Checklist Sécurité ACTIVE DIRECTORY 2025

Ayi NEDJIMI Consultants
ayinedjimi-consultants.fr
v1.0 — 2026-04-04 · 295 controles

Sommaire

Section 1 — ARCHITECTURE & TIERING

1.0 — ARCHITECTURE & TIERING

1.1.1 *Modèle d'accès Enterprise (Tiering Model)*

MITRE ATT&CK : T1078

DESCRIPTION :

Le modèle de tiering Microsoft sépare l'infrastructure en 3 niveaux (Tier 0: AD/DC, Tier 1: Serveurs, Tier 2: Workstations) pour limiter les mouvements latéraux. L'absence de séparation permet l'élévation de privilèges entre niveaux.

```
# Vérifier l'existence des OUs de tiering
Get-ADOrganizationalUnit -Filter "Name -like '*Tier*'" | Select Name,DistinguishedName
# Vérifier les GPO de tiering
Get-GPO -All | Where-Object {$_.DisplayName -like "*Tier*"}
# Comptes dans les groupes privilégiés par tier
Get-ADGroupMember "Tier 0 Admins" -Recursive
```

REMÉDIATION :

1. Créer la structure OU Tiering
2. Implémenter les GPO de restriction par tier
3. Migrer les comptes selon le modèle

VALEUR PAR DÉFAUT :

Aucun tiering implémenté

1.1.2 *Niveau fonctionnel de forêt minimum*

MITRE ATT&CK : T1484

DESCRIPTION :

Le niveau fonctionnel détermine les fonctionnalités AD disponibles. Windows Server 2019+ apporte des améliorations de sécurité importantes comme l'authentification Kerberos AES256 par défaut.

```
Get-ADForest | Select Name,ForestMode
Get-ADDomain | Select Name,DomainMode
```

REMÉDIATION :

1. Upgrader tous les DC vers WS2019+
2. Élever le niveau fonctionnel : Set-ADForestMode -Identity forest.com -ForestMode Windows2019Forest

VALEUR PAR DÉFAUT :

Windows2019Forest recommandé

1.1.3 *Architecture sites et sous-réseaux*

MITRE ATT&CK : T1018

DESCRIPTION :

Une architecture sites incorrecte peut causer des problèmes de réplication, d'authentification et faciliter la reconnaissance réseau pour un attaquant.

```
Get-ADReplicationSite | Select Name,Description
Get-ADReplicationSubnet | Select Name,Site,Location
Get-ADReplicationSiteLink | Select Name,Cost,ReplicationFrequencyInMinutes
```

REMÉDIATION :

1. Créer des sites correspondant à la topologie réseau
2. Associer les sous-réseaux aux sites appropriés
3. Configurer les liens de sites avec des coûts adéquats

VALEUR PAR DÉFAUT :

Site par défaut uniquement

1.1.4 *Séparation des rôles FSMO*

MITRE ATT&CK : T1484

DESCRIPTION :

Les rôles FSMO centralisés sur un seul DC créent un point de défaillance unique. La dispersion améliore la disponibilité et limite l'impact d'une compromission.

```
# Vérifier les détenteurs de rôles FSMO
Get-ADForest | Select SchemaMaster,DomainNamingMaster
Get-ADDomain | Select PDCEmulator,RIDMaster,InfrastructureMaster
netdom query fsmo
```

REMÉDIATION :

1. Séparer les rôles sur des DC différents
2. Documenter les détenteurs de rôles
3. Tester les procédures de transfert/saisie

VALEUR PAR DÉFAUT :

Tous rôles sur le premier DC

1.1.5 *Configuration des trusts inter-domaines*

MITRE ATT&CK : T1482

DESCRIPTION :

Les trusts bidirectionnels permettent l'authentification et l'accès aux ressources entre domaines/forêts. Mal configurés, ils exposent à des attaques de type Golden Ticket inter-domaines.

```
Get-ADTrust -Filter * | Select Name,Direction,TrustType,SelectiveAuthentication,SIDFilteringEnabled
# Vérifier les SID History dangereux
Get-ADUser -Filter * -Properties SIDHistory | Where-Object {$_.SIDHistory}
```

REMÉDIATION :

