiement de 3 PAW pour les administrateurs Tier 0. Configuration du réseau dédié (VLAN 10). Ajout des comptes Tier 0 au groupe Protected Users après tests de compatibilité.Mois 4: Tier 1 & 2Mise en place d'un Jump Server pour l'administration Tier 1. Durcissement des GPO par tier. Configuration Credential Guard sur les postes Windows 10.Mois 5: Validation et FormationNouvelle analyse BloodHound montrant 0 chemin d'attaque direct vers Tier 0. Formation de l'ensemble des équipes IT. Documentation complète livrée.

## Défis Rencontrés

Défi #1: Résistance au changementProblème:Les administrateurs se plaignaient de la "complexité" d'utiliser un PAW séparé.Solution:Sessions de formation pratiques montrant des attaques réelles bloquées grâce au tiering. Sponsorship visible du directeur IT lors de réunions d'équipe.

Défi #2: Budget limitéProblème:Budget initial de 3 PAW insuffisant (besoin de 5).Solution:Reconditionnement de 2 anciens PC fixes performants en PAW, économisant 3000€. Utilisation maximale des outils gratuits (LAPS, Protected Users, GPO natives).

Défi #3: Application métier incompatible avec Protected UsersProblème:Une application ERP critique ne fonctionnait pas avec Kerberos uniquement.Solution:Configuration des SPN manquants sur le serveur ERP. Migration progressive avec période de test de 2 semaines avant activation définitive.

## Résultats Obtenus

0 chemin d'attaqueDe Tier 2 vers Tier 0 (vs 47 initialement)👥78% de réductionComptes Domain Admins (23 → 5) 🔑100% LAPSSur tous les endpoints 💰Budget: 28 000€Vs estimation initiale 35 000€

Impact MesurableDétection de 2 tentatives d'escalade de privilèges bloquées par le tiering dans les 6 mois suivantsTemps de détection des anomalies divisé par 4 grâce à l'audit amélioréConformité réglementaire validée lors de l'audit annuel0 incident de sécurité Tier 0 depuis le déploiement (18 mois)

### Témoignage

Au début, notre équipe était sceptique. Utiliser des PAW semblait lourd. Mais après avoir vu une démonstration d'attaque Pass-the-Hash bloquée grâce au tiering, tout le monde a compris l'intérêt. Aujourd'hui, c'est devenu naturel et on dort mieux la nuit!— Responsable IT, PME Manufacturing

### Leçons Apprises

Ce qui a bien fonctionnéApproche progressive:Commencer par Tier 0 a permis des gains rapides et visiblesCommunication:Impliquer les équipes dès le début avec des démos d'attaqueQuick wins:LAPS et nettoyage Domain Admins ont montré des résultats immédiatsFormation:Sessions pratiques plus efficaces que la théorie

## Cas #2: Groupe Bancaire International

8 500 employés | 12 000 endpoints | Secteur: Finance | Durée: 18 mois

### Contexte

Groupe bancaire avec présence dans 15 pays, infrastructure AD complexe avec 6 forêts interconnectées. Équipe IT de 80 personnes réparties sur plusieurs sites.

**Motivations:** Conformité réglementaire stricte (DORA, PCI-DSS), prévention contre APT ciblant le secteur financier, et recommandations d'un audit de sécurité externe.

### État Initial

156Comptes privilégiés6Forêts AD280Serveurs12KEndpoints

## Approche Projet

Phase 1 (Mois 1-4): Audit GlobalAudit approfondi des 6 forêts avec BloodHound. Découverte de chemins d'attaque critiques entre forêts. Cartographie complète de tous les comptes privilégiés. Identification de 47 comptes de service Tier 0 avec SPN (risque Kerberoasting majeur).Phase 2 (Mois 5-10): Déploiement PiloteSélection d'une forêt pilote (2000 utilisateurs). Déploiement de 12 PAW Tier 0. Implémentation complète du tiering sur le pilote. Tests approfondis pendant 2 mois. Ajustements basés sur les retours terrain.Phase 3 (Mois 11-18): Déploiement GlobalExtension progressive aux 5 autres forêts (1 par mois). Déploiement de 65 PAW au total. Mise en place d'un SOC dédié avec règles de détection spécifiques. Formation de 120 administrateurs. Certification de conformité obtenue.

## Innovations Spécifiques

Solutions Avancées DéployéesPAW Virtualisés:Solution "Virtual PAW" avec isolation VSM pour les admins en télétravailSIEM Intégré:Microsoft Sentinel avec 85 règles de détection custom pour violations de tieringAutomation:Pipeline CI/CD pour déploiement automatisé des GPO de sécuritéBastion Tier 0:Jump Servers hautement disponibles (cluster actif/actif)HSM:Stockage des clés LAPS dans HSM pour conformité

## Résultats

93% réductionChemins d'attaque critiques✅100% conformitéDORA, PCI-DSS, ISO 27001🎯12 attaques détectéesTentatives bloquées en < 5 min💰Budget: 680 K€ROI atteint en 14 mois

## Témoignage

Le tiering est devenu un pilier de notre stratégie de cyberdéfense. Nous avons détecté et bloqué 12 tentatives d'intrusion avancées en 2 ans, dont 3 APT ciblant spécifiquement le secteur bancaire. Sans le tiering, au moins 2 de ces attaques auraient probablement compromis notre AD.— CISO, Groupe Bancaire International

# Cas #3: Collectivité Territoriale

1 200 agents | 1 500 endpoints | Secteur: Public | Durée: 7 mois

## Contexte

Métropole française de taille moyenne gérant des services publics critiques (état civil, police municipale, services sociaux). Infrastructure vieillissante avec dette technique importante.

**Déclencheur:** Attaque ransomware sur une collectivité voisine ayant paralysé les services pendant 3 semaines, causant un arrêt complet des services publics et une perte estimée à 2M€.

## Approche Pragmatique

Contrainte budgétaire forte obligeant à maximiser l'utilisation des outils natifs et gratuits.

Mois 1-2: Sécurisation Express Tier 0Focus sur les contrôles gratuits et à impact immédiat. Réduction drastique de Domain Admins (42 → 4). Activation Protected Users. Déploiement LAPS (gratuit). Audit avancé sur DC.Mois 3-4: PAW à Coût RéduitReconditionnement de 5 PC existants en PAW. Utilisation de Windows 10 Pro (déjà possédé) au lieu d'Enterprise. Configuration manuelle mais efficace.Mois 5-7: Extension et FormationExtension Tier 1 et 2. Formation interne de tous les agents IT. Documentation complète en français. Exercice de simulation d'attaque (table-top exercise).

## Solutions Créatives (Budget Limité)

Optimisations BudgétairesPAW reconditionnés:5 anciens PC reconditionnés au lieu de neufs (-8 000€)SIEM gratuit:Graylog open-source au lieu de Splunk (-40 000€/an)Formation interne:Formation en interne sans consultant externe (-15 000€)Outils natifs Windows:100% outils Microsoft gratuits (LAPS, Protected Users, GPO)BloodHound CE:Version Community Edition gratuiteBudget total: 18 500€(vs estimation initiale 65 000€)

## Résultats

72% économieBudget: 18.5K€ vs 65K€ estimé🔒90% réductionComptes Domain Admins (42 → 4)🎯1 attaque bloquéeRansomware stoppé au Tier 2📜Conformité RGSRéférentiel Général de Sécurité

## Impact Réel

Incident Réel Bloqué (Mois 11 post-déploiement)Un agent a cliqué sur un lien de phishing, compromettant son poste Tier 2. Le ransomware s'est propagé à 15 postes du même réseau mais:✅LAPS a empêchéla propagation latérale (mots de passe admin uniques)✅Silos d'authentification ont bloquétoute tentative d'escalade vers Tier 1✅L'audit avancé a détectél'anomalie en 4 minutes✅L'Active Directory n'a pas été compromis✅Services publics maintenussans interruptionEstimation des dommages évités: 1.8 M€(basé sur l'incident de la collectivité voisine)

## Témoignage

Avec un budget très contraint, nous pensions que le tiering était inaccessible. En réalité, 80% de la sécurité vient des outils gratuits bien configurés. Quand nous avons bloqué le ransomware 11 mois après le déploiement, le retour sur investissement était déjà de 9700% ! Le tiering nous a littéralement sauvés.— DSI, Métropole Française

## Leçons Apprises

Points Clés pour Secteur PublicBudget limité n'est pas un obstacle:Les outils natifs suffisent pour 80% des besoinsReconditionnement:Les PAW ne nécessitent pas du matériel neufFormation interne:Monter en compétence les équipes plutôt qu'externaliserOpen source:Graylog, BloodHound CE sont des alternatives viablesROI prouvé:Un seul incident bloqué suffit à rentabiliser le projet

ANNEXE D

# Erreurs Courantes

Cette page compile les erreurs les plus fréquentes observées lors de déploiements réels.Basé sur l'analyse de dizaines de projets de tiering, voici les pièges à éviter absolument pour assurer le succès de votre implémentation.

# Erreurs de Conception

**L'erreur:** Essayer d'implémenter un tiering parfait sur les 3 tiers simultanément dès le démarrage, avec tous les contrôles possibles activés en même temps.

### Pourquoi c'est problématique:

- Projet devient trop complexe et ingérable
- Délais s'allongent indéfiniment (paralysie par analyse)
- Résistance au changement maximale (trop de changements d'un coup)
- Risque d'abandon du projet (équipes découragées)
- Aucun bénéfice visible avant des mois

### La bonne approche:

- **Phase 1:** Sécuriser UNIQUEMENT le Tier 0 (80% des bénéfices)
- **Quick wins:** Protected Users + LAPS + nettoyage Domain Admins (2-4 semaines)
- **Itération:** Améliorer progressivement avec retours terrain
- **Extension:** Tier 1 puis Tier 2 seulement après validation Tier 0

> *Statistique:Les projets avec approche itérative ont un taux de succès de 87% vs 34% pour les projets "big bang".*

**L'erreur:** Implémenter le tiering uniquement au niveau Active Directory (OUs, GPO, silos) sans aucune segmentation réseau entre les tiers.

### Conséquences:

- Un poste Tier 2 compromis peut tenter des attaques réseau directes vers Tier 0
- Pass-the-Hash latéral reste possible via SMB entre tiers
- Attaques de type relay (NTLM, Kerberos) non bloquées
- Efficacité du tiering réduite de 60%

### Solution:

- **VLANs séparés:** Un VLAN par tier minimum
  Exemple de segmentation:
  VLAN 10: Tier 0 (DC, ADCS, PAW)
  VLAN 20-25: Tier 1 (Serveurs par fonction)
  VLAN 40: Tier 2 (Postes utilisateurs)
  VLAN 30: DMZ (Accès Internet)
- **Firewall inter-VLAN:** Règles strictes autorisant uniquement les flux nécessaires
- **Principe deny-all:** Tout est bloqué par défaut, autorisations explicites uniquement
- **Monitoring:** Alertes sur toute tentative de connexion inter-tiers non autorisée

# Erreurs sur les Comptes Privilégiés

**L'erreur:** Utiliser des comptes de service membres de Domain Admins avec des SPN configurés, créant une cible parfaite pour Kerberoasting.

### Impact:

- N'importe quel utilisateur du domaine peut demander un ticket TGS pour ce service
- Le ticket contient un hash du mot de passe, crackable offline
- Si le mot de passe est faible, compromission Tier 0 garantie
- Attaque totalement silencieuse (requête Kerberos légitime)

### Solutions (par ordre de préférence):

- **1. Supprimer le compte de service des groupes Tier 0** (meilleure option)
  Principe du moindre privilège:
  Remove-ADGroupMember -Identity "Domain Admins" -Members "svc_backup"
  # Donner uniquement les droits spécifiques nécessaires
- **2. Utiliser des gMSA (Group Managed Service Accounts)**
  - Mots de passe auto-gérés de 240 caractères
  - Rotation automatique tous les 30 jours
  - Impossible à craquer (complexité extrême)

  Création d'un gMSA:
  New-ADServiceAccount -Name "gMSA_Backup" -DNSHostName "gmsa-backup.domain.com" \\
  -PrincipalsAllowedToRetrieveManagedPassword "Backup_Servers"
- **3. Mot de passe ultra-complexe si impossible autrement**
  - Minimum 25 caractères aléatoires
  - Stocké dans coffre-fort (CyberArk, Thycotic, etc.)
  - Rotation trimestrielle forcée

> *Réalité terrain:67% des mots de passe de comptes de service sont crackés en < 48h avec une machine standard.*

**L'erreur:** Laisser le compte Administrator intégré (RID 500) actif, avec un mot de passe connu de plusieurs personnes, non renommé.

### Risques:

- RID 500 toujours identifiable même si renommé
- Cible #1 des attaques par force brute
- Impossibleà verrouiller (lockout policy ne s'applique pas)
- Souvent mot de passe partagé = compromission si une personne part

### Bonnes pratiques:

- **1. Renommer le compte**
  Renommage (GUI ou PowerShell):
  Rename-ADObject -Identity (Get-ADUser -Filter {SID -like "*-500"}) \\
  -NewName "Legacy_Admin_DO_NOT_USE"
- **2. Définir un mot de passe ultra-complexe unique**
  - 35+ caractères aléatoires
  - Stocké dans coffre-fort physique scellé
  - Accès procédure break-glass uniquement
- **3. Désactiver si possible** (Attention: certains outils legacy en ont besoin)
  Disable-ADAccount -Identity (Get-ADUser -Filter {SID -like "*-500"})
- **4. Monitorer toute utilisation**
  - Alerte SIEM immédiate si connexion détectée
  - Audit Event ID 4624 (logon) pour ce compte

# Erreurs PAW & Administration

**L'erreur:** "Par commodité", autoriser la consultation d'emails, la navigation Internet ou l'utilisation d'Office sur un PAW Tier 0.

### Pourquoi c'est catastrophique:

- **Email = vecteur d'attaque #1** (phishing, pièces jointes malveillantes)
- **Navigation web:** Drive-by downloads, exploitation de vulnérabilités navigateur
- **Un seul clic malveillant** compromet le PAW = Tier 0 compromis
- **Contourne totalement** l'isolation recherchée

### Règles strictes PAW:

- **ZÉRO accès Internet** sur le PAW (blocage firewall)
- **ZÉRO email** (pas de client Outlook, pas de webmail)
- **Usage unique:** Administration Active Directory, point final
- **GPO bloquant:** Installation d'applications interdite

> *Statistique réelle:92% des compromissions Tier 0 impliquent un phishing ou un email malveillant cliqué par un administrateur.*

**L'erreur:** Un administrateur se connecte sur son PAW avec son compte utilisateur standard ou son compte admin Tier 1 "pour vérifier quelque chose rapidement".

### Conséquences immédiates:

- Credentials Tier 1/2 stockés en mémoire sur la machine Tier 0
- Si le compte Tier 2 est compromis → accès au PAW → compromission Tier 0
- Crée un "pont" entre les tiers (violation du tiering)
- Annule l'isolation

### Configuration obligatoire:

- **Silos d'authentification:** INTERDIRE toute connexion non-Tier 0 sur PAW
  Configuration silo (PowerShell):
  New-ADAuthenticationPolicySilo -Name "Silo_Tier0" \\
  -UserAuthenticationPolicy "Policy_Tier0_Users" \\
  -ComputerAuthenticationPolicy "Policy_Tier0_Computers" \\
  -Enforce

  # Résultat: Toute tentative de logon avec compte non-Tier 0 = REFUSÉE
- **GPO restrictive:** Autoriser uniquement groupe "Tier 0 Admins" à se connecter
- **Alertes SIEM:** Notifier immédiatement si connexion anormale détectée

# Erreurs LAPS

**L'erreur:** Donner la permission de lire les mots de passe LAPS au groupe "Domain Users" ou "Authenticated Users" par facilité.

### Impact:

- N'importe quel utilisateur du domaine peut lire TOUS les mots de passe admin locaux
- Compromission d'un seul compte utilisateur = accès à toutes les machines
- Annule totalement le bénéfice de LAPS

### Configuration sécurisée:

- **Principe du moindre privilège strict:**
  Permissions recommandées:
  ```
  # Tier 0 : Seuls Domain Admins
  Set-AdmPwdReadPasswordPermission -OrgUnit "OU=Tier0,DC=domain,DC=com" \\
    -AllowedPrincipals "Domain Admins"

  # Tier 1 : Groupe dédié "Tier1_Server_Admins"
  Set-AdmPwdReadPasswordPermission -OrgUnit
  "OU=Tier1_Servers,DC=domain,DC=com" \\
    -AllowedPrincipals "Tier1_Server_Admins"

  # Tier 2 : Groupe "Helpdesk" (support desktop uniquement)
  Set-AdmPwdReadPasswordPermission -OrgUnit
  "OU=Workstations,DC=domain,DC=com" \\
    -AllowedPrincipals "Helpdesk_Tier2"
  ```
- **Audit obligatoire:** Logger toutes les lectures de mots de passe LAPS
  - Event ID 4662 dans Security log
  - Alerte si lecture anormale (hors heures, compte inhabituel)
- **Révision trimestrielle** des permissions avec:
  ```
  Find-AdmPwdExtendedRights -Identity "OU=Computers,DC=domain,DC=com" | \\
    Format-Table ExtendedRightHolders
  ```

# Erreurs de Monitoring

**L'erreur:** Déployer le tiering mais ne jamais activer l'audit avancé ni configurer de monitoring, en se disant "on verra plus tard".