1. Activer SID Filtering sur tous les trusts externes
2. Implémenter Selective Authentication
3. Auditer et nettoyer les SID History

VALEUR PAR DÉFAUT :

SID Filtering désactivé sur trusts internes

1.1.6 *Contrôle des connexions clients LDAP*

MITRE ATT&CK : T1041

DESCRIPTION :

Les connexions LDAP non sécurisées permettent l'interception des credentials et des requêtes. LDAPS et LDAP Signing doivent être imposés.

```
# Vérifier les paramètres LDAP sur DC
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name "LDAPServerIntegrity"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name "LdapEnforceChannelBinding"
```

REMÉDIATION :

1. Set LDAPServerIntegrity = 2 (required signing)
2. Set LdapEnforceChannelBinding = 2 (always)
3. Configurer certificats LDAPS

VALEUR PAR DÉFAUT :

LDAPServerIntegrity = 1 (négocié)

1.1.7 *Isolation des contrôleurs de domaine*

MITRE ATT&CK : T1210

DESCRIPTION :

Les DC doivent être isolés dans des VLANs dédiés avec des règles firewall strictes. L'exposition directe facilite les attaques DCSync et DCShadow.

```
# Vérifier les interfaces réseau des DC
Get-NetAdapter | Select Name,InterfaceDescription,Status
Get-NetFirewallRule -DisplayGroup "Active Directory Domain Services" | Select DisplayName,Enabled,Action
```

REMÉDIATION :

1. Placer les DC dans un VLAN dédié
2. Configurer des règles firewall strictes
3. Surveiller le trafic réseau des DC

VALEUR PAR DÉFAUT :

Aucune isolation réseau

1.1.8 *Contrôle des ports et services DC*

MITRE ATT&CK : T1046

DESCRIPTION :

Les DC exposent de nombreux services réseau. Seuls les ports nécessaires doivent être ouverts pour limiter la surface d'attaque.

```
# Ports ouverts sur le DC
Get-NetTCPConnection -State Listen | Select LocalAddress,LocalPort,OwningProcess
Get-Service | Where-Object {$_.Status -eq "Running" -and $_.Name -like "*AD*"}
```

REMÉDIATION :

1. Désactiver les services non nécessaires
2. Configurer le firewall Windows
3. Auditer régulièrement les ports ouverts

VALEUR PAR DÉFAUT :

Nombreux services/ports ouverts

1.1.9 *Redondance et haute disponibilité*

MITRE ATT&CK : T1489

DESCRIPTION :

Un nombre insuffisant de DC par site peut causer des interruptions de service. La recommandation est minimum 2 DC par site critique.

```
# Nombre de DC par site
Get-ADDomainController | Group-Object Site | Select Name,Count
# État de réplication entre DC
Get-ADReplicationFailure -Target * -Scope Domain
```

REMÉDIATION :

1. Déployer minimum 2 DC par site critique
2. Vérifier la santé de réplication
3. Tester les procédures de basculement

VALEUR PAR DÉFAUT :

Souvent un seul DC par site

1.1.10 *Contrôle des objets GPO orphelins*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les GPO non liées ou avec des permissions incorrectes peuvent être exploitées pour l'élévation de privilèges ou la persistence.

```
# GPO non liées
Get-GPO -All | Where-Object {(Get-GPOReport -Guid $_.Id -ReportType XML) -notmatch "LinksTo"}
# Permissions GPO dangereuses
Get-GPPermission -All | Where-Object {$_.Permission -match "Edit" -and $_.Trustee -notlike "*Admin*"}
```

REMÉDIATION :

1. Supprimer les GPO orphelines
2. Auditer les permissions GPO
3. Implémenter des processus de gouvernance GPO

VALEUR PAR DÉFAUT :

GPO orphelines présentes

1.1.11 *Gestion des comptes de service intégrés*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les comptes built-in comme Administrator, Guest, krbtgt doivent être sécurisés. Le compte Guest doit être désactivé, Administrator renommé.

```
Get-ADUser Administrator -Properties Enabled,PasswordLastSet,BadLogonCount
Get-ADUser Guest -Properties Enabled
Get-ADUser krbtgt -Properties PasswordLastSet,AccountNotDelegated
```