### Problème:

- **Aucune visibilité** sur les violations de tiering
- **Impossibilité de détecter** tentatives d'intrusion
- **Pas de preuve** en cas d'incident (forensics impossible)
- **Non-conformité** réglementaire (RGPD, ISO 27001)
- **Faux sentiment de sécurité**

### Monitoring minimal obligatoire:

- **1. Audit avancé sur DC (gratuit):**
  Activer via GPO:
  Computer Config > Policies > Windows Settings > Security Settings > \\
  Advanced Audit Policy Configuration > Audit Policies

  Activer:
  - Account Logon > Audit Kerberos Authentication Service (Success, Failure)
  - Account Management > Audit User Account Management (Success, Failure)
  - DS Access > Audit Directory Service Changes (Success, Failure)
  - Logon/Logoff > Audit Logon (Success, Failure)
  - Privilege Use > Audit Sensitive Privilege Use (Success, Failure)
- **2. Collecte centralisée des logs (SIEM):**
  - Gratuit: Graylog, Elastic Stack
  - Payant: Splunk, Microsoft Sentinel, QRadar
  - Minimum: Windows Event Forwarding vers serveur central
- **3. Règles de détection critiques:**
  - Connexion compte Tier 0 sur machine Tier 1/2
  - Modification membership groupe Domain Admins
  - Création de compte Tier 0
  - Échec authentification répété sur DC
  - Utilisation compte Administrator intégré

> *Temps de détection moyen:SANS monitoring = 287 jours | AVEC monitoring = 12 heures*

# Erreurs Humaines & Processus

**L'erreur:** Déployer le tiering sans former les administrateurs, en supposant qu'ils comprendront "naturellement" les nouvelles contraintes.

### Résultats prévisibles:

- **Contournements:** Les admins trouvent des "shortcuts" qui cassent la sécurité
- **Erreurs:** Mauvaise utilisation des PAW, connexions inappropriées
- **Résistance:** "C'était mieux avant", sabotage passif
- **Démotivation:** Équipe frustrée et non engagée

### Programme de formation requis:

- **Session 1 - Sensibilisation (2h):**
  - Pourquoi le tiering (exemples attaques réelles)
  - Démonstration Pass-the-Hash sans tiering
  - Même démo BLOQUÉE par le tiering
  - Impact métier d'une compromission AD
- **Session 2 - Pratique PAW (3h):**
  - Utilisation quotidienne du PAW
  - Outils d'administration autorisés
  - Cas d'usage pratiques
  - Troubleshooting courant
- **Session 3 - Procédures (2h):**
  - Workflow pour tâches courantes
  - Procédure d'escalade si problème
  - Que faire en cas d'incident
- **Suivi:**
  - Point mensuel les 3 premiers mois
  - Retours terrain et ajustements
  - Recyclage annuel

> *Impact mesurable:Projets AVEC formation complète = 92% adhésion équipes vs 41% SANS formation*

**L'erreur:** Imposer des règles strictes de tiering sans aucun processus documenté pour gérer les exceptions légitimes, bloquant les admins.

### Conséquence:

- Admins bloqués dans l'urgence (incident de production)
- Contournements sauvages non documentés
- Perte de crédibilité du projet
- Création de "comptes shadow" hors processus

### Processus d'exception requis:

- **1. Définir les cas d'exception valides:**
  - Incident de production critique (P1)
  - Maintenance programmée approuvée
  - Disaster recovery
- **2. Workflow d'approbation:**
  Exemple de workflow:
  1. Demandeur remplit formulaire (justification, durée, scope)
  2. Approbation N+2 (ou astreinte si urgence)
  3. Validation RSSI (ou délégué)
  4. Activation temporaire (max 24h)
  5. Audit post-exception obligatoire
  6. Révocation automatique à expiration
- **3. Traçabilité complète:**
  - Toutes les exceptions loggées
  - Revue mensuelle des exceptions
  - Analyse des tendances (si trop d'exceptions = processus à revoir)
- **4. Comptes break-glass:**
  - 2 comptes de secours en coffre physique
  - MDP ultra-complexe sous scellés
  - Utilisables uniquement si AD totalement indisponible
  - Alerte critique immédiate si utilisés

ANNEXE E

# Glossaire

## A

### Active Directory (AD)

Service d'annuaire développé par Microsoft permettant de centraliser la gestion des ressources réseau (utilisateurs, ordinateurs, groupes, etc.) dans un environnement Windows. Il fournit les services d'authentification et d'autorisation pour l'ensemble du domaine.

*Exemple : Dans une entreprise, Active Directory stocke tous les comptes utilisateurs et définit qui peut accéder à quelles ressources.*

Voir aussi :Contrôleur de Domaine,Forêt,Domaine

### Attack Path (Chemin d'Attaque)

Séquence de relations, permissions ou vulnérabilités qu'un attaquant peut exploiter pour progresser depuis un point d'entrée initial vers une cible privilégiée (généralement le Tier 0). Les outils comme BloodHound permettent de visualiser ces chemins.

*Exemple : Un compte utilisateur Tier 2 → membre du groupe "Admins Serveurs" → ayant des droits sur un serveur Tier 1 → où un administrateur Tier 0 s'est connecté = chemin d'attaque vers Tier 0.*

Voir aussi :BloodHound,Mouvement Latéral

### Authentication Silo (Silo d'Authentification)

Fonctionnalité de Windows Server permettant de restreindre où et comment les comptes privilégiés peuvent s'authentifier. Un silo définit quels comptes peuvent accéder à quels systèmes, empêchant l'utilisation de comptes Tier 0 sur des systèmes de niveau inférieur.

*Exemple : Un silo "Tier0-DomainAdmins" autorise les comptes Domain Admins à s'authentifier uniquement sur les contrôleurs de domaine et les PAW Tier 0.*

Voir aussi :Tier 0,PAW

## B

### BloodHound

Outil d'audit Active Directory utilisant la théorie des graphes pour identifier les chemins d'attaque. Il collecte les relations entre objets AD (appartenances, délégations, sessions) et les visualise pour révéler comment un attaquant pourrait compromettre les comptes privilégiés.

*Exemple : BloodHound peut révéler qu'un compte utilisateur standard a un chemin indirect vers Domain Admin via 5 sauts de délégations et appartenances de groupes.*

Voir aussi :Chemin d'Attaque,SharpHound

### Break-Glass Account (Compte Bris de Glace)

Compte d'urgence hautement privilégié stocké de manière sécurisée et utilisé uniquement en cas de situation exceptionnelle (perte d'accès à tous les comptes normaux, défaillance MFA, etc.). Son utilisation déclenche des alertes immédiates.

*Exemple : Mot de passe ultra-complexe stocké dans un coffre-fort physique scellé, utilisable uniquement si tous les comptes Domain Admin sont verrouillés.*

Voir aussi :Tier 0,Procédures d'Urgence

## C

### Credential Guard

Technologie de sécurité Windows qui utilise la virtualisation (Virtual Secure Mode) pour isoler les secrets d'authentification (hashes, tickets Kerberos) dans un environnement protégé, les rendant inaccessibles même si le système est compromis. Protection contre Pass-the-Hash et Pass-the-Ticket.

*Exemple : Même si un malware compromet LSASS.exe, il ne peut pas extraire les credentials car ils sont isolés dans le Trustlet VSM.*

Voir aussi :VSM,Pass-the-Hash,Remote Credential Guard

### Control Path (Chemin de Contrôle)

Relation ou ensemble de relations permettant à un objet (utilisateur, groupe, système) d'exercer un contrôle administratif sur un autre objet. Exemple : appartenance à un groupe, délégation de droits, propriété d'objet AD.

*Exemple : Un utilisateur membre du groupe "Server Operators" a un chemin de contrôle vers tous les serveurs du domaine.*

Voir aussi :Délégation,Chemin d'Attaque

## D

### DCSync

Technique d'attaque qui exploite les permissions de réplication AD pour extraire les hashes de mots de passe de tous les comptes du domaine sans avoir besoin d'accéder directement au

contrôleur de domaine. Requiert les privilèges "Replicating Directory Changes" et "Replicating Directory Changes All".

*Exemple : Un attaquant avec ces permissions peut exécuter mimikatz "lsadump::dcsync /domain:contoso.com /user:Administrator" pour obtenir le hash de n'importe quel compte.*

Voir aussi :Pass-the-Hash,Golden Ticket

### Domain Admin (Administrateur de Domaine)

Membre du groupe "Domain Admins", disposant de privilèges administratifs complets sur tous les systèmes membres du domaine Active Directory. Ce groupe fait partie du Tier 0 et doit être strictement contrôlé.

*Exemple : Un compte Domain Admin peut administrer tous les serveurs et postes du domaine, modifier Active Directory, et créer de nouveaux comptes privilégiés.*

Voir aussi :Tier 0,Enterprise Admin

## E

### EDR (Endpoint Detection and Response)

Solution de sécurité avancée pour les endpoints (postes, serveurs) qui surveille en continu les comportements suspects, détecte les menaces, et permet une réponse automatisée ou guidée aux incidents. Va au-delà de l'antivirus traditionnel.

*Exemple : L'EDR détecte une tentative de dump LSASS.exe, bloque l'action, isole le poste compromis et alerte l'équipe sécurité.*

Voir aussi :SIEM,SOAR

### Enterprise Admin

Groupe de sécurité au niveau de la forêt Active Directory disposant de privilèges administratifs sur tous les domaines de la forêt. Utilisé uniquement pour des opérations exceptionnelles au niveau forêt. Doit rester vide en temps normal.

*Exemple : Ajout d'un nouveau domaine à la forêt, modification du schéma AD, gestion des relations d'approbation entre domaines.*

Voir aussi :Forêt,Tier 0,Domain Admin

## G

### Golden Ticket

Technique d'attaque sophistiquée où l'attaquant forge un ticket TGT Kerberos en utilisant le hash du compte krbtgt. Ce ticket permet de s'authentifier en tant que n'importe quel utilisateur du domaine, y compris des comptes inexistants, pendant une longue durée.

*Exemple : Après avoir obtenu le hash krbtgt via DCSync, l'attaquant crée un Golden Ticket valable 10 ans pour le compte "Administrator" et maintient ainsi une persistance même après changement des mots de passe.*

Voir aussi :DCSync,Kerberos,Silver Ticket

### GPO (Group Policy Object)

Objet Active Directory contenant un ensemble de paramètres de configuration qui peuvent être appliqués à des utilisateurs ou ordinateurs. Les GPO permettent de centraliser la gestion de la sécurité, des restrictions et des configurations.

*Exemple : Une GPO Tier 0 peut imposer des mots de passe de 20 caractères minimum, activer Credential Guard, et bloquer l'exécution de tous les programmes non signés.*

Voir aussi :OU,Durcissement

## K

### Kerberos

Protocole d'authentification réseau utilisant des tickets temporaires pour sécuriser l'authentification sans transmettre de mots de passe sur le réseau. Protocole par défaut et recommandé pour Active Directory, plus sécurisé que NTLM.

*Exemple : Un utilisateur s'authentifie et reçoit un TGT (Ticket Granting Ticket), qu'il utilise ensuite pour obtenir des TGS (Ticket Granting Service) pour accéder à différentes ressources sans ressaisir son mot de passe.*

Voir aussi :NTLM,Golden Ticket,Kerberoasting

### Kerberoasting

Technique d'attaque où l'attaquant demande des tickets de service Kerberos (TGS) pour des comptes de service, puis tente de craquer offline les hashes contenus dans ces tickets pour obtenir les mots de passe des comptes de service.

*Exemple : Un attaquant avec un compte utilisateur standard peut demander un TGS pour tous les SPN du domaine, puis utiliser hashcat pour craquer les hashes des comptes de service ayant des mots de passe faibles.*

Voir aussi :SPN,gMSA,Kerberos

## L

### LAPS (Local Administrator Password Solution)

Solution gratuite Microsoft qui gère automatiquement les mots de passe des comptes administrateurs locaux. LAPS génère un mot de passe unique et complexe pour chaque machine, le stocke dans AD, et le rotate régulièrement. Empêche les attaques Pass-the-Hash latérales.

*Exemple : Au lieu d'avoir le même mot de passe "Admin123" sur tous les postes, LAPS génère "Rp9#mK2vL5@qN8" pour PC-001, "qL7$nV4wP2@tM6" pour PC-002, etc., et les change tous les 30 jours.*

Voir aussi :Pass-the-Hash,Mouvement Latéral

# P

### PAW (Privileged Access Workstation)

Poste de travail durci et isolé, dédié exclusivement à l'administration des ressources privilégiées. Un PAW Tier 0 n'a pas d'accès Internet, pas d'email, et ne peut être utilisé que pour administrer le Tier 0. Protège contre le vol de credentials.

*Exemple : Un administrateur utilise son PC normal pour l'email et Internet (Tier 2), puis se connecte physiquement à un PAW Tier 0 isolé pour administrer les contrôleurs de domaine.*

Voir aussi :Tier 0,Jump Server,Credential Guard

### Pass-the-Hash (PtH)

Technique d'attaque où l'attaquant vole le hash NTLM d'un mot de passe (sans connaître le mot de passe en clair) et l'utilise directement pour s'authentifier sur d'autres systèmes. Particulièrement efficace si le même compte local admin existe sur plusieurs machines avec le même mot de passe.

*Exemple : L'attaquant compromet PC-001, extrait le hash du compte administrateur local, puis utilise ce hash pour s'authentifier sur PC-002, PC-003, etc., sans jamais connaître le mot de passe.*

Voir aussi :LAPS,Credential Guard,NTLM

### Protected Users Group

Groupe de sécurité introduit dans Windows Server 2012 R2 qui applique automatiquement des restrictions de sécurité renforcées à ses membres : blocage NTLM, tickets Kerberos limités à 4h, impossibilité de délégation Kerberos, pas de cache des credentials.

*Exemple : Un compte Domain Admin ajouté au groupe Protected Users ne pourra plus s'authentifier via NTLM et ses tickets Kerberos expireront après 4 heures maximum.*

Voir aussi :Tier 0,Kerberos,NTLM

# S

### SIEM (Security Information and Event Management)

Plateforme centralisée qui collecte, corrèle et analyse les logs de sécurité de toutes les sources (serveurs, pare-feu, AD, endpoints). Permet de détecter les anomalies, les violations du tiering, et les attaques en temps réel.

*Exemple : Le SIEM détecte qu'un compte Tier 0 s'est authentifié sur un poste Tier 2, corrèle avec d'autres événements suspects, et génère une alerte critique automatique.*

Voir aussi :EDR,SOAR

### SOAR (Security Orchestration, Automation and Response)

Plateforme qui automatise la réponse aux incidents de sécurité via des playbooks prédéfinis. Peut enrichir automatiquement les alertes, isoler des systèmes, désactiver des comptes, et orchestrer des actions complexes sans intervention humaine.

*Exemple : Détection d'un compte Tier 0 compromis → playbook SOAR désactive automatiquement le compte, isole les systèmes accédés, collecte les forensics, et notifie le RSSI par SMS.*

Voir aussi :SIEM,Réponse aux Incidents

## T

### Tier 0

Niveau le plus sensible du modèle de tiering, comprenant toutes les ressources ayant un contrôle administratif direct sur Active Directory : contrôleurs de domaine, comptes Domain/Enterprise Admins, PAW Tier 0, et infrastructures support critiques (hyperviseurs hébergeant les DC, etc.).

*Exemple : Contrôleurs de domaine DC01 et DC02, comptes Domain Admins, PAW Tier 0, serveurs de PKI, systèmes de sauvegarde des DC.*

Voir aussi :Tier 1,Tier 2,Modèle de Tiering

### Tier 1

Niveau intermédiaire comprenant les serveurs applicatifs et d'infrastructure qui hébergent les services métier de l'organisation : serveurs de bases de données, serveurs d'applications, serveurs de fichiers, Exchange, etc.

*Exemple : Serveurs SQL hébergeant l'ERP, serveurs Exchange, serveurs de fichiers métier, serveurs d'applications web internes.*

Voir aussi :Tier 0,Tier 2,Jump Server

### Tier 2

Niveau comprenant les postes de travail des utilisateurs finaux et les ressources auxquelles ils accèdent quotidiennement. Point d'entrée le plus exposé aux attaques (phishing, malware, etc.) mais sans privilèges sur les niveaux supérieurs.

*Exemple : PC des employés, laptops, stations de travail, tablettes professionnelles.*

Voir aussi :Tier 0,Tier 1,EDR

### Tiering Model (Modèle de Tiering)

Modèle de sécurité qui segmente les ressources IT en trois niveaux hiérarchiques (Tier 0, 1, 2) basés sur leur criticité et leur exposition. Principe fondamental : aucun secret d'un tier ne doit être accessible depuis un tier de niveau inférieur.