REMÉDIATION :

1. Désactiver le compte Guest
2. Renommer le compte Administrator
3. Définir AccountNotDelegated sur krbtgt

VALEUR PAR DÉFAUT :

Comptes avec noms par défaut

1.1.12 *Contrôle du catalogue global*

MITRE ATT&CK : T1018

DESCRIPTION :

Le catalogue global contient des informations sur tous les objets de la forêt. Un nombre insuffisant de serveurs GC peut impacter les performances d'authentification.

```
# Serveurs de catalogue global
Get-ADDomainController -Filter * | Select Name,Site,IsGlobalCatalog
# Vérifier la réplication du GC
Get-ADReplicationConnection -Filter * | Where-Object {$_.ReplicatedNamingContexts -like "*3268*"}
```

REMÉDIATION :

1. Configurer au moins un GC par site principal
2. Vérifier la réplication GC
3. Monitorer les performances d'authentification

VALEUR PAR DÉFAUT :

GC sur tous les DC en single-domain

1.1.13 *Protection contre DCShadow*

MITRE ATT&CK : T1207

DESCRIPTION :

L'attaque DCShadow permet à un attaquant de s'enregistrer comme DC temporaire pour injecter des changements dans AD. La détection nécessite un monitoring spécifique.

```
# Vérifier les enregistrements SPN suspects
Get-ADUser -Filter * -Properties ServicePrincipalNames | Where-Object {$_.ServicePrincipalNames -like "*GC/*" -or $_.ServicePrincip
Get-ADComputer -Filter * -Properties ServicePrincipalNames | Where-Object {$_.ServicePrincipalNames -like "*GC/*"}
```

REMÉDIATION :

1. Monitorer les créations de SPN DC
2. Restreindre les permissions ms-DS-MachineAccountQuota
3. Alerter sur les nouveaux objets DC

VALEUR PAR DÉFAUT :

Aucune protection spécifique

1.1.14 *Configuration des UPN alternatives*

MITRE ATT&CK : T1078

DESCRIPTION :

Les UPN suffixes alternatifs peuvent faciliter les attaques par confusion d'identité. Seuls les suffixes légitimes doivent être configurés.

```
# Suffixes UPN configurés
Get-ADForest | Select UPNSuffixes
# Utilisateurs avec UPN non-standard
Get-ADUser -Filter * -Properties UserPrincipalName | Where-Object {$_.UserPrincipalName -notlike "*@domain.com"}
```

REMÉDIATION :

1. Auditer tous les suffixes UPN
2. Supprimer les suffixes non utilisés
3. Standardiser les UPN utilisateurs

VALEUR PAR DÉFAUT :

Suffixe de domaine uniquement

1.1.15 *Contrôle des liens de sites coûteux*

MITRE ATT&CK : T1018

DESCRIPTION :

Des coûts de liens incorrects peuvent causer une réplication excessive ou insuffisante, impactant les performances et la cohérence AD.

```
# Liens de sites et coûts
Get-ADReplicationSiteLink | Select Name,Cost,ReplicationFrequencyInMinutes,Sites
# Connexions de réplication générées
Get-ADReplicationConnection -Filter * | Select Name,ReplicatedNamingContexts,FromServer,ToServer
```

REMÉDIATION :

1. Ajuster les coûts selon la bande passante
2. Optimiser la fréquence de réplication
3. Surveiller la charge de réplication

VALEUR PAR DÉFAUT :

Coût 100 pour DEFAULTIPSITELINK

1.1.16 *Validation de la cohérence DNS*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Les enregistrements DNS AD incorrects peuvent causer des problèmes d'authentification et faciliter les attaques de redirection.

```
# Enregistrements SRV critiques
nslookup -type=SRV _ldap._tcp.domain.com
nslookup -type=SRV _kerberos._tcp.domain.com
# Vérifier la cohérence DNS sur tous les DC
dcdiag /test:dns /v
```

REMÉDIATION :

1. Corriger les enregistrements SRV manquants
2. Vérifier la résolution DNS sur tous les DC
3. Configurer des forwarders DNS redondants

VALEUR PAR DÉFAUT :

Enregistrements automatiques

1.1.17 *Contrôle des quotas d'objets AD*

MITRE ATT&CK : T1484

DESCRIPTION :

Les quotas AD limitent le nombre d'objets qu'un principal peut créer, prévenant les attaques DoS et l'abus de privilèges.

```
# Quotas définis
Get-ADObject -SearchBase "CN=NTDS Quotas,CN=NTDS Settings,CN=Configuration,DC=domain,DC=com" -Filter *
# Utilisation actuelle par principal
dsquery * -filter "(&(objectClass=user)(objectCategory=person))" -attr distinguishedName,msDS-QuotaUsed
```

REMÉDIATION :

1. Définir des quotas appropriés par type d'utilisateur
2. Monitorer l'utilisation des quotas
3. Alerter sur les dépassements

VALEUR PAR DÉFAUT :

Quotas illimités pour tous

1.1.18 *Architecture multi-forêt*

MITRE ATT&CK : T1482

DESCRIPTION :

Dans les environnements multi-forêts, l'isolation de sécurité entre forêts doit être maintenue. Les trusts doivent suivre le principe du moindre privilège.

```
# Trusts de forêt
Get-ADTrust -Filter "TrustType -eq 'Forest'" | Select Name,Direction,SelectiveAuthentication,SIDFilteringEnabled
# Comptes avec privilèges inter-forêts
Get-ADGroupMember "Enterprise Admins" -Server rootdomain.com
```

REMÉDIATION :

1. Limiter les trusts au strict nécessaire
2. Activer Selective Authentication
3. Éviter les comptes privilégiés inter-forêts

VALEUR PAR DÉFAUT :

Configuration permissive

1.1.19 *Contrôle des objets protégés AdminSDHolder*

MITRE ATT&CK : T1484.001

DESCRIPTION :

AdminSDHolder protège les comptes privilégiés en réinitialisant leurs ACL toutes les heures. Les modifications non autorisées peuvent compromettre cette protection.

```
# État d'AdminSDHolder
Get-ADObject -Identity "CN=AdminSDHolder,CN=System,DC=domain,DC=com" -Properties nTSecurityDescriptor,Description
# Comptes avec adminCount=1
Get-ADUser -Filter {adminCount -eq 1} -Properties adminCount,memberOf | Select Name,adminCount,memberOf
```

REMÉDIATION :

1. Restaurer les ACL d'AdminSDHolder par défaut
2. Vérifier que SDProp fonctionne (service Protected Storage)
3. Auditer les comptes avec adminCount orphelins

VALEUR PAR DÉFAUT :

ACL par défaut intactes

1.1.20 *Surveillance des modifications de schéma*

MITRE ATT&CK : T1484

DESCRIPTION :

Les modifications de schéma AD sont permanentes et peuvent introduire des vulnérabilités. Elles doivent être strictement contrôlées et auditées.

```
# Versions de schéma
Get-ADObject -Identity "CN=Schema,CN=Configuration,DC=domain,DC=com" -Properties objectVersion,whenChanged
# Membres du groupe Schema Admins
Get-ADGroupMember "Schema Admins"
```

REMÉDIATION :

1. Vider le groupe Schema Admins
2. Activer l'audit des modifications de schéma
3. Documenter toutes les extensions de schéma

VALEUR PAR DÉFAUT :

Groupe Schema Admins vide

1.1.21 *Contrôle des permissions sur les conteneurs système*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les conteneurs système AD (System, Configuration, Schema) contiennent des objets critiques. Leurs permissions doivent être strictement contrôlées.

```
# Permissions sur les conteneurs critiques
dsacls "CN=System,DC=domain,DC=com"
dsacls "CN=Configuration,DC=domain,DC=com"
dsacls "CN=Schema,CN=Configuration,DC=domain,DC=com"
```

REMÉDIATION :

1. Supprimer les permissions non-standards
2. Limiter les accès aux groupes système
3. Auditer régulièrement les permissions

VALEUR PAR DÉFAUT :

Permissions restrictives par défaut

1.1.22 *Configuration des sites Read-Only DC (RODC)*

MITRE ATT&CK : T1078

DESCRIPTION :