*Exemple : Un administrateur Tier 0 n'utilise JAMAIS ses credentials Tier 0 pour se connecter à un serveur Tier 1 ou un poste Tier 2.*

Voir aussi :Tier 0,Tier 1,Tier 2

ANNEXE F

# Scripts PowerShell

Collection complète de scripts PowerShell pour auditer, déployer et maintenir le modèle de tiering Active Directory. Chaque script est documenté, testé et prêt à l'emploi.

## Audit-ADTiering.ps1

Audit global de votre Active Directory pour identifier les chemins d'attaque et les violations de tiering.

- Liste tous les comptes privilégiés
- Identifie les comptes Tier 0
- Vérifie Protected Users
- Export CSV et HTML
- Recommandations automatiques

```
<#
.SYNOPSIS
    Audit complet d'Active Directory pour le modèle de tiering
.DESCRIPTION
    Ce script audite votre AD et identifie :
    - Tous les comptes privilégiés
    - Les comptes Tier 0
    - Les membres de Protected Users
    - Les violations potentielles de tiering
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
    [string]$OutputPath = "C:\\ADTiering\\Audit",
    [switch]$ExportHTML,
    [switch]$ExportCSV
)

# Vérification module AD
if (-not (Get-Module -ListAvailable -Name ActiveDirectory)) {
    Write-Error "Module ActiveDirectory requis. Installez les RSAT."
    exit 1
}

Import-Module ActiveDirectory
```

```
# Création du dossier de sortie
if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== Audit Active Directory - Modèle de Tiering ===" -ForegroundColor Cyan
Write-Host ""

# 1. Identification des groupes privilégiés Tier 0
Write-Host "[1/6] Analyse des groupes privilégiés Tier 0..." -ForegroundColor Yellow

$Tier0Groups = @(
    "Domain Admins",
    "Enterprise Admins",
    "Schema Admins",
    "Administrators",
    "Account Operators",
    "Backup Operators",
    "Server Operators",
    "Print Operators",
    "DnsAdmins",
    "Group Policy Creator Owners"
)

$Tier0Members = @()
foreach ($group in $Tier0Groups) {
    try {
        $members = Get-ADGroupMember -Identity $group -Recursive -ErrorAction SilentlyContinue
        foreach ($member in $members) {
            if ($member.objectClass -eq 'user') {
                $Tier0Members += [PSCustomObject]@{
                    Username = $member.SamAccountName
                    Name = $member.Name
                    Group = $group
                    Enabled = (Get-ADUser $member -Properties Enabled).Enabled
                }
            }
        }
    } catch {
        Write-Warning "Impossible de lire le groupe: $group"
    }
}

Write-Host "   ✓ Trouvé $($Tier0Members.Count) membres dans les groupes Tier 0" -ForegroundColor Green

# 2. Vérification Protected Users
Write-Host "[2/6] Vérification du groupe Protected Users..." -ForegroundColor Yellow

$ProtectedUsers = Get-ADGroupMember -Identity "Protected Users" -ErrorAction SilentlyContinue
$ProtectedUsersList = $ProtectedUsers | Where-Object {$_.objectClass -eq 'user'} | Select-Object
-ExpandProperty SamAccountName

Write-Host "   ✓ $($ProtectedUsersList.Count) comptes dans Protected Users" -ForegroundColor Green

# 3. Identification des comptes Tier 0 non protégés
Write-Host "[3/6] Identification des comptes Tier 0 non protégés..." -ForegroundColor Yellow

$UnprotectedTier0 = $Tier0Members | Where-Object {
    $_.Username -notin $ProtectedUsersList -and $_.Enabled -eq $true
} | Select-Object Username, Name, Group -Unique

Write-Host "   ⚠️  $($UnprotectedTier0.Count) comptes Tier 0 NON dans Protected Users" -ForegroundColor
Red

# 4. Vérification des comptes avec SPN (risque Kerberoasting)
Write-Host "[4/6] Recherche de comptes à risque (Kerberoasting)..." -ForegroundColor Yellow

$UsersWithSPN = Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties ServicePrincipalName,
MemberOf
```

```
$Tier0WithSPN = $UsersWithSPN | Where-Object {
    $userGroups = $_.MemberOf
    $isTier0 = $false
    foreach ($group in $Tier0Groups) {
        if ($userGroups -match $group) {
            $isTier0 = $true
            break
        }
    }
    $isTier0
}

Write-Host "   ⚠️  $($Tier0WithSPN.Count) comptes Tier 0 avec SPN (risque Kerberoasting)"
-ForegroundColor Red

# 5. Recherche des comptes admin inactifs
Write-Host "[5/6] Recherche de comptes admin inactifs..." -ForegroundColor Yellow

$InactiveThreshold = (Get-Date).AddDays(-90)
$InactiveAdmins = @()

foreach ($member in $Tier0Members) {
    $user = Get-ADUser $member.Username -Properties LastLogonDate
    if ($user.LastLogonDate -lt $InactiveThreshold -or $null -eq $user.LastLogonDate) {
        $InactiveAdmins += [PSCustomObject]@{
            Username = $user.SamAccountName
            Name = $user.Name
            LastLogon = $user.LastLogonDate
            Group = $member.Group
        }
    }
}

Write-Host "   ⚠️  $($InactiveAdmins.Count) comptes admin inactifs depuis 90+ jours" -ForegroundColor
Red

# 6. Analyse des contrôleurs de domaine
Write-Host "[6/6] Analyse des contrôleurs de domaine..." -ForegroundColor Yellow

$DomainControllers = Get-ADDomainController -Filter * | Select-Object Name, OperatingSystem, IPv4Address

Write-Host "   ✓ $($DomainControllers.Count) contrôleurs de domaine trouvés" -ForegroundColor Green

# === GÉNÉRATION DES RAPPORTS ===
Write-Host ""
Write-Host "=== Génération des rapports ===" -ForegroundColor Cyan

# Export CSV
if ($ExportCSV) {
    $Tier0Members | Export-Csv -Path "$OutputPath\Tier0_Members.csv" -NoTypeInformation -Encoding UTF8
    $UnprotectedTier0 | Export-Csv -Path "$OutputPath\Tier0_Unprotected.csv" -NoTypeInformation
-Encoding UTF8
    $InactiveAdmins | Export-Csv -Path "$OutputPath\Inactive_Admins.csv" -NoTypeInformation -Encoding
UTF8
    Write-Host "✓ Rapports CSV générés dans: $OutputPath" -ForegroundColor Green
}

# Rapport console
Write-Host ""
Write-Host "=== RÉSUMÉ DE L'AUDIT ===" -ForegroundColor Cyan
Write-Host ""
Write-Host "📊 Statistiques Tier 0:" -ForegroundColor White
Write-Host "   - Comptes privilégiés totaux: $($Tier0Members.Count)" -ForegroundColor White
Write-Host "   - Comptes dans Protected Users: $($ProtectedUsersList.Count)" -ForegroundColor Green
Write-Host "   - Comptes Tier 0 non protégés: $($UnprotectedTier0.Count)" -ForegroundColor $
(if($UnprotectedTier0.Count -gt 0){'Red'}else{'Green'})
Write-Host "   - Comptes avec SPN (Kerberoast): $($Tier0WithSPN.Count)" -ForegroundColor $
(if($Tier0WithSPN.Count -gt 0){'Red'}else{'Green'})
```

```
Write-Host "   - Comptes inactifs (90j+): $($InactiveAdmins.Count)" -ForegroundColor $
(if($InactiveAdmins.Count -gt 0){'Yellow'}else{'Green'})
Write-Host ""
Write-Host "🖥️  Infrastructure:" -ForegroundColor White
Write-Host "   - Contrôleurs de domaine: $($DomainControllers.Count)" -ForegroundColor White
Write-Host ""

# Recommandations
Write-Host "=== RECOMMANDATIONS PRIORITAIRES ===" -ForegroundColor Cyan
Write-Host ""

if ($UnprotectedTier0.Count -gt 0) {
    Write-Host "🔴 CRITIQUE: Ajouter les comptes Tier 0 au groupe Protected Users" -ForegroundColor Red
    Write-Host "   Commande: Add-ADGroupMember -Identity 'Protected Users' -Members <username>"
-ForegroundColor Gray
    Write-Host ""
}

if ($Tier0WithSPN.Count -gt 0) {
    Write-Host "🟡 IMPORTANT: Vérifier les comptes Tier 0 avec SPN" -ForegroundColor Yellow
    Write-Host "   Risque de Kerberoasting sur comptes privilégiés" -ForegroundColor Gray
    Write-Host ""
}

if ($InactiveAdmins.Count -gt 0) {
    Write-Host "🟡 IMPORTANT: Désactiver ou supprimer les comptes admin inactifs" -ForegroundColor
Yellow
    Write-Host "   $($InactiveAdmins.Count) comptes sans connexion depuis 90+ jours" -ForegroundColor
Gray
    Write-Host ""
}

Write-Host "✅ Audit terminé!" -ForegroundColor Green
Write-Host "   Résultats enregistrés dans: $OutputPath" -ForegroundColor White
Write-Host ""

# Retour des résultats
return [PSCustomObject]@{
    Tier0MembersCount = $Tier0Members.Count
    ProtectedUsersCount = $ProtectedUsersList.Count
    UnprotectedTier0Count = $UnprotectedTier0.Count
    Tier0WithSPNCount = $Tier0WithSPN.Count
    InactiveAdminsCount = $InactiveAdmins.Count
    DomainControllersCount = $DomainControllers.Count
}
```

## Verify-LAPS.ps1

Vérifie le déploiement et la conformité LAPS sur tous les postes de travail et serveurs.

- Vérifie extension de schéma
- Liste machines sans LAPS
- Contrôle rotation mots de passe
- Vérifie les permissions AD
- Rapport détaillé de conformité

```
<#
.SYNOPSIS
    Vérification du déploiement et de la conformité LAPS
.DESCRIPTION
```

```
    Audite le déploiement LAPS :
    - Vérifie l'extension de schéma
    - Liste les machines sans LAPS
    - Contrôle la rotation des mots de passe
    - Vérifie les permissions
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
    [string]$OutputPath = "C:\\LAPS\\Audit",
    [int]$MaxPasswordAge = 30
)

Import-Module ActiveDirectory

# Vérification module LAPS
if (-not (Get-Module -ListAvailable -Name AdmPwd.PS)) {
    Write-Warning "Module LAPS (AdmPwd.PS) non trouvé. Installation depuis PowerShell Gallery..."
    try {
        Install-Module -Name AdmPwd.PS -Force -AllowClobber
        Import-Module AdmPwd.PS
    } catch {
        Write-Error "Impossible d'installer le module LAPS. Installez-le manuellement."
        exit 1
    }
} else {
    Import-Module AdmPwd.PS
}

if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== Audit LAPS (Local Administrator Password Solution) ===" -ForegroundColor Cyan
Write-Host ""

# 1. Vérification extension schéma
Write-Host "[1/5] Vérification de l'extension du schéma AD..." -ForegroundColor Yellow

try {
    $schema = Get-ADObject -SearchBase (Get-ADRootDSE).schemaNamingContext \
        -Filter {name -eq "ms-Mcs-AdmPwd"} -ErrorAction Stop

    if ($schema) {
        Write-Host "   ✓ Schéma AD étendu pour LAPS" -ForegroundColor Green
        $schemaExtended = $true
    } else {
        Write-Host "   ✗ Schéma AD NON étendu pour LAPS" -ForegroundColor Red
        Write-Host "     Exécutez: Import-Module AdmPwd.PS; Update-AdmPwdADSchema" -ForegroundColor
Yellow
        $schemaExtended = $false
    }
} catch {
    Write-Host "   ✗ Impossible de vérifier le schéma" -ForegroundColor Red
    $schemaExtended = $false
}

if (-not $schemaExtended) {
    Write-Host ""
    Write-Host "❌ LAPS n'est pas déployé. Arrêt de l'audit." -ForegroundColor Red
    exit 1
}

# 2. Récupération de tous les ordinateurs
Write-Host "[2/5] Récupération de tous les ordinateurs..." -ForegroundColor Yellow

$AllComputers = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd, ms-Mcs-AdmPwdExpirationTime,
```

```
OperatingSystem, LastLogonDate

Write-Host "   ✓ $($AllComputers.Count) ordinateurs trouvés" -ForegroundColor Green

# 3. Analyse des machines avec/sans LAPS
Write-Host "[3/5] Analyse du déploiement LAPS..." -ForegroundColor Yellow

$ComputersWithLAPS = $AllComputers | Where-Object {$_."ms-Mcs-AdmPwd" -ne $null}
$ComputersWithoutLAPS = $AllComputers | Where-Object {$_."ms-Mcs-AdmPwd" -eq $null -and $_.Enabled -eq
$true}

Write-Host "   ✓ Machines avec LAPS: $($ComputersWithLAPS.Count)" -ForegroundColor Green
Write-Host "   ⚠️  Machines SANS LAPS: $($ComputersWithoutLAPS.Count)" -ForegroundColor $
(if($ComputersWithoutLAPS.Count -gt 0){'Red'}else{'Green'})

# 4. Vérification de l'expiration des mots de passe
Write-Host "[4/5] Vérification de l'expiration des mots de passe..." -ForegroundColor Yellow

$ExpiredPasswords = @()
$ExpiringInWeek = @()
$CurrentDate = Get-Date

foreach ($computer in $ComputersWithLAPS) {
    if ($computer."ms-Mcs-AdmPwdExpirationTime") {
        $expirationTime = [DateTime]::FromFileTime($computer."ms-Mcs-AdmPwdExpirationTime")
        $daysUntilExpiration = ($expirationTime - $CurrentDate).Days

        if ($expirationTime -lt $CurrentDate) {
            $ExpiredPasswords += [PSCustomObject]@{
                ComputerName = $computer.Name
                ExpirationDate = $expirationTime
                DaysOverdue = [Math]::Abs($daysUntilExpiration)
            }
        } elseif ($daysUntilExpiration -le 7) {
            $ExpiringInWeek += [PSCustomObject]@{
                ComputerName = $computer.Name
                ExpirationDate = $expirationTime
                DaysRemaining = $daysUntilExpiration
            }
        }
    }
}

Write-Host "   ⚠️  Mots de passe expirés: $($ExpiredPasswords.Count)" -ForegroundColor $
(if($ExpiredPasswords.Count -gt 0){'Red'}else{'Green'})
Write-Host "   ⚠️  Expire dans 7 jours: $($ExpiringInWeek.Count)" -ForegroundColor Yellow

# 5. Vérification des permissions
Write-Host "[5/5] Vérification des permissions LAPS..." -ForegroundColor Yellow

$OUs = Get-ADOrganizationalUnit -Filter * | Select-Object -First 5

$PermissionIssues = @()
foreach ($ou in $OUs) {
    try {
        $perms = Get-AdmPwdPermission -Identity $ou.DistinguishedName -ErrorAction SilentlyContinue
        if (-not $perms) {
            $PermissionIssues += $ou.DistinguishedName
        }
    } catch {
        # Permissions non configurées
    }
}

Write-Host "   ℹ️  Vérification permissions terminée" -ForegroundColor Cyan

# === GÉNÉRATION DU RAPPORT ===
Write-Host ""
Write-Host "=== RAPPORT LAPS ===" -ForegroundColor Cyan
```

```
Write-Host ""

$coveragePercent = [Math]::Round(($ComputersWithLAPS.Count / $AllComputers.Count) * 100, 2)

Write-Host "📊 Déploiement:" -ForegroundColor White
Write-Host "   - Total ordinateurs: $($AllComputers.Count)" -ForegroundColor White
Write-Host "   - Avec LAPS: $($ComputersWithLAPS.Count) ($coveragePercent%)" -ForegroundColor $
(if($coveragePercent -ge 95){'Green'}elseif($coveragePercent -ge 80){'Yellow'}else{'Red'})
Write-Host "   - Sans LAPS: $($ComputersWithoutLAPS.Count)" -ForegroundColor $
(if($ComputersWithoutLAPS.Count -gt 0){'Red'}else{'Green'})
Write-Host ""
Write-Host "🔐 Mots de passe:" -ForegroundColor White
Write-Host "   - Expirés: $($ExpiredPasswords.Count)" -ForegroundColor $(if($ExpiredPasswords.Count -gt
0){'Red'}else{'Green'})
Write-Host "   - Expirent sous 7j: $($ExpiringInWeek.Count)" -ForegroundColor Yellow
Write-Host ""

# Export CSV
$ComputersWithoutLAPS | Export-Csv -Path "$OutputPath\Computers_Without_LAPS.csv" -NoTypeInformation
-Encoding UTF8
$ExpiredPasswords | Export-Csv -Path "$OutputPath\Expired_Passwords.csv" -NoTypeInformation -Encoding
UTF8

Write-Host "✅ Rapport généré dans: $OutputPath" -ForegroundColor Green
Write-Host ""

# Recommandations
if ($ComputersWithoutLAPS.Count -gt 0) {
    Write-Host "🔴 ACTION REQUISE: Déployer LAPS sur $($ComputersWithoutLAPS.Count) machines"
-ForegroundColor Red
    Write-Host "   Liste disponible: $OutputPath\Computers_Without_LAPS.csv" -ForegroundColor Gray
    Write-Host ""
}

if ($ExpiredPasswords.Count -gt 0) {
    Write-Host "🟡 ATTENTION: $($ExpiredPasswords.Count) mots de passe LAPS expirés" -ForegroundColor
Yellow
    Write-Host "   Les machines doivent se reconnecter à AD pour rotation" -ForegroundColor Gray
    Write-Host ""
}

return [PSCustomObject]@{
    TotalComputers = $AllComputers.Count
    WithLAPS = $ComputersWithLAPS.Count
    WithoutLAPS = $ComputersWithoutLAPS.Count
    CoveragePercent = $coveragePercent
    ExpiredPasswords = $ExpiredPasswords.Count
}
```

## Audit-ProtectedUsers.ps1

Audite le groupe Protected Users et identifie les comptes Tier 0 qui devraient y être ajoutés.