Les RODC dans des sites distants réduisent les risques de compromission. Les Password Replication Policy doivent être configurées selon le principe du moindre privilège.

```
# RODC configurés
Get-ADDomainController -Filter {IsReadOnly -eq $true} | Select Name,Site,IsReadOnly
# Password Replication Policy
Get-ADAccountResultantPasswordReplicationPolicy -Identity username -DomainController RODCname
```

REMÉDIATION :

1. Déployer des RODC dans les sites à risque
2. Configurer des PRP restrictives
3. Monitorer les tentatives de réplication de mots de passe

VALEUR PAR DÉFAUT :

Pas de RODC configurés

1.1.23 *Contrôle des objets Computer orphelins*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les comptes ordinateur obsolètes augmentent la surface d'attaque. Ils doivent être régulièrement nettoyés.

```
# Ordinateurs non connectés depuis 90+ jours
$date = (Get-Date).AddDays(-90)
Get-ADComputer -Filter {LastLogonTimeStamp -lt $date -and OperatingSystem -like "*"} -Properties LastLogonTimeStamp,OperatingSystem
```

REMÉDIATION :

1. Identifier les ordinateurs obsolètes
2. Désactiver puis supprimer après validation
3. Automatiser le nettoyage avec des scripts

VALEUR PAR DÉFAUT :

Pas de nettoyage automatique

1.1.24 *Validation de la topologie de réplication*

MITRE ATT&CK : T1018

DESCRIPTION :

Une topologie de réplication optimale assure la convergence rapide des changements tout en minimisant le trafic réseau.

```
# Connexions de réplication
Get-ADReplicationConnection -Filter * | Select Name,AutoGenerated,FromServer,ToServer,ReplicatedNamingContexts
# Analyse de la topologie
repadmin /showrepl /csv > replication-status.csv
```

REMÉDIATION :

1. Optimiser les connexions automatiques KCC
2. Créer des connexions manuelles si nécessaire
3. Surveiller la latence de réplication

VALEUR PAR DÉFAUT :

Topologie générée automatiquement par KCC

1.1.25 *Contrôle des attributs sensibles non répliqués*

MITRE ATT&CK : T1003.006

DESCRIPTION :

Certains attributs sensibles ne doivent pas être répliqués vers les RODC pour limiter l'exposition en cas de compromission.

```
# Attributs dans Filtered Attribute Set (FAS)
Get-ADObject -SearchBase "CN=Schema,CN=Configuration,DC=domain,DC=com" -Filter {searchFlags -band 512} | Select Name,lDAPDisplayNam
```

REMÉDIATION :

1. Identifier les attributs sensibles métier
2. Les ajouter au Filtered Attribute Set si nécessaire
3. Tester l'impact sur les applications

VALEUR PAR DÉFAUT :

FAS contient attributs système sensibles

2.0 — COMPTES PRIVILÉGIÉS

2.1.1 *Limitation des membres Domain Admins*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Le groupe Domain Admins a un contrôle total sur le domaine. Le nombre de membres doit être minimal (<5) et chaque ajout justifié et temporaire.

```
# Membres Domain Admins
Get-ADGroupMember "Domain Admins" -Recursive | Select Name,SamAccountName,objectClass,LastLogonDate
# Historique des modifications
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4728,4729} | Where-Object {$_.Message -like "*Domain Admins*"}
```

REMÉDIATION :

1. Limiter à maximum 5 membres permanents
2. Utiliser des comptes dédiés (pas de comptes utilisateur normaux)
3. Implémenter JIT pour les accès temporaires

VALEUR PAR DÉFAUT :

Administrateur et parfois Administrateurs du domaine

2.1.2 *Sécurisation du groupe Enterprise Admins*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Enterprise Admins contrôle toute la forêt. Ce groupe doit être vide sauf pendant les opérations de maintenance critique de la forêt.

```
# Membres Enterprise Admins
Get-ADGroupMember "Enterprise Admins" -Server (Get-ADForest).RootDomain | Select Name,SamAccountName,LastLogonDate
# Vérifier dans tous les domaines enfants
Get-ADTrust -Filter * | ForEach-Object {Get-ADGroupMember "Enterprise Admins" -Server $_.Target}
```

REMÉDIATION :