- Liste membres actuels
- Identifie comptes Tier 0 manquants
- Vérifie compatibilité applications
- Test pré-ajout automatique
- Recommandations d'ajout

```
<#
.SYNOPSIS
    Audit du groupe Protected Users et recommandations
.DESCRIPTION
    Audite le groupe Protected Users et identifie les comptes Tier 0
    qui devraient y être ajoutés
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
    [string]$OutputPath = "C:\\ADTiering\\ProtectedUsers",
    [switch]$TestMode
)

Import-Module ActiveDirectory

if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== Audit Protected Users Group ===" -ForegroundColor Cyan
Write-Host ""

# Vérification niveau fonctionnel
$domain = Get-ADDomain
$domainLevel = $domain.DomainMode

Write-Host "[1/4] Vérification prérequis..." -ForegroundColor Yellow

if ($domainLevel -lt "Windows2012R2Domain") {
    Write-Host "   ✗ Niveau fonctionnel insuffisant: $domainLevel" -ForegroundColor Red
    Write-Host "     Protected Users requis Windows Server 2012 R2 minimum" -ForegroundColor Yellow
    exit 1
} else {
    Write-Host "   ✓ Niveau fonctionnel compatible: $domainLevel" -ForegroundColor Green
}

# Membres actuels de Protected Users
Write-Host "[2/4] Analyse des membres actuels..." -ForegroundColor Yellow

try {
    $ProtectedUsers = Get-ADGroupMember -Identity "Protected Users" -ErrorAction Stop
    $ProtectedUserAccounts = $ProtectedUsers | Where-Object {$_.objectClass -eq 'user'}
    Write-Host "   ✓ $($ProtectedUserAccounts.Count) comptes dans Protected Users" -ForegroundColor
Green
} catch {
    Write-Host "   ✗ Impossible de lire Protected Users" -ForegroundColor Red
    exit 1
}

# Identification des comptes Tier 0
Write-Host "[3/4] Identification des comptes Tier 0..." -ForegroundColor Yellow

$Tier0Groups = @(
    "Domain Admins",
    "Enterprise Admins",
    "Schema Admins",
    "Administrators",
    "Account Operators",
    "Backup Operators",
    "Server Operators"
)

$AllTier0Users = @()
foreach ($group in $Tier0Groups) {
    try {
```

```
        $members = Get-ADGroupMember -Identity $group -Recursive -ErrorAction SilentlyContinue
        foreach ($member in $members) {
            if ($member.objectClass -eq 'user') {
                $user = Get-ADUser $member -Properties Enabled, LastLogonDate, ServicePrincipalName
                $AllTier0Users += [PSCustomObject]@{
                    SamAccountName = $user.SamAccountName
                    Name = $user.Name
                    Group = $group
                    Enabled = $user.Enabled
                    LastLogon = $user.LastLogonDate
                    HasSPN = ($null -ne $user.ServicePrincipalName -and $user.ServicePrincipalName.Count
-gt 0)
                }
            }
        }
    } catch {
        Write-Warning "Impossible de lire: $group"
    }
}

$UniqueTier0Users = $AllTier0Users | Select-Object SamAccountName, Name, Enabled, LastLogon, HasSPN
-Unique

Write-Host "   ✓ $($UniqueTier0Users.Count) comptes Tier 0 uniques identifiés" -ForegroundColor Green

# Identification des comptes manquants
Write-Host "[4/4] Identification des comptes à ajouter..." -ForegroundColor Yellow

$protectedUsernames = $ProtectedUserAccounts | Select-Object -ExpandProperty SamAccountName

$MissingFromProtected = $UniqueTier0Users | Where-Object {
    $_.SamAccountName -notin $protectedUsernames -and
    $_.Enabled -eq $true -and
    $_.SamAccountName -ne "Administrator" # Ne jamais ajouter le compte Administrator intégré
}

Write-Host "   ⚠️  $($MissingFromProtected.Count) comptes Tier 0 manquants" -ForegroundColor $
(if($MissingFromProtected.Count -gt 0){'Red'}else{'Green'})

# === RAPPORT ===
Write-Host ""
Write-Host "=== RAPPORT PROTECTED USERS ===" -ForegroundColor Cyan
Write-Host ""
Write-Host "📊 Statistiques:" -ForegroundColor White
Write-Host "   - Comptes Tier 0 totaux: $($UniqueTier0Users.Count)" -ForegroundColor White
Write-Host "   - Dans Protected Users: $($ProtectedUserAccounts.Count)" -ForegroundColor Green
Write-Host "   - Manquants: $($MissingFromProtected.Count)" -ForegroundColor $
(if($MissingFromProtected.Count -gt 0){'Red'}else{'Green'})
Write-Host ""

if ($MissingFromProtected.Count -gt 0) {
    Write-Host "🔴 COMPTES À AJOUTER À PROTECTED USERS:" -ForegroundColor Red
    Write-Host ""

    $MissingFromProtected | ForEach-Object {
        $warning = ""
        if ($_.HasSPN) {
            $warning = " ⚠️  HAS SPN - TEST FIRST"
        }
        Write-Host "   - $($_.SamAccountName) ($($_.Name))$warning" -ForegroundColor Yellow
    }

    Write-Host ""
    Write-Host "📝 Commandes pour ajouter (TESTEZ D'ABORD!):" -ForegroundColor Cyan
    $MissingFromProtected | ForEach-Object {
        if (-not $_.HasSPN) {
            Write-Host "   Add-ADGroupMember -Identity 'Protected Users' -Members $($_.SamAccountName)"
-ForegroundColor Gray
        }
```

```
    }

    Write-Host ""
    Write-Host "⚠️  ATTENTION - Comptes avec SPN:" -ForegroundColor Yellow
    $WithSPN = $MissingFromProtected | Where-Object {$_.HasSPN}
    if ($WithSPN) {
        Write-Host "   Les comptes suivants ont des SPN et nécessitent des tests approfondis:"
-ForegroundColor Yellow
        $WithSPN | ForEach-Object {
            Write-Host "   - $($_.SamAccountName)" -ForegroundColor Red
        }
        Write-Host "   Protected Users bloque NTLM, DES, RC4. Vérifiez la compatibilité applicative!"
-ForegroundColor Yellow
    }
}

# Export CSV
$MissingFromProtected | Export-Csv -Path "$OutputPath\Missing_From_Protected_Users.csv"
-NoTypeInformation -Encoding UTF8
$ProtectedUserAccounts | Export-Csv -Path "$OutputPath\Current_Protected_Users.csv" -NoTypeInformation
-Encoding UTF8

Write-Host ""
Write-Host "✅ Rapport généré: $OutputPath" -ForegroundColor Green
Write-Host ""

# Restrictions de Protected Users
Write-Host "=== RAPPEL - Restrictions Protected Users ===" -ForegroundColor Cyan
Write-Host "Les comptes dans Protected Users ont les restrictions suivantes:" -ForegroundColor White
Write-Host "   ✗ Pas de NTLM" -ForegroundColor Yellow
Write-Host "   ✗ Pas de DES ou RC4 pour Kerberos" -ForegroundColor Yellow
Write-Host "   ✗ Durée de vie TGT: 4 heures max (vs 10h par défaut)" -ForegroundColor Yellow
Write-Host "   ✗ Pas de délégation Kerberos" -ForegroundColor Yellow
Write-Host "   ✗ Pas de cache credentials" -ForegroundColor Yellow
Write-Host ""
Write-Host "⚠️  TESTEZ en environnement de LAB avant la production!" -ForegroundColor Red
Write-Host ""

return [PSCustomObject]@{
    Tier0Total = $UniqueTier0Users.Count
    InProtectedUsers = $ProtectedUserAccounts.Count
    MissingCount = $MissingFromProtected.Count
    WithSPNCount = ($MissingFromProtected | Where-Object {$_.HasSPN}).Count
}
```

## Test-TieringCompliance.ps1

Vérifie la conformité de votre implémentation avec les bonnes pratiques du tiering.

- Score de conformité global
- Vérifie séparation des tiers
- Détecte violations inter-tiers
- Dashboard visuel
- Plan d'action priorisé

```
<#
.SYNOPSIS
    Vérifie la conformité du modèle de tiering
.DESCRIPTION
    Calcule un score de conformité et identifie les violations
```

```
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
    [string]$OutputPath = "C:\\ADTiering\\Compliance"
)

Import-Module ActiveDirectory

if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== Test de Conformité Tiering ===" -ForegroundColor Cyan
Write-Host ""

$ComplianceScore = 0
$TotalChecks = 0
$Issues = @()

# Check 1: Protected Users déployé
Write-Host "[1/10] Vérification Protected Users..." -ForegroundColor Yellow
$TotalChecks++

try {
    $ProtectedUsers = Get-ADGroupMember -Identity "Protected Users" -ErrorAction Stop
    if ($ProtectedUsers.Count -gt 0) {
        Write-Host "   ✓ Protected Users configuré ($($ProtectedUsers.Count) membres)" -ForegroundColor
Green
        $ComplianceScore++
    } else {
        Write-Host "   ✗ Protected Users vide" -ForegroundColor Red
        $Issues += "Protected Users group has no members"
    }
} catch {
    Write-Host "   ✗ Protected Users non accessible" -ForegroundColor Red
    $Issues += "Cannot access Protected Users group"
}

# Check 2: LAPS déployé
Write-Host "[2/10] Vérification LAPS..." -ForegroundColor Yellow
$TotalChecks++

try {
    $schema = Get-ADObject -SearchBase (Get-ADRootDSE).schemaNamingContext \
        -Filter {name -eq "ms-Mcs-AdmPwd"} -ErrorAction Stop
    if ($schema) {
        Write-Host "   ✓ LAPS déployé (schéma étendu)" -ForegroundColor Green
        $ComplianceScore++
    } else {
        Write-Host "   ✗ LAPS non déployé" -ForegroundColor Red
        $Issues += "LAPS schema not extended"
    }
} catch {
    Write-Host "   ✗ LAPS non vérifié" -ForegroundColor Red
    $Issues += "Cannot verify LAPS deployment"
}

# Check 3: Audit avancé activé
Write-Host "[3/10] Vérification de l'audit avancé..." -ForegroundColor Yellow
$TotalChecks++

$AuditGPO = Get-GPO -Name "Advanced Audit Policy" -ErrorAction SilentlyContinue
if ($AuditGPO) {
    Write-Host "   ✓ GPO d'audit avancé trouvée" -ForegroundColor Green
    $ComplianceScore++
} else {
```

```
    Write-Host "   ⚠️  GPO d'audit avancé non trouvée" -ForegroundColor Yellow
    $Issues += "Advanced Audit Policy GPO not found"
}

# Check 4: Nombre de Domain Admins
Write-Host "[4/10] Vérification du nombre de Domain Admins..." -ForegroundColor Yellow
$TotalChecks++

$DomainAdmins = Get-ADGroupMember -Identity "Domain Admins"
if ($DomainAdmins.Count -le 5) {
    Write-Host "   ✓ Domain Admins limité ($($DomainAdmins.Count) membres)" -ForegroundColor Green
    $ComplianceScore++
} else {
    Write-Host "   ✗ Trop de Domain Admins ($($DomainAdmins.Count) membres)" -ForegroundColor Red
    $Issues += "Too many Domain Admins: $($DomainAdmins.Count) (recommended: <= 5)"
}

# Check 5: Compte Administrator renommé
Write-Host "[5/10] Vérification renommage compte Administrator..." -ForegroundColor Yellow
$TotalChecks++

$BuiltinAdmin = Get-ADUser -Filter {SID -like "*-500"} -Properties SamAccountName
if ($BuiltinAdmin.SamAccountName -ne "Administrator") {
    Write-Host "   ✓ Compte Administrator renommé ($($BuiltinAdmin.SamAccountName))" -ForegroundColor
Green
    $ComplianceScore++
} else {
    Write-Host "   ⚠️  Compte Administrator non renommé" -ForegroundColor Yellow
    $Issues += "Built-in Administrator account not renamed"
}

# Check 6: Présence d'OUs Tier 0/1/2
Write-Host "[6/10] Vérification structure OU tiering..." -ForegroundColor Yellow
$TotalChecks++

$Tier0OU = Get-ADOrganizationalUnit -Filter {Name -like "*Tier*0*"} -ErrorAction SilentlyContinue
$Tier1OU = Get-ADOrganizationalUnit -Filter {Name -like "*Tier*1*"} -ErrorAction SilentlyContinue
$Tier2OU = Get-ADOrganizationalUnit -Filter {Name -like "*Tier*2*"} -ErrorAction SilentlyContinue

if ($Tier0OU -and $Tier1OU -and $Tier2OU) {
    Write-Host "   ✓ Structure OU tiering présente" -ForegroundColor Green
    $ComplianceScore++
} else {
    Write-Host "   ✗ Structure OU tiering incomplète" -ForegroundColor Red
    $Issues += "Tiering OU structure incomplete or not found"
}

# Check 7: Comptes de service avec SPN
Write-Host "[7/10] Vérification comptes de service..." -ForegroundColor Yellow
$TotalChecks++

$ServiceAccountsWithSPN = Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties
ServicePrincipalName
$PrivilegedWithSPN = $ServiceAccountsWithSPN | Where-Object {
    $userGroups = (Get-ADUser $_ -Properties MemberOf).MemberOf
    $userGroups -match "Domain Admins|Enterprise Admins|Administrators"
}

if ($PrivilegedWithSPN.Count -eq 0) {
    Write-Host "   ✓ Aucun compte privilégié avec SPN" -ForegroundColor Green
    $ComplianceScore++
} else {
    Write-Host "   ✗ $($PrivilegedWithSPN.Count) comptes privilégiés avec SPN (Kerberoasting)"
-ForegroundColor Red
    $Issues += "$($PrivilegedWithSPN.Count) privileged accounts with SPN (Kerberoasting risk)"
}

# Check 8: Comptes admin inactifs
Write-Host "[8/10] Vérification comptes admin inactifs..." -ForegroundColor Yellow
```

```
$TotalChecks++

$InactiveThreshold = (Get-Date).AddDays(-90)
$InactiveAdmins = Get-ADUser -Filter {AdminCount -eq 1 -and Enabled -eq $true} -Properties LastLogonDate
|
    Where-Object {$_.LastLogonDate -lt $InactiveThreshold -or $null -eq $_.LastLogonDate}

if ($InactiveAdmins.Count -eq 0) {
    Write-Host "   ✓ Aucun compte admin inactif" -ForegroundColor Green
    $ComplianceScore++
} else {
    Write-Host "   ✗ $($InactiveAdmins.Count) comptes admin inactifs (90j+)" -ForegroundColor Red
    $Issues += "$($InactiveAdmins.Count) inactive admin accounts"
}

# Check 9: Niveau fonctionnel domaine
Write-Host "[9/10] Vérification niveau fonctionnel..." -ForegroundColor Yellow
$TotalChecks++

$domain = Get-ADDomain
if ($domain.DomainMode -ge "Windows2012R2Domain") {
    Write-Host "   ✓ Niveau fonctionnel compatible ($($domain.DomainMode))" -ForegroundColor Green
    $ComplianceScore++
} else {
    Write-Host "   ✗ Niveau fonctionnel insuffisant ($($domain.DomainMode))" -ForegroundColor Red
    $Issues += "Domain functional level too low: $($domain.DomainMode)"
}

# Check 10: GPO de durcissement
Write-Host "[10/10] Vérification GPO de sécurité..." -ForegroundColor Yellow
$TotalChecks++

$SecurityGPOs = @("PAW", "Tier 0", "Tier 1", "Tier 2")
$FoundGPOs = 0
foreach ($gpoName in $SecurityGPOs) {
    if (Get-GPO -Name "*$gpoName*" -ErrorAction SilentlyContinue) {
        $FoundGPOs++
    }
}

if ($FoundGPOs -ge 2) {
    Write-Host "   ✓ GPO de sécurité trouvées ($FoundGPOs)" -ForegroundColor Green
    $ComplianceScore++
} else {
    Write-Host "   ⚠️  Peu de GPO de sécurité ($FoundGPOs)" -ForegroundColor Yellow
    $Issues += "Few security GPOs found: $FoundGPOs"
}

# === CALCUL DU SCORE ===
$CompliancePercent = [Math]::Round(($ComplianceScore / $TotalChecks) * 100, 2)

Write-Host ""
Write-Host "=== RÉSULTAT DE CONFORMITÉ ===" -ForegroundColor Cyan
Write-Host ""
Write-Host "📊 Score: $ComplianceScore / $TotalChecks ($CompliancePercent%)" -ForegroundColor $(
    if ($CompliancePercent -ge 80) {'Green'}
    elseif ($CompliancePercent -ge 60) {'Yellow'}
    else {'Red'}
)
Write-Host ""

if ($CompliancePercent -ge 80) {
    Write-Host "✅ EXCELLENT - Votre tiering est bien configuré!" -ForegroundColor Green
} elseif ($CompliancePercent -ge 60) {
    Write-Host "⚠️  MOYEN - Plusieurs améliorations nécessaires" -ForegroundColor Yellow
} else {
    Write-Host "🔴 INSUFFISANT - Travail important requis" -ForegroundColor Red
}
```

```
Write-Host ""
Write-Host "=== PROBLÈMES IDENTIFIÉS ($($Issues.Count)) ===" -ForegroundColor Cyan
$Issues | ForEach-Object {
    Write-Host "   • $_" -ForegroundColor Red
}

# Export
$Report = [PSCustomObject]@{
    Date = Get-Date
    ComplianceScore = $ComplianceScore
    TotalChecks = $TotalChecks
    CompliancePercent = $CompliancePercent
    Issues = $Issues -join "; "
}

$Report | Export-Csv -Path "$OutputPath\Compliance_Report.csv" -NoTypeInformation -Encoding UTF8

Write-Host ""
Write-Host "✅ Rapport généré: $OutputPath\Compliance_Report.csv" -ForegroundColor Green

return $Report
```

## Invoke-BloodHoundCollection.ps1

Automatise la collecte de données BloodHound avec les bonnes pratiques de sécurité.

- Télécharge SharpHound automatiquement
- Configuration optimisée
- Collection sécurisée
- Archivage automatique des résultats
- Planification possible

```
<#
.SYNOPSIS
    Collection automatisée de données BloodHound
.DESCRIPTION
    Télécharge SharpHound, collecte les données AD et archive les résultats
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
    [string]$OutputPath = "C:\\BloodHound",
    [string]$CollectionMethod = "All",
    [switch]$Stealth
)

# Création du dossier
if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== BloodHound Data Collection ===" -ForegroundColor Cyan
Write-Host ""

# Téléchargement de SharpHound
Write-Host "[1/3] Téléchargement de SharpHound..." -ForegroundColor Yellow

$SharpHoundURL = "https://github.com/BloodHoundAD/BloodHound/raw/master/Collectors/SharpHound.exe"
```

```
$SharpHoundPath = Join-Path $OutputPath "SharpHound.exe"

try {
    if (-not (Test-Path $SharpHoundPath)) {
        Invoke-WebRequest -Uri $SharpHoundURL -OutFile $SharpHoundPath -UseBasicParsing
        Write-Host "   ✓ SharpHound téléchargé" -ForegroundColor Green
    } else {
        Write-Host "   ✓ SharpHound déjà présent" -ForegroundColor Green
    }
} catch {
    Write-Host "   ✗ Erreur de téléchargement" -ForegroundColor Red
    Write-Host "   Téléchargez manuellement depuis: $SharpHoundURL" -ForegroundColor Yellow
    exit 1
}

# Collection des données
Write-Host "[2/3] Collection des données AD..." -ForegroundColor Yellow

$timestamp = Get-Date -Format "yyyyMMdd_HHmmss"
$collectionArgs = "-c $CollectionMethod --outputdirectory \"$OutputPath\" --outputprefix
\"BH_$timestamp\""

if ($Stealth) {
    $collectionArgs += " --Stealth"
}

try {
    $process = Start-Process -FilePath $SharpHoundPath -ArgumentList $collectionArgs -Wait -PassThru
-NoNewWindow

    if ($process.ExitCode -eq 0) {
        Write-Host "   ✓ Collection terminée" -ForegroundColor Green
    } else {
        Write-Host "   ⚠️  Collection terminée avec avertissements (code: $($process.ExitCode))"
-ForegroundColor Yellow
    }
} catch {
    Write-Host "   ✗ Erreur lors de la collection" -ForegroundColor Red
    Write-Error $_.Exception.Message
    exit 1
}

# Archivage
Write-Host "[3/3] Archivage des résultats..." -ForegroundColor Yellow

$zipFiles = Get-ChildItem -Path $OutputPath -Filter "*.zip"
if ($zipFiles.Count -gt 0) {
    Write-Host "   ✓ $($zipFiles.Count) fichier(s) généré(s)" -ForegroundColor Green

    # Créer un dossier d'archive
    $archiveFolder = Join-Path $OutputPath "Archive_$timestamp"
    New-Item -Path $archiveFolder -ItemType Directory | Out-Null

    # Copier les anciens ZIP dans l'archive
    $oldZips = Get-ChildItem -Path $OutputPath -Filter "*.zip" | Where-Object {$_.Name -notlike
"*$timestamp*"}
    if ($oldZips) {
        $oldZips | Move-Item -Destination $archiveFolder
        Write-Host "   ✓ $($oldZips.Count) ancien(s) fichier(s) archivé(s)" -ForegroundColor Green
    }
} else {
    Write-Host "   ⚠️  Aucun fichier ZIP généré" -ForegroundColor Yellow
}

# Résumé
Write-Host ""
Write-Host "=== COLLECTION TERMINÉE ===" -ForegroundColor Cyan
Write-Host ""
Write-Host "📁 Résultats:" -ForegroundColor White
```

```
Write-Host "   Dossier: $OutputPath" -ForegroundColor Gray
$newZip = Get-ChildItem -Path $OutputPath -Filter "*$timestamp*.zip" | Select-Object -First 1
if ($newZip) {
    Write-Host "   Fichier: $($newZip.Name)" -ForegroundColor Gray
    Write-Host "   Taille: $([Math]::Round($newZip.Length / 1MB, 2)) MB" -ForegroundColor Gray
}
Write-Host ""
Write-Host "📊 Prochaines étapes:" -ForegroundColor White
Write-Host "   1. Téléchargez et installez BloodHound GUI" -ForegroundColor Gray
Write-Host "   2. Importez le fichier ZIP dans BloodHound" -ForegroundColor Gray
Write-Host "   3. Analysez les chemins d'attaque vers Tier 0" -ForegroundColor Gray
Write-Host ""
Write-Host "🔍 Requêtes recommandées dans BloodHound:" -ForegroundColor White
Write-Host "   • Shortest Paths to Domain Admins" -ForegroundColor Gray
Write-Host "   • Find Principals with DCSync Rights" -ForegroundColor Gray
Write-Host "   • Find Computers where Domain Users are Local Admin" -ForegroundColor Gray
Write-Host "   • Find Dangerous Privileges for Domain Users Group" -ForegroundColor Gray
Write-Host ""
Write-Host "⚠️  IMPORTANT: Sécurisez ces fichiers!" -ForegroundColor Yellow
Write-Host "   Ils contiennent une cartographie complète de votre AD" -ForegroundColor Yellow
Write-Host ""

Write-Host "✅ Collection BloodHound terminée!" -ForegroundColor Green
```

## Audit-TieringGPO.ps1

Vérifie que vos GPO respectent les bonnes pratiques de sécurité pour chaque tier.

- Liste toutes les GPO par tier
- Vérifie configurations critiques
- Détecte GPO dangereuses
- Analyse des permissions
- Rapport de conformité

```
<#
.SYNOPSIS
    Audit des GPO pour le tiering
.DESCRIPTION
    Vérifie que les GPO respectent les bonnes pratiques de sécurité
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
    [string]$OutputPath = "C:\\ADTiering\\GPO_Audit"
)

Import-Module GroupPolicy
Import-Module ActiveDirectory

if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== Audit GPO Tiering ===" -ForegroundColor Cyan
Write-Host ""

# Récupération de toutes les GPO
Write-Host "[1/4] Récupération de toutes les GPO..." -ForegroundColor Yellow
```

```
$AllGPOs = Get-GPO -All
Write-Host "   ✓ $($AllGPOs.Count) GPO trouvées" -ForegroundColor Green

# Catégorisation des GPO par Tier (basé sur le nom ou OU de liaison)
Write-Host "[2/4] Catégorisation des GPO..." -ForegroundColor Yellow

$GPOsByTier = @{
    Tier0 = @()
    Tier1 = @()
    Tier2 = @()
    Unknown = @()
}

foreach ($gpo in $AllGPOs) {
    if ($gpo.DisplayName -match "Tier.*0|PAW|DC|Domain.Controller") {
        $GPOsByTier.Tier0 += $gpo
    } elseif ($gpo.DisplayName -match "Tier.*1|Server") {
        $GPOsByTier.Tier1 += $gpo
    } elseif ($gpo.DisplayName -match "Tier.*2|Workstation|Desktop") {
        $GPOsByTier.Tier2 += $gpo
    } else {
        $GPOsByTier.Unknown += $gpo
    }
}

Write-Host "   Tier 0: $($GPOsByTier.Tier0.Count) GPO" -ForegroundColor Red
Write-Host "   Tier 1: $($GPOsByTier.Tier1.Count) GPO" -ForegroundColor Green
Write-Host "   Tier 2: $($GPOsByTier.Tier2.Count) GPO" -ForegroundColor Blue
Write-Host "   Non catégorisée: $($GPOsByTier.Unknown.Count) GPO" -ForegroundColor Yellow

# Vérification des GPO critiques
Write-Host "[3/4] Vérification des GPO de sécurité requises..." -ForegroundColor Yellow

$RequiredGPOs = @(
    "PAW",
    "Tier 0",
    "LAPS",
    "Audit",
    "Credential Guard"
)

$MissingGPOs = @()
foreach ($required in $RequiredGPOs) {
    $found = $AllGPOs | Where-Object {$_.DisplayName -like "*$required*"}
    if (-not $found) {
        $MissingGPOs += $required
    }
}

if ($MissingGPOs.Count -eq 0) {
    Write-Host "   ✓ Toutes les GPO critiques présentes" -ForegroundColor Green
} else {
    Write-Host "   ⚠️  GPO manquantes: $($MissingGPOs -join ', ')" -ForegroundColor Red
}

# Analyse des permissions GPO
Write-Host "[4/4] Analyse des permissions GPO..." -ForegroundColor Yellow

$DangerousPermissions = @()
foreach ($gpo in $GPOsByTier.Tier0) {
    $permissions = Get-GPPermission -Guid $gpo.Id -All

    $domainUsers = $permissions | Where-Object {
        $_.Trustee.Name -eq "Domain Users" -and $_.Permission -match "Edit|Modify"
    }

    if ($domainUsers) {
        $DangerousPermissions += [PSCustomObject]@{
```

```
            GPOName = $gpo.DisplayName
            Issue = "Domain Users has edit rights on Tier 0 GPO"
            Severity = "CRITICAL"
        }
    }
}

if ($DangerousPermissions.Count -eq 0) {
    Write-Host "   ✓ Aucune permission dangereuse détectée" -ForegroundColor Green
} else {
    Write-Host "   ✗ $($DangerousPermissions.Count) problèmes de permissions" -ForegroundColor Red
}

# === RAPPORT ===
Write-Host ""
Write-Host "=== RAPPORT GPO ===" -ForegroundColor Cyan
Write-Host ""
Write-Host "📊 Distribution des GPO:" -ForegroundColor White
Write-Host "   Tier 0: $($GPOsByTier.Tier0.Count)" -ForegroundColor Red
Write-Host "   Tier 1: $($GPOsByTier.Tier1.Count)" -ForegroundColor Green
Write-Host "   Tier 2: $($GPOsByTier.Tier2.Count)" -ForegroundColor Blue
Write-Host "   Non catégorisée: $($GPOsByTier.Unknown.Count)" -ForegroundColor Yellow
Write-Host ""

if ($MissingGPOs.Count -gt 0) {
    Write-Host "🔴 GPO MANQUANTES:" -ForegroundColor Red
    $MissingGPOs | ForEach-Object {
        Write-Host "   - $_" -ForegroundColor Yellow
    }
    Write-Host ""
}

if ($DangerousPermissions.Count -gt 0) {
    Write-Host "🔴 PERMISSIONS DANGEREUSES:" -ForegroundColor Red
    $DangerousPermissions | ForEach-Object {
        Write-Host "   - $($_.GPOName): $($_.Issue)" -ForegroundColor Red
    }
    Write-Host ""
}

# Export
$AllGPOs | Select-Object DisplayName, CreationTime, ModificationTime, GpoStatus |
    Export-Csv -Path "$OutputPath\All_GPOs.csv" -NoTypeInformation -Encoding UTF8

$DangerousPermissions | Export-Csv -Path "$OutputPath\Dangerous_Permissions.csv" -NoTypeInformation
-Encoding UTF8

Write-Host "✅ Rapport généré: $OutputPath" -ForegroundColor Green
```

## Test-CredentialGuard.ps1

Vérifie si Credential Guard est activé et fonctionne correctement sur vos systèmes critiques.

- Test prérequis matériels
- Vérifie activation CG
- Test Remote Credential Guard
- Diagnostic complet
- Guide de correction

```
<#
.SYNOPSIS
    Vérifie Credential Guard et Remote Credential Guard
.DESCRIPTION
    Teste les prérequis et le statut de Credential Guard
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
    [string]$OutputPath = "C:\\ADTiering\\CredentialGuard"
)

if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== Vérification Credential Guard ===" -ForegroundColor Cyan
Write-Host ""

$Results = @{
    ComputerName = $env:COMPUTERNAME
    Timestamp = Get-Date
    Checks = @()
}

# Check 1: Version Windows
Write-Host "[1/6] Vérification version Windows..." -ForegroundColor Yellow

$OS = Get-CimInstance Win32_OperatingSystem
$IsCompatible = $false

if ($OS.Caption -match "Windows 10|Windows 11|Server 2016|Server 2019|Server 2022") {
    Write-Host "   ✓ OS compatible: $($OS.Caption)" -ForegroundColor Green
    $IsCompatible = $true
    $Results.Checks += "OS_Compatible"
} else {
    Write-Host "   ✗ OS incompatible: $($OS.Caption)" -ForegroundColor Red
    $Results.Checks += "OS_Incompatible"
}

# Check 2: UEFI et Secure Boot
Write-Host "[2/6] Vérification UEFI et Secure Boot..." -ForegroundColor Yellow

try {
    $SecureBoot = Confirm-SecureBootUEFI
    if ($SecureBoot) {
        Write-Host "   ✓ Secure Boot activé" -ForegroundColor Green
        $Results.Checks += "SecureBoot_Enabled"
    } else {
        Write-Host "   ✗ Secure Boot désactivé" -ForegroundColor Red
        $Results.Checks += "SecureBoot_Disabled"
    }
} catch {
    Write-Host "   ✗ UEFI non disponible (BIOS Legacy?)" -ForegroundColor Red
    $Results.Checks += "UEFI_NotAvailable"
}

# Check 3: Virtualisation
Write-Host "[3/6] Vérification support virtualisation..." -ForegroundColor Yellow

$Processor = Get-CimInstance Win32_Processor
if ($Processor.VirtualizationFirmwareEnabled) {
    Write-Host "   ✓ Virtualisation activée dans firmware" -ForegroundColor Green
    $Results.Checks += "Virtualization_Enabled"
} else {
    Write-Host "   ✗ Virtualisation désactivée" -ForegroundColor Red
```

```
    $Results.Checks += "Virtualization_Disabled"
}

# Check 4: Credential Guard activé
Write-Host "[4/6] Vérification statut Credential Guard..." -ForegroundColor Yellow

$DeviceGuard = Get-CimInstance -ClassName Win32_DeviceGuard -Namespace
root\Microsoft\Windows\DeviceGuard -ErrorAction SilentlyContinue

if ($DeviceGuard) {
    $CGStatus = $DeviceGuard.SecurityServicesRunning

    # 1 = Credential Guard running
    if ($CGStatus -contains 1) {
        Write-Host "   ✓ Credential Guard ACTIF" -ForegroundColor Green
        $Results.Checks += "CredentialGuard_Running"
        $Results.CredentialGuardStatus = "Running"
    } else {
        Write-Host "   ✗ Credential Guard non actif" -ForegroundColor Red
        $Results.Checks += "CredentialGuard_NotRunning"
        $Results.CredentialGuardStatus = "Not Running"
    }

    # Configuration
    $CGConfig = $DeviceGuard.SecurityServicesConfigured
    if ($CGConfig -contains 1) {
        Write-Host "   ✓ Credential Guard configuré" -ForegroundColor Green
        $Results.Checks += "CredentialGuard_Configured"
    }
} else {
    Write-Host "   ⚠️  Impossible de vérifier le statut" -ForegroundColor Yellow
    $Results.CredentialGuardStatus = "Unknown"
}

# Check 5: Remote Credential Guard
Write-Host "[5/6] Vérification Remote Credential Guard..." -ForegroundColor Yellow

# Vérifier via registre
$RCGKey = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"
$DisableRestrictedAdmin = Get-ItemProperty -Path $RCGKey -Name "DisableRestrictedAdmin" -ErrorAction
SilentlyContinue

if ($DisableRestrictedAdmin.DisableRestrictedAdmin -eq 0) {
    Write-Host "   ✓ Remote Credential Guard disponible" -ForegroundColor Green
    $Results.Checks += "RCG_Available"
} else {
    Write-Host "   ⚠️  Remote Credential Guard non configuré" -ForegroundColor Yellow
    $Results.Checks += "RCG_NotConfigured"
}

# Check 6: TPM
Write-Host "[6/6] Vérification TPM..." -ForegroundColor Yellow

$TPM = Get-Tpm -ErrorAction SilentlyContinue
if ($TPM -and $TPM.TpmPresent) {
    Write-Host "   ✓ TPM présent et activé (version $($TPM.ManufacturerVersion))" -ForegroundColor Green
    $Results.Checks += "TPM_Present"
} else {
    Write-Host "   ⚠️  TPM non disponible (recommandé mais pas obligatoire)" -ForegroundColor Yellow
    $Results.Checks += "TPM_NotPresent"
}

# === RAPPORT ===
Write-Host ""
Write-Host "=== RAPPORT CREDENTIAL GUARD ===" -ForegroundColor Cyan
Write-Host ""
Write-Host "💻 Système: $($OS.Caption)" -ForegroundColor White
Write-Host "🛡️  Credential Guard: $($Results.CredentialGuardStatus)" -ForegroundColor $(
    if ($Results.CredentialGuardStatus -eq "Running") {'Green'} else {'Red'}
```

```
)
Write-Host ""

# Recommandations
if ($Results.CredentialGuardStatus -ne "Running") {
    Write-Host "=== ACTIONS POUR ACTIVER CREDENTIAL GUARD ===" -ForegroundColor Cyan
    Write-Host ""

    if ($Results.Checks -notcontains "SecureBoot_Enabled") {
        Write-Host "1. Activer Secure Boot dans le BIOS/UEFI" -ForegroundColor Yellow
    }

    if ($Results.Checks -notcontains "Virtualization_Enabled") {
        Write-Host "2. Activer VT-x (Intel) ou AMD-V dans le BIOS/UEFI" -ForegroundColor Yellow
    }

    Write-Host "3. Activer Credential Guard via GPO:" -ForegroundColor Yellow
    Write-Host "   Computer Configuration > Policies > Administrative Templates >" -ForegroundColor Gray
    Write-Host "   System > Device Guard > Turn On Virtualization Based Security" -ForegroundColor Gray
    Write-Host "   → Activé avec Secure Boot et DMA Protection" -ForegroundColor Gray
    Write-Host ""
    Write-Host "   Ou via PowerShell:" -ForegroundColor Yellow
    Write-Host '   New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard" -Name
"EnableVirtualizationBasedSecurity" -Value 1 -PropertyType DWORD -Force' -ForegroundColor Gray
    Write-Host '   New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name
"LsaCfgFlags" -Value 1 -PropertyType DWORD -Force' -ForegroundColor Gray
    Write-Host ""
    Write-Host "4. Redémarrer le système" -ForegroundColor Yellow
    Write-Host ""
}

# Test Remote Credential Guard
Write-Host "=== TEST REMOTE CREDENTIAL GUARD ===" -ForegroundColor Cyan
Write-Host "Pour utiliser RCG lors d'une connexion RDP:" -ForegroundColor White
Write-Host '   mstsc.exe /v:servername /remoteGuard' -ForegroundColor Gray
Write-Host ""
Write-Host "Ou via GPO:" -ForegroundColor White
Write-Host "   Computer Configuration > Policies > Administrative Templates >" -ForegroundColor Gray
Write-Host "   System > Credentials Delegation > Restrict delegation of credentials to remote servers"
-ForegroundColor Gray
Write-Host ""

# Export
$Results | Export-Clixml -Path "$OutputPath\CredentialGuard_Report.xml"

Write-Host "✅ Rapport généré: $OutputPath\CredentialGuard_Report.xml" -ForegroundColor Green

return $Results
```

## Audit-NTLMUsage.ps1

Identifie les utilisations de NTLM pour préparer sa désactivation sur le Tier 0.

- Analyse logs NTLM
- Liste applications utilisant NTLM
- Identifie comptes concernés
- Plan de migration vers Kerberos
- Statistiques d'usage

```
<#
.SYNOPSIS
    Audit de l'utilisation NTLM
.DESCRIPTION
    Analyse les logs pour identifier l'utilisation de NTLM et préparer sa désactivation
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
    [string]$OutputPath = "C:\\ADTiering\\NTLM_Audit",
    [int]$DaysToAnalyze = 7,
    [string[]]$DomainControllers = @()
)

Import-Module ActiveDirectory

if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== Audit Utilisation NTLM ===" -ForegroundColor Cyan
Write-Host ""

# Récupération des DC si non spécifiés
if ($DomainControllers.Count -eq 0) {
    Write-Host "[1/4] Récupération des contrôleurs de domaine..." -ForegroundColor Yellow
    $DomainControllers = (Get-ADDomainController -Filter *).HostName
    Write-Host "   ✓ $($DomainControllers.Count) DC trouvés" -ForegroundColor Green
}

# Vérification de l'audit NTLM
Write-Host "[2/4] Vérification de l'audit NTLM..." -ForegroundColor Yellow

$AuditEnabled = $false
foreach ($dc in $DomainControllers | Select-Object -First 1) {
    try {
        $auditSetting = Get-ItemProperty -Path "\$dc\HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0"
-Name "AuditReceivingNTLMTraffic" -ErrorAction SilentlyContinue

        if ($auditSetting.AuditReceivingNTLMTraffic -ge 1) {
            Write-Host "   ✓ Audit NTLM activé sur $dc" -ForegroundColor Green
            $AuditEnabled = $true
        } else {
            Write-Host "   ⚠️  Audit NTLM non activé sur $dc" -ForegroundColor Yellow
        }
    } catch {
        Write-Host "   ⚠️  Impossible de vérifier l'audit sur $dc" -ForegroundColor Yellow
    }
}

if (-not $AuditEnabled) {
    Write-Host ""
    Write-Host "🔴 ATTENTION: Audit NTLM non activé!" -ForegroundColor Red
    Write-Host "   Pour activer l'audit, créez une GPO avec:" -ForegroundColor Yellow
    Write-Host "   Computer Configuration > Windows Settings > Security Settings >" -ForegroundColor
Gray
    Write-Host "   Local Policies > Security Options >" -ForegroundColor Gray
    Write-Host "   'Network security: Restrict NTLM: Audit NTLM authentication in this domain'"
-ForegroundColor Gray
    Write-Host "   → Activer pour tous les comptes" -ForegroundColor Gray
    Write-Host ""
    Write-Host "   Ou via registre:" -ForegroundColor Yellow
    Write-Host '   HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\AuditReceivingNTLMTraffic = 2'
-ForegroundColor Gray
    Write-Host ""
}
```

```
# Collecte des événements NTLM
Write-Host "[3/4] Analyse des événements NTLM (derniers $DaysToAnalyze jours)..." -ForegroundColor
Yellow

$StartDate = (Get-Date).AddDays(-$DaysToAnalyze)
$NTLMEvents = @()

foreach ($dc in $DomainControllers) {
    Write-Host "   Analyse de $dc..." -ForegroundColor Gray

    try {
        # Event ID 8004: NTLM authentication attempt
        $events = Get-WinEvent -ComputerName $dc -FilterHashtable @{
            LogName = 'Microsoft-Windows-NTLM/Operational'
            ID = 8004
            StartTime = $StartDate
        } -ErrorAction SilentlyContinue

        foreach ($event in $events) {
            $xml = [xml]$event.ToXml()
            $NTLMEvents += [PSCustomObject]@{
                Time = $event.TimeCreated
                DC = $dc
                UserName = $xml.Event.EventData.Data | Where-Object {$_.Name -eq 'UserName'} | Select-
Object -ExpandProperty '#text'
                Workstation = $xml.Event.EventData.Data | Where-Object {$_.Name -eq 'Workstation'} |
Select-Object -ExpandProperty '#text'
                TargetServer = $xml.Event.EventData.Data | Where-Object {$_.Name -eq 'TargetName'} |
Select-Object -ExpandProperty '#text'
            }
        }

        Write-Host "     ✓ $($events.Count) événements trouvés" -ForegroundColor Green
    } catch {
        Write-Host "     ⚠️  Erreur lors de la lecture des logs" -ForegroundColor Yellow
    }
}

Write-Host "   ✓ Total: $($NTLMEvents.Count) authentifications NTLM" -ForegroundColor $(
    if ($NTLMEvents.Count -eq 0) {'Green'} else {'Yellow'}
)

# Analyse des données
Write-Host "[4/4] Analyse des utilisations NTLM..." -ForegroundColor Yellow

$TopUsers = $NTLMEvents | Group-Object UserName | Sort-Object Count -Descending | Select-Object -First
10
$TopServers = $NTLMEvents | Group-Object TargetServer | Sort-Object Count -Descending | Select-Object
-First 10
$TopWorkstations = $NTLMEvents | Group-Object Workstation | Sort-Object Count -Descending | Select-
Object -First 10

# === RAPPORT ===
Write-Host ""
Write-Host "=== RAPPORT NTLM ===" -ForegroundColor Cyan
Write-Host ""
Write-Host "📊 Statistiques ($DaysToAnalyze derniers jours):" -ForegroundColor White
Write-Host "   Total authentifications NTLM: $($NTLMEvents.Count)" -ForegroundColor $(
    if ($NTLMEvents.Count -eq 0) {'Green'}
    elseif ($NTLMEvents.Count -lt 100) {'Yellow'}
    else {'Red'}
)
Write-Host ""

if ($NTLMEvents.Count -gt 0) {
    Write-Host "🔝 Top 10 utilisateurs NTLM:" -ForegroundColor White
    $TopUsers | ForEach-Object {
        Write-Host "   $($_.Name): $($_.Count) auth" -ForegroundColor Yellow
```

```
    }
    Write-Host ""

    Write-Host "🔝 Top 10 serveurs cibles:" -ForegroundColor White
    $TopServers | ForEach-Object {
        Write-Host "   $($_.Name): $($_.Count) auth" -ForegroundColor Yellow
    }
    Write-Host ""

    Write-Host "=== PLAN DE MIGRATION VERS KERBEROS ===" -ForegroundColor Cyan
    Write-Host ""
    Write-Host "1. Identifier les applications utilisant NTLM" -ForegroundColor Yellow
    Write-Host "   Analyser les serveurs listés ci-dessus" -ForegroundColor Gray
    Write-Host ""
    Write-Host "2. Configurer les SPN manquants" -ForegroundColor Yellow
    Write-Host "   setspn -A HTTP/<serveur> <compte_service>" -ForegroundColor Gray
    Write-Host ""
    Write-Host "3. Tester avec les comptes identifiés" -ForegroundColor Yellow
    Write-Host ""
    Write-Host "4. Bloquer NTLM pour les comptes Tier 0" -ForegroundColor Yellow
    Write-Host "   Ajouter au groupe Protected Users" -ForegroundColor Gray
    Write-Host ""
    Write-Host "5. Monitorer les tentatives bloquées" -ForegroundColor Yellow
    Write-Host ""
}

# Export
$NTLMEvents | Export-Csv -Path "$OutputPath\NTLM_Events.csv" -NoTypeInformation -Encoding UTF8
$TopUsers | Export-Csv -Path "$OutputPath\Top_NTLM_Users.csv" -NoTypeInformation -Encoding UTF8
$TopServers | Export-Csv -Path "$OutputPath\Top_NTLM_Servers.csv" -NoTypeInformation -Encoding UTF8

Write-Host "✅ Rapports générés: $OutputPath" -ForegroundColor Green

return [PSCustomObject]@{
    TotalNTLMAuth = $NTLMEvents.Count
    UniqueUsers = ($NTLMEvents | Select-Object -Unique UserName).Count
    UniqueServers = ($NTLMEvents | Select-Object -Unique TargetServer).Count
}
```

## Find-Tier0Resources.ps1

Identifie automatiquement toutes les ressources qui doivent être catégorisées Tier 0.

- Identifie contrôleurs de domaine
- Trouve serveurs ADCS
- Détecte serveurs ADFS
- Liste comptes privilégiés
- Inventaire complet Tier 0

```
<#
.SYNOPSIS
    Découverte automatique des ressources Tier 0
.DESCRIPTION
    Identifie toutes les ressources devant être catégorisées Tier 0
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
```

```
    [string]$OutputPath = "C:\\ADTiering\\Tier0_Discovery"
)

Import-Module ActiveDirectory

if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== Découverte Ressources Tier 0 ===" -ForegroundColor Cyan
Write-Host ""

$Tier0Inventory = @{
    DomainControllers = @()
    CertificateServers = @()
    ADFSServers = @()
    PrivilegedAccounts = @()
    ServiceAccounts = @()
    AdminWorkstations = @()
}

# 1. Contrôleurs de domaine
Write-Host "[1/6] Identification des contrôleurs de domaine..." -ForegroundColor Yellow

$DCs = Get-ADDomainController -Filter *
$Tier0Inventory.DomainControllers = $DCs | Select-Object Name, OperatingSystem, IPv4Address,
IsGlobalCatalog

Write-Host "   ✓ $($DCs.Count) contrôleurs de domaine" -ForegroundColor Green

# 2. Serveurs de certificats (ADCS)
Write-Host "[2/6] Recherche des serveurs ADCS..." -ForegroundColor Yellow

$CAServers = Get-ADObject -Filter {objectClass -eq 'pKIEnrollmentService'} -SearchBase (Get-
ADRootDSE).configurationNamingContext
$Tier0Inventory.CertificateServers = $CAServers | Select-Object Name, DistinguishedName

Write-Host "   ✓ $($CAServers.Count) serveurs de certificats" -ForegroundColor Green

# 3. Serveurs ADFS
Write-Host "[3/6] Recherche des serveurs ADFS..." -ForegroundColor Yellow

# Recherche via SCP
$ADFSServers = Get-ADObject -Filter {keywords -like "*ADFS*"} -Properties ServicePrincipalName
$Tier0Inventory.ADFSServers = $ADFSServers | Select-Object Name, DistinguishedName

Write-Host "   ✓ $($ADFSServers.Count) serveurs ADFS potentiels" -ForegroundColor $(
    if ($ADFSServers.Count -gt 0) {'Green'} else {'Gray'}
)

# 4. Comptes privilégiés
Write-Host "[4/6] Identification des comptes privilégiés..." -ForegroundColor Yellow

$PrivilegedGroups = @(
    "Domain Admins",
    "Enterprise Admins",
    "Schema Admins",
    "Administrators",
    "Account Operators",
    "Backup Operators",
    "Server Operators",
    "Print Operators",
    "DnsAdmins"
)

$AllPrivilegedUsers = @()
foreach ($group in $PrivilegedGroups) {
    try {
        $members = Get-ADGroupMember -Identity $group -Recursive -ErrorAction SilentlyContinue
```

```
        foreach ($member in $members) {
            if ($member.objectClass -eq 'user') {
                $user = Get-ADUser $member -Properties Enabled, PasswordLastSet, LastLogonDate
                $AllPrivilegedUsers += [PSCustomObject]@{
                    Username = $user.SamAccountName
                    Name = $user.Name
                    Group = $group
                    Enabled = $user.Enabled
                    PasswordLastSet = $user.PasswordLastSet
                    LastLogon = $user.LastLogonDate
                }
            }
        }
    } catch {
        Write-Warning "Groupe non accessible: $group"
    }
}

$UniquePrivilegedUsers = $AllPrivilegedUsers | Select-Object Username, Name, Enabled, PasswordLastSet,
LastLogon -Unique
$Tier0Inventory.PrivilegedAccounts = $UniquePrivilegedUsers

Write-Host "   ✓ $($UniquePrivilegedUsers.Count) comptes privilégiés uniques" -ForegroundColor Green

# 5. Comptes de service Tier 0
Write-Host "[5/6] Identification des comptes de service Tier 0..." -ForegroundColor Yellow

$ServiceAccounts = Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties ServicePrincipalName,
MemberOf

$Tier0ServiceAccounts = $ServiceAccounts | Where-Object {
    $isTier0 = $false
    foreach ($group in $PrivilegedGroups) {
        if ($_.MemberOf -match $group) {
            $isTier0 = $true
            break
        }
    }
    $isTier0
}

$Tier0Inventory.ServiceAccounts = $Tier0ServiceAccounts | Select-Object SamAccountName, Name,
ServicePrincipalName

Write-Host "   ✓ $($Tier0ServiceAccounts.Count) comptes de service Tier 0" -ForegroundColor $(
    if ($Tier0ServiceAccounts.Count -gt 0) {'Yellow'} else {'Green'}
)

# 6. Postes d'administration (PAW/Jump Servers)
Write-Host "[6/6] Recherche des postes d'administration..." -ForegroundColor Yellow

$AdminWorkstations = Get-ADComputer -Filter {Name -like "*PAW*" -or Name -like "*Admin*" -or Name -like
"*Jump*"} -Properties OperatingSystem

$Tier0Inventory.AdminWorkstations = $AdminWorkstations | Select-Object Name, OperatingSystem,
DistinguishedName

Write-Host "   ✓ $($AdminWorkstations.Count) postes d'administration identifiés" -ForegroundColor $(
    if ($AdminWorkstations.Count -gt 0) {'Green'} else {'Yellow'}
)

# === RAPPORT ===
Write-Host ""
Write-Host "=== INVENTAIRE TIER 0 ===" -ForegroundColor Cyan
Write-Host ""
Write-Host "📊 Ressources Tier 0 identifiées:" -ForegroundColor White
Write-Host ""
Write-Host "🖥️  Infrastructure:" -ForegroundColor White
Write-Host "   Contrôleurs de domaine: $($DCs.Count)" -ForegroundColor Gray
```

```
Write-Host "   Serveurs de certificats (ADCS): $($CAServers.Count)" -ForegroundColor Gray
Write-Host "   Serveurs ADFS: $($ADFSServers.Count)" -ForegroundColor Gray
Write-Host "   Postes d'administration: $($AdminWorkstations.Count)" -ForegroundColor Gray
Write-Host ""
Write-Host "👥 Comptes:" -ForegroundColor White
Write-Host "   Comptes privilégiés: $($UniquePrivilegedUsers.Count)" -ForegroundColor Gray
Write-Host "   Comptes de service Tier 0: $($Tier0ServiceAccounts.Count)" -ForegroundColor Gray
Write-Host ""

if ($Tier0ServiceAccounts.Count -gt 0) {
    Write-Host "⚠️  ATTENTION - Comptes de service privilégiés:" -ForegroundColor Yellow
    Write-Host "   Les comptes de service avec privilèges Tier 0 sont un risque majeur (Kerberoasting)"
-ForegroundColor Yellow
    Write-Host "   Comptes identifiés:" -ForegroundColor Yellow
    $Tier0ServiceAccounts | ForEach-Object {
        Write-Host "   - $($_.SamAccountName)" -ForegroundColor Red
    }
    Write-Host ""
}

# Liste détaillée des DC
Write-Host "=== CONTRÔLEURS DE DOMAINE ===" -ForegroundColor Cyan
$DCs | Format-Table Name, OperatingSystem, IPv4Address, IsGlobalCatalog -AutoSize | Out-String | Write-
Host

# Export
$Tier0Inventory.DomainControllers | Export-Csv -Path "$OutputPath\Tier0_DomainControllers.csv"
-NoTypeInformation -Encoding UTF8
$Tier0Inventory.PrivilegedAccounts | Export-Csv -Path "$OutputPath\Tier0_PrivilegedAccounts.csv"
-NoTypeInformation -Encoding UTF8
$Tier0Inventory.ServiceAccounts | Export-Csv -Path "$OutputPath\Tier0_ServiceAccounts.csv"
-NoTypeInformation -Encoding UTF8
$Tier0Inventory.CertificateServers | Export-Csv -Path "$OutputPath\Tier0_CertificateServers.csv"
-NoTypeInformation -Encoding UTF8
$Tier0Inventory.AdminWorkstations | Export-Csv -Path "$OutputPath\Tier0_AdminWorkstations.csv"
-NoTypeInformation -Encoding UTF8

# Inventaire complet en JSON
$Tier0Inventory | ConvertTo-Json -Depth 3 | Out-File -FilePath
"$OutputPath\Tier0_Complete_Inventory.json" -Encoding UTF8

Write-Host "✅ Inventaire complet exporté: $OutputPath" -ForegroundColor Green
Write-Host ""

Write-Host "=== PROCHAINES ÉTAPES ===" -ForegroundColor Cyan
Write-Host "1. Créer des OUs dédiées Tier 0" -ForegroundColor Yellow
Write-Host "2. Déplacer toutes ces ressources dans les OUs Tier 0" -ForegroundColor Yellow
Write-Host "3. Appliquer les GPO de sécurité Tier 0" -ForegroundColor Yellow
Write-Host "4. Configurer les restrictions d'authentification (silos)" -ForegroundColor Yellow
Write-Host "5. Déployer des PAW pour tous les admins Tier 0" -ForegroundColor Yellow
Write-Host ""

return $Tier0Inventory
```

## Deploy-SecurityBaselines.ps1

Applique les baselines de sécurité Microsoft recommandées pour chaque tier.

- Import baselines Microsoft
- Configuration par tier
- Application automatique
- Vérification post-déploiement

• Rollback si nécessaire

```
<#
.SYNOPSIS
    Déploiement des baselines de sécurité Microsoft
.DESCRIPTION
    Télécharge et applique les Security Baselines Microsoft
.AUTHOR
    Ayi NEDJIMI Consultants - https://www.ayinedjimi-consultants.fr
#>

[CmdletBinding()]
param(
    [string]$OutputPath = "C:\\ADTiering\\Baselines",
    [ValidateSet("Tier0", "Tier1", "Tier2", "All")]
    [string]$Tier = "All",
    [switch]$TestMode
)

Import-Module GroupPolicy

if (-not (Test-Path $OutputPath)) {
    New-Item -Path $OutputPath -ItemType Directory | Out-Null
}

Write-Host "=== Déploiement Security Baselines Microsoft ===" -ForegroundColor Cyan
Write-Host ""

# Vérification du Security Compliance Toolkit
Write-Host "[1/4] Vérification du Security Compliance Toolkit..." -ForegroundColor Yellow

$SCTPath = "C:\\Program Files (x86)\\Microsoft Security Compliance Toolkit 1.0"
if (-not (Test-Path $SCTPath)) {
    Write-Host "   ⚠️  Security Compliance Toolkit non trouvé" -ForegroundColor Yellow
    Write-Host ""
    Write-Host "   Téléchargez-le depuis:" -ForegroundColor Yellow
    Write-Host "   https://www.microsoft.com/en-us/download/details.aspx?id=55319" -ForegroundColor Gray
    Write-Host ""
    Write-Host "   Ce script va créer des GPO basées sur les recommandations Microsoft" -ForegroundColor
Cyan
}

# Configuration baseline Tier 0
Write-Host "[2/4] Configuration baseline Tier 0..." -ForegroundColor Yellow

if ($Tier -eq "Tier0" -or $Tier -eq "All") {
    Write-Host "   Création GPO Tier 0 Security Baseline..." -ForegroundColor Gray

    if (-not $TestMode) {
        try {
            $Tier0GPO = New-GPO -Name "Tier 0 - Security Baseline" -ErrorAction Stop
            Write-Host "   ✓ GPO créée: $($Tier0GPO.DisplayName)" -ForegroundColor Green

            # Configurations recommandées Tier 0
            # Désactiver NTLM
            Set-GPRegistryValue -Name $Tier0GPO.DisplayName -Key
"HKLM\System\CurrentControlSet\Control\Lsa" -ValueName "LmCompatibilityLevel" -Type DWord -Value 5

            # Credential Guard
            Set-GPRegistryValue -Name $Tier0GPO.DisplayName -Key
"HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" -ValueName "EnableVirtualizationBasedSecurity" -Type
DWord -Value 1
            Set-GPRegistryValue -Name $Tier0GPO.DisplayName -Key
"HKLM\SYSTEM\CurrentControlSet\Control\Lsa" -ValueName "LsaCfgFlags" -Type DWord -Value 1

            Write-Host "   ✓ Configurations de sécurité appliquées" -ForegroundColor Green
        } catch {
            Write-Host "   ✗ Erreur: $($_.Exception.Message)" -ForegroundColor Red
```

```
        }
    } else {
        Write-Host "   [TEST MODE] GPO Tier 0 serait créée" -ForegroundColor Cyan
    }
}

# Configuration baseline Tier 1
Write-Host "[3/4] Configuration baseline Tier 1..." -ForegroundColor Yellow

if ($Tier -eq "Tier1" -or $Tier -eq "All") {
    Write-Host "   Création GPO Tier 1 Security Baseline..." -ForegroundColor Gray

    if (-not $TestMode) {
        try {
            $Tier1GPO = New-GPO -Name "Tier 1 - Security Baseline" -ErrorAction Stop
            Write-Host "   ✓ GPO créée: $($Tier1GPO.DisplayName)" -ForegroundColor Green

            # LAPS pour serveurs
            Set-GPRegistryValue -Name $Tier1GPO.DisplayName -Key "HKLM\Software\Policies\Microsoft
Services\AdmPwd" -ValueName "AdmPwdEnabled" -Type DWord -Value 1
            Set-GPRegistryValue -Name $Tier1GPO.DisplayName -Key "HKLM\Software\Policies\Microsoft
Services\AdmPwd" -ValueName "PasswordComplexity" -Type DWord -Value 4
            Set-GPRegistryValue -Name $Tier1GPO.DisplayName -Key "HKLM\Software\Policies\Microsoft
Services\AdmPwd" -ValueName "PasswordLength" -Type DWord -Value 15

            Write-Host "   ✓ LAPS configuré" -ForegroundColor Green
        } catch {
            Write-Host "   ✗ Erreur: $($_.Exception.Message)" -ForegroundColor Red
        }
    } else {
        Write-Host "   [TEST MODE] GPO Tier 1 serait créée" -ForegroundColor Cyan
    }
}

# Configuration baseline Tier 2
Write-Host "[4/4] Configuration baseline Tier 2..." -ForegroundColor Yellow

if ($Tier -eq "Tier2" -or $Tier -eq "All") {
    Write-Host "   Création GPO Tier 2 Security Baseline..." -ForegroundColor Gray

    if (-not $TestMode) {
        try {
            $Tier2GPO = New-GPO -Name "Tier 2 - Security Baseline" -ErrorAction Stop
            Write-Host "   ✓ GPO créée: $($Tier2GPO.DisplayName)" -ForegroundColor Green

            # LAPS pour postes
            Set-GPRegistryValue -Name $Tier2GPO.DisplayName -Key "HKLM\Software\Policies\Microsoft
Services\AdmPwd" -ValueName "AdmPwdEnabled" -Type DWord -Value 1
            Set-GPRegistryValue -Name $Tier2GPO.DisplayName -Key "HKLM\Software\Policies\Microsoft
Services\AdmPwd" -ValueName "PasswordLength" -Type DWord -Value 12

            # Windows Defender
            Set-GPRegistryValue -Name $Tier2GPO.DisplayName -Key
"HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" -ValueName
"DisableRealtimeMonitoring" -Type DWord -Value 0

            Write-Host "   ✓ Configurations appliquées" -ForegroundColor Green
        } catch {
            Write-Host "   ✗ Erreur: $($_.Exception.Message)" -ForegroundColor Red
        }
    } else {
        Write-Host "   [TEST MODE] GPO Tier 2 serait créée" -ForegroundColor Cyan
    }
}

# === RAPPORT ===
Write-Host ""
Write-Host "=== DÉPLOIEMENT TERMINÉ ===" -ForegroundColor Cyan
Write-Host ""
```

```
if ($TestMode) {
    Write-Host "⚠️  MODE TEST - Aucune GPO créée" -ForegroundColor Yellow
    Write-Host "   Relancez sans -TestMode pour appliquer" -ForegroundColor Yellow
} else {
    Write-Host "✅ Security Baselines déployées avec succès!" -ForegroundColor Green
    Write-Host ""
    Write-Host "📋 Prochaines étapes:" -ForegroundColor White
    Write-Host "   1. Liez les GPO aux OUs appropriées" -ForegroundColor Gray
    Write-Host "   2. Testez sur un petit groupe pilote" -ForegroundColor Gray
    Write-Host "   3. Surveillez les logs d'événements" -ForegroundColor Gray
    Write-Host "   4. Étendez progressivement" -ForegroundColor Gray
}

Write-Host ""

Write-Host "📚 Documentation Security Baselines:" -ForegroundColor White
Write-Host "   https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-
baselines" -ForegroundColor Gray
Write-Host ""

Write-Host "✅ Script terminé!" -ForegroundColor Green
```

ANNEXE G

# Templates

Collection de documents types prêts à l'emploi pour structurer et documenter votre projet de tiering Active Directory.

# Planning & Gouvernance

## Plan de Projet Tiering WORD

Plan de projet complet pour l'implémentation du modèle de tiering, incluant phases, jalons, ressources et budget.

- Planning sur 6-12 mois
- Répartition par phases
- Matrice RACI incluse
- Budget prévisionnel

```
PLAN DE PROJET - IMPLÉMENTATION MODÈLE DE TIERING ACTIVE DIRECTORY

Document Confidentiel
Société: [VOTRE ENTREPRISE]
Date: [DATE]
Version: 1.0

═══════════════════════════════════════════════════════════

TABLE DES MATIÈRES

1. CONTEXTE ET OBJECTIFS
2. PÉRIMÈTRE DU PROJET
3. ORGANISATION DU PROJET
4. PLANNING ET JALONS
5. RESSOURCES ET BUDGET
6. RISQUES ET MITIGATION
7. CRITÈRES DE SUCCÈS

═══════════════════════════════════════════════════════════

1. CONTEXTE ET OBJECTIFS

1.1 Contexte
L'Active Directory de l'entreprise représente un actif critique contenant
l'ensemble des identités et droits d'accès. Une compromission de cet
environnement aurait des conséquences catastrophiques.

Le modèle de tiering permet de segmenter les privilèges en trois tiers
distincts afin de limiter la propagation latérale en cas d'attaque.

1.2 Objectifs du Projet
- Sécuriser l'Active Directory contre les attaques modernes
- Implémenter le modèle de tiering en 3 niveaux
- Réduire de 70-90% les chemins d'attaque vers Tier 0
- Assurer la conformité avec les standards de sécurité

1.3 Bénéfices Attendus
- Protection renforcée contre ransomwares
- Réduction du risque de compromission totale
- Amélioration de la traçabilité
- Conformité réglementaire

═══════════════════════════════════════════════════════════

2. PÉRIMÈTRE DU PROJET

2.1 Dans le Périmètre
✓ Identification et classification des ressources par tier
✓ Déploiement de PAW pour admins Tier 0
✓ Implémentation LAPS sur tous les postes
✓ Configuration groupe Protected Users
```

✓ Mise en place silos d'authentification
✓ Configuration GPO de sécurité par tier
✓ Formation des équipes IT

2.2 Hors Périmètre
✗ Migration vers Azure AD
✗ Refonte complète de l'infrastructure
✗ Projets de virtualisation non liés

═══════════════════════════════════════════════════════

3. ORGANISATION DU PROJET

3.1 Sponsor Exécutif
- [NOM] - [FONCTION]
- Responsabilités: Sponsorship, arbitrages stratégiques

3.2 Chef de Projet
- [NOM] - [FONCTION]
- Responsabilités: Pilotage global, reporting, coordination

3.3 Équipe Projet

| Rôle | Nom & Responsabilités |
|---|---|
| Lead Technique AD | [NOM] - Architecture & config |
| Expert Sécurité | [NOM] - Audit & validation |
| Admin Systèmes | [NOM] - Déploiement & tests |
| Responsable Réseau | [NOM] - Segmentation réseau |
| Change Manager | [NOM] - Communication & formation |

3.4 Matrice RACI
[Tableau RACI détaillé avec toutes les tâches]

═══════════════════════════════════════════════════════

4. PLANNING ET JALONS

4.1 Durée Totale: 9 mois

PHASE 1: AUDIT ET PRÉPARATION (Mois 1-2)
─────────────────────────────────────────

Semaine 1-2: Audit de l'existant
  - Exécution BloodHound
  - Inventaire comptes privilégiés
  - Cartographie infrastructure

Semaine 3-4: Conception architecture
  - Design structure OU
  - Plan de segmentation réseau
  - Définition des silos

Semaine 5-8: Préparation environnement
  - Création OUs Tier 0/1/2
  - Préparation GPO
  - Documentation procédures

JALON 1: Architecture validée et approuvée

PHASE 2: SÉCURISATION TIER 0 (Mois 3-5)
─────────────────────────────────────────

Mois 3:
  - Déploiement premiers PAW (2-3 unités)
  - Configuration Protected Users
  - Activation audit avancé DC

Mois 4:
  - Extension déploiement PAW

```
  - Configuration silos authentification
  - Blocage NTLM pour Tier 0

Mois 5:
  - Tests et validation
  - Ajustements configuration
  - Formation admins Tier 0

JALON 2: Tier 0 sécurisé et opérationnel

PHASE 3: IMPLÉMENTATION TIER 1 (Mois 6-7)
──────────────────────────────────────────

  - Déploiement Jump Servers
  - Configuration LAPS serveurs
  - GPO de durcissement
  - Tests et validation

JALON 3: Tier 1 implémenté

PHASE 4: RENFORCEMENT TIER 2 (Mois 8)
──────────────────────────────────────

  - Déploiement LAPS postes
  - Configuration Credential Guard
  - Durcissement sécurité
  - Formation utilisateurs

JALON 4: Tier 2 sécurisé

PHASE 5: FINALISATION (Mois 9)
──────────────────────────────

  - Mise en place monitoring
  - Tests de pénétration
  - Documentation finale
  - Transfert aux équipes Run

JALON FINAL: Projet clôturé et validé
```

═══════════════════════════════════════════════════════════

5. RESSOURCES ET BUDGET

5.1 Ressources Humaines

| Ressource | Charge | Période |
|---|---|---|
| Chef de Projet | 0.5 ETP | 9 mois |
| Lead Technique | 1.0 ETP | 9 mois |
| Admin Systèmes | 0.8 ETP | 6 mois |
| Expert Sécurité | 0.3 ETP | 9 mois |
| Consultant Externe | 20j | Phases 1-2 |

5.2 Budget Matériel

| Élément | Quantité | Coût (€) |
|---|---|---|
| PAW (hardware) | 10 | 15 000 |
| Jump Servers (VM) | 2 | 0 |
| Licences logicielles | - | 5 000 |
| Formation | - | 8 000 |
| Consulting | 20j | 20 000 |
| Divers et imprévus (10%) | - | 4 800 |
| TOTAL BUDGET | | 52 800 € |

═══════════════════════════════════════════════════════════

6. RISQUES ET MITIGATION

```
┌─────────────────────────────────────────────────────────────┐
│ RISQUE 1: Résistance au changement des admins               │
├─────────────────────────────────────────────────────────────┤
│ Probabilité: ÉLEVÉE | Impact: ÉLEVÉ                         │
│                                                             │
│ Mitigation:                                                 │
│ - Communication claire sur les bénéfices                    │
│ - Formation approfondie                                     │
│ - Sponsorship direction                                     │
│ - Déploiement progressif avec pilotes volontaires           │
└─────────────────────────────────────────────────────────────┘

[... autres risques ...]

═══════════════════════════════════════════════════════════

7. CRITÈRES DE SUCCÈS

✓ Aucun chemin d'attaque Tier 2 → Tier 0 dans BloodHound
✓ 100% des comptes Tier 0 dans Protected Users
✓ LAPS déployé sur 100% des endpoints
✓ PAW déployés pour tous les admins Tier 0
✓ 0 incident lié au tiering pendant 3 mois
✓ Satisfaction équipes IT > 80%

═══════════════════════════════════════════════════════════

FIN DU DOCUMENT

© Ayi NEDJIMI Consultants | www.ayinedjimi-consultants.fr
```

## Charte de Gouvernance WORD

Document de gouvernance définissant les rôles, responsabilités et processus de décision pour le tiering.

- Définition des rôles
- Matrice de décision
- Processus d'escalade
- Comités et réunions

```
CHARTE DE GOUVERNANCE - MODÈLE DE TIERING AD

Document: Charte de Gouvernance
Version: 1.0
Statut: APPROUVÉ
Classification: Interne Confidentiel

═══════════════════════════════════════════════════════════

1. OBJET ET PÉRIMÈTRE

Cette charte définit les principes de gouvernance du modèle de tiering
Active Directory, les rôles et responsabilités des acteurs, ainsi que
les processus de décision et d'escalade.

Périmètre:
- Active Directory de production
- Tous les comptes privilégiés
- Infrastructure Tier 0, 1 et 2

═══════════════════════════════════════════════════════════

2. PRINCIPES DE GOUVERNANCE

2.1 Séparation des Privilèges
Aucun compte ne doit disposer de privilèges sur plusieurs tiers.

2.2 Principe du Moindre Privilège
Chaque compte dispose uniquement des droits strictement nécessaires.

2.3 Principe de Défense en Profondeur
Plusieurs couches de sécurité sont implémentées.

2.4 Principe de Traçabilité
Toute action administrative est tracée et auditée.

═══════════════════════════════════════════════════════════

3. RÔLES ET RESPONSABILITÉS

3.1 PROPRIÉTAIRE TIER 0 (Tier 0 Owner)
─────────────────────────────────────────
Responsabilités:
✓ Approuve tous les changements Tier 0
✓ Valide les nouveaux admins Tier 0
✓ Révise trimestriellement les accès
✓ Arbitre les exceptions

Titulaire: [NOM] - [FONCTION]

3.2 ADMINISTRATEURS TIER 0
─────────────────────────────────────────
```

```
Responsabilités:
✓ Administrent l'Active Directory
✓ Gèrent les contrôleurs de domaine
✓ Utilisent exclusivement des PAW
✓ Respectent les procédures strictes

Membres: [LISTE]

[... suite des rôles ...]

═══════════════════════════════════════════════════════════

4. PROCESSUS DE DÉCISION

4.1 Ajout d'un Nouveau Compte Tier 0
┌──────────────────────────────────────────────┐
│ 1. Demande formelle avec justification       │
│ 2. Validation N+2 du demandeur               │
│ 3. Approbation Tier 0 Owner                  │
│ 4. Validation RSSI                           │
│ 5. Création compte + formation obligatoire   │
└──────────────────────────────────────────────┘

Délai: 5 jours ouvrés maximum

[... autres processus ...]

═══════════════════════════════════════════════════════════

FIN DU DOCUMENT
```

## Tableau de Bord Projet EXCEL

Tableau de bord Excel avec KPI, indicateurs d'avancement et reporting automatisé pour le suivi du projet.

- KPI automatisés
- Graphiques dynamiques
- Suivi budget vs réalisé
- Alertes automatiques

```
TABLEAU DE BORD PROJET TIERING - APERÇU

Fichier Excel avec 8 onglets:

1. 📊 DASHBOARD
   - Vue d'ensemble du projet
   - KPI principaux (avancement, budget, délais)
   - Graphiques automatiques
   - Alertes et indicateurs

2. 📅 PLANNING
   - Diagramme de Gantt
   - Jalons et livrables
   - Dépendances entre tâches

3. 💰 BUDGET
   - Suivi budget vs réalisé
   - Analyse des écarts
   - Prévisions de dépenses

4. 👥 RESSOURCES
   - Allocation des ressources
   - Charge de travail
   - Disponibilité

5. ⚠️ RISQUES
   - Registre des risques
   - Probabilité × Impact
   - Plans de mitigation

6. ✅ ACTIONS
   - Liste des actions ouvertes
   - Responsables et échéances
   - Statuts et priorités

7. 📈 KPI
   - Indicateurs clés
   - Tendances et évolutions
   - Objectifs vs réalisé

8. 📋 CONFORMITÉ
   - Checklist de conformité
   - Taux de complétion
   - Écarts identifiés

═══════════════════════════════════════════════════

INDICATEURS CLÉS:

✓ Avancement global: [Auto-calculé]
✓ Budget consommé: [Formule]
✓ Délai respecté: [Indicateur]
```

```
✓ Risques ouverts: [Compteur]
✓ Actions en retard: [Alerte]

Macros VBA incluses pour automatisation!
```

# Procédures Opérationnelles

## Procédure PAW WORD

Procédure complète de déploiement, configuration et utilisation des Privileged Access Workstations (PAW).

- Guide de déploiement
- Configuration step-by-step
- Bonnes pratiques d'usage
- Troubleshooting

```
PROCÉDURE DE DÉPLOIEMENT PAW
Privileged Access Workstation

Version: 2.0
Date: [DATE]
Statut: Validé

═══════════════════════════════════════════════════════════

SOMMAIRE
1. Introduction
2. Prérequis
3. Installation Hardware
4. Configuration Windows
5. Durcissement Sécurité
6. Intégration AD
7. Tests et Validation
8. Mise en Service
9. Maintenance
10. Troubleshooting

═══════════════════════════════════════════════════════════

1. INTRODUCTION

Les PAW (Privileged Access Workstations) sont des postes de travail
hautement sécurisés dédiés exclusivement à l'administration des
ressources Tier 0.

Caractéristiques:
✓ Aucune connexion Internet
✓ Pas d'email
✓ Administration AD uniquement
✓ Durcissement maximal

═══════════════════════════════════════════════════════════

2. PRÉREQUIS

2.1 Matériel Requis
┌─────────────────────────────────────────┐
│ CPU: Intel i5/i7 ou équivalent AMD      │
│ RAM: 16 GB minimum                      │
│ Stockage: SSD 256 GB                    │
│ TPM: Version 2.0 obligatoire            │
│ UEFI: Secure Boot compatible            │
└─────────────────────────────────────────┘

2.2 Logiciels
- Windows 10/11 Enterprise
- Licence Office (optionnel)
- RSAT Tools
```

```
- Sysmon
- PowerShell 5.1+

2.3 Configuration Réseau
- VLAN dédié Tier 0
- Pas d'accès Internet
- Routage vers DC uniquement

═══════════════════════════════════════════════════════════

3. INSTALLATION HARDWARE (Étape par Étape)

ÉTAPE 1: Déballage et inventaire
┌─────────────────────────────────────┐
│ □ Sortir le matériel du carton      │
│ □ Vérifier l'état (pas de dommages) │
│ □ Noter le numéro de série          │
│ □ Enregistrer dans l'inventaire     │
└─────────────────────────────────────┘

ÉTAPE 2: Configuration BIOS/UEFI
┌─────────────────────────────────────┐
│ □ Démarrer et accéder au BIOS       │
│ □ Activer UEFI mode (désactiver Legacy)│
│ □ Activer Secure Boot               │
│ □ Activer TPM 2.0                   │
│ □ Activer VT-x / AMD-V              │
│ □ Désactiver le boot USB/réseau     │
│ □ Définir mot de passe BIOS         │
│ □ Sauvegarder et redémarrer         │
└─────────────────────────────────────┘

[... suite détaillée de toutes les étapes ...]

═══════════════════════════════════════════════════════════

10. TROUBLESHOOTING

PROBLÈME: Le PAW ne peut pas joindre le domaine
──────────────────────────────────────────────
Vérifications:
1. □ Connectivité réseau (ping DC)
2. □ DNS configuré correctement
3. □ Pare-feu Windows autorise AD
4. □ Compte machine créé dans bonne OU
5. □ Horloge synchronisée (< 5 min écart)

Solution: [Détails...]

[... autres problèmes courants ...]

═══════════════════════════════════════════════════════════

ANNEXES
- Annexe A: Checklist complète de déploiement
- Annexe B: Commandes PowerShell utiles
- Annexe C: Configuration GPO recommandée

FIN DU DOCUMENT
```

## Procédure LAPS WORD

Guide complet pour déployer et gérer LAPS (Local Administrator Password Solution) dans votre environnement.

- Installation & configuration
- Extension schéma AD
- Configuration GPO
- Récupération mots de passe

```
PROCÉDURE LAPS
Local Administrator Password Solution

═══════════════════════════════════════════════════════════

TABLE DES MATIÈRES
1. Vue d'ensemble LAPS
2. Prérequis
3. Extension du schéma AD
4. Configuration des permissions
5. Déploiement du client
6. Configuration GPO
7. Utilisation et récupération MDP
8. Dépannage

═══════════════════════════════════════════════════════════

1. VUE D'ENSEMBLE

LAPS (Local Administrator Password Solution) est une solution Microsoft
gratuite qui gère automatiquement les mots de passe des comptes
administrateurs locaux sur les machines Windows.

Bénéfices:
✓ Mot de passe unique par machine
✓ Rotation automatique
✓ Stockage sécurisé dans AD
✓ Blocage Pass-the-Hash latéral

═══════════════════════════════════════════════════════════

2. PRÉREQUIS

2.1 Infrastructure
□ Active Directory (2003 ou supérieur)
□ Schéma AD modifiable (Schema Admin)
□ PowerShell 5.1+ sur le serveur
□ Module Active Directory

2.2 Téléchargements
□ LAPS.msi (64-bit) depuis Microsoft Download Center
   URL: https://www.microsoft.com/download/...

═══════════════════════════════════════════════════════════

3. EXTENSION DU SCHÉMA AD

⚠️ ATTENTION: Cette étape modifie le schéma AD de manière irréversible!
              Testez d'abord en environnement de lab!

ÉTAPE 3.1: Installation du module PowerShell
─────────────────────────────────────────────
```

```
Sur un serveur AD avec droits Schema Admin:

1. Installer LAPS (option Management Tools uniquement)
   > msiexec /i LAPS.x64.msi ADDLOCAL=Management

2. Importer le module
   > Import-Module AdmPwd.PS

3. Vérifier le module
   > Get-Command -Module AdmPwd.PS

ÉTAPE 3.2: Extension du schéma
──────────────────────────────────────────────────
1. Étendre le schéma AD
   > Update-AdmPwdADSchema

   Résultat attendu:
   ✓ "Schema update successful"

2. Vérifier l'extension
   > Get-ADObject -SearchBase (Get-ADRootDSE).schemaNamingContext \
                  -Filter {name -eq "ms-Mcs-AdmPwd"}

   Si l'objet existe: ✓ Schéma étendu avec succès

[... suite de la procédure détaillée ...]

═══════════════════════════════════════════════════════

7. UTILISATION - RÉCUPÉRATION DES MOTS DE PASSE

Via PowerShell:
──────────────
> Get-AdmPwdPassword -ComputerName PC001

Via GUI:
────────
1. Ouvrir "LAPS UI"
2. Entrer le nom de l'ordinateur
3. Cliquer "Search"
4. Le mot de passe s'affiche (avec date d'expiration)

⚠️ Traçabilité: Toutes les lectures sont auditées dans les logs AD!

FIN DU DOCUMENT
```

## Plan de Réponse aux Incidents WORD

Plan d'intervention en cas de compromission détectée, avec procédures spécifiques par tier.

- Workflow d'escalade
- Actions par niveau de sévérité
- Procédures de confinement
- Checklist de récupération

# Documentation Technique

### Architecture Détaillée WORD

Document d'architecture technique complète avec diagrammes, flux et spécifications pour chaque tier.

- Schémas d'architecture
- Flux réseau détaillés
- Matrice de flux
- Spécifications techniques

### Runbook Opérationnel WORD

Guide opérationnel quotidien pour les équipes IT : tâches récurrentes, vérifications et maintenance.

- Tâches quotidiennes/hebdo/mensuelles
- Procédures de vérification
- Commandes PowerShell
- Checklists de validation

### Matrice de Flux Réseau EXCEL

Matrice Excel détaillant tous les flux réseau autorisés entre les tiers, avec ports et protocoles.

- Flux par tier (0/1/2)
- Ports et protocoles
- Règles firewall
- Validation automatique

# Communication & Formation

### Plan de Communication WORD

Stratégie de communication pour accompagner le changement : emails types, présentations, FAQ utilisateurs.

- Emails d'annonce
- Messages par phase
- FAQ utilisateurs
- Communication de crise

### Support de Formation PPTX

Présentation PowerPoint complète pour former les administrateurs au modèle de tiering.

- 60+ slides
- Animations et schémas
- Notes du formateur
- Quiz d'évaluation

### Guide Utilisateur PAW PDF

Guide pratique pour les administrateurs utilisant des PAW : bonnes pratiques, FAQ et troubleshooting.

- Guide pas-à-pas
- Captures d'écran
- FAQ utilisateurs
- Aide au dépannage

# À propos de l'auteur

**Ayi NEDJIMI** est consultant senior en cybersécurité avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et Active Directory. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer, il intervient sur des missions de pentest AD, sécurité Cloud et conformité réglementaire.

Spécialiste reconnu de la sécurisation Active Directory, il a accompagné de nombreuses organisations dans la mise en place du modèle de tiering, allant des PME industrielles aux grands groupes bancaires. Son approche pragmatique, combinant expertise technique approfondie et compréhension des contraintes opérationnelles, permet des déploiements réussis et durables.

Fondateur d'**Ayinedjimi Consultants**, il partage régulièrement son expertise à travers des publications techniques, des guides pratiques et des formations spécialisées en sécurité des infrastructures Microsoft.

## Domaines d'expertise

- Audit et sécurisation Active Directory
- Implémentation du modèle de tiering
- Tests d'intrusion et Red Team
- Sécurité Cloud (Azure AD, Microsoft 365)
- Conformité et gouvernance (ISO 27001, NIS2, RGPD)
- Intelligence Artificielle et cybersécurité (ISO 42001)

## Certifications

- OSCP — Offensive Security Certified Professional
- CISSP — Certified Information Systems Security Professional
- ISO 27001 Lead Auditor

- ISO 42001 Lead Implementer

## Contact

Site web : www.ayinedjimi-consultants.fr

LinkedIn : linkedin.com/in/ayi-nedjimi