1. Vider complètement le groupe
2. Ajouter temporairement seulement pour les opérations forêt
3. Alerter sur toute modification

VALEUR PAR DÉFAUT :

Administrateur du domaine racine

2.1.3 *Contrôle du groupe Schema Admins*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Schema Admins peut modifier le schéma AD de façon permanente et irréversible. Le groupe doit être vide sauf pendant les extensions de schéma planifiées.

```
# Membres Schema Admins
Get-ADGroupMember "Schema Admins" -Server (Get-ADForest).RootDomain
# Historique des modifications de schéma
Get-WinEvent -FilterHashtable @{LogName='Directory Service';ID=1137}
```

REMÉDIATION :

1. Vider complètement le groupe
2. Ajouter temporairement uniquement pour extensions planifiées
3. Documenter toutes les modifications de schéma

VALEUR PAR DÉFAUT :

Administrateur du domaine racine

2.1.4 *Audit des comptes de service privilégiés*

MITRE ATT&CK : T1078.003

DESCRIPTION :

Les comptes de service avec des privilèges élevés sont des cibles d'attaque privilégiées. Ils doivent utiliser des mots de passe complexes et être régulièrement rotés.

```
# Comptes de service dans groupes privilégiés
Get-ADUser -Filter {(memberOf -like "*Domain Admins*") -or (memberOf -like "*Enterprise Admins*") -or (ServicePrincipalName -like "
```

REMÉDIATION :

1. Migrer vers des Group Managed Service Accounts (gMSA)
2. Retirer les privilèges excessifs
3. Implémenter la rotation automatique des mots de passe

VALEUR PAR DÉFAUT :

Comptes de service souvent sur-privilégiés

2.1.5 *Configuration des Group Managed Service Accounts (gMSA)*

MITRE ATT&CK : T1003.002

DESCRIPTION :

Les gMSA automatisent la gestion des mots de passe de comptes de service et éliminent les risques liés aux mots de passe partagés ou obsolètes.

```
# gMSA configurés
Get-ADServiceAccount -Filter * | Select Name,Enabled,PrincipalsAllowedToRetrieveManagedPassword
# Services utilisant encore des comptes utilisateur classiques
Get-Service | Where-Object {$_.StartName -like "*\*" -and $_.StartName -notlike "*$"}
```

REMÉDIATION :

1. Créer des gMSA pour tous les services critiques
2. Migrer les services existants vers gMSA
3. Désactiver les anciens comptes de service

VALEUR PAR DÉFAUT :

Comptes de service manuels

2.1.6 *Protection du compte KRBTGT*

MITRE ATT&CK : T1558.001

DESCRIPTION :

Le compte KRBTGT chiffre les tickets Kerberos. Son compromission permet la création de Golden Tickets. Le mot de passe doit être roté régulièrement.

```
Get-ADUser krbtgt -Properties PasswordLastSet,AccountNotDelegated,msDS-SupportedEncryptionTypes
# Vérifier la rotation récente (>180 jours = critique)
$krbtgt = Get-ADUser krbtgt -Properties PasswordLastSet
(Get-Date) - $krbtgt.PasswordLastSet
```

REMÉDIATION :

1. Programmer une rotation semestrielle du KRBTGT
2. Utiliser l'outil Microsoft New-KrbtgtKeys.ps1
3. Coordonner avec tous les DC de la forêt

VALEUR PAR DÉFAUT :

Jamais changé depuis création domaine

2.1.7 *Comptes avec délégation Kerberos non contrainte*

MITRE ATT&CK : T1558.003

DESCRIPTION :

La délégation non contrainte permet à un service d'emprunter l'identité de n'importe quel utilisateur vers n'importe quel service. Très dangereux pour l'élévation de privilèges.

```
# Comptes avec délégation non contrainte (hors DCs)
Get-ADUser -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation,ServicePrincipalName
Get-ADComputer -Filter {TrustedForDelegation -eq $true -and PrimaryGroupID -ne 516} -Properties TrustedForDelegation,ServicePrincip
```

REMÉDIATION :

1. Migrer vers délégation contrainte ou RBCD
2. Désactiver la délégation non contrainte sur tous les objets non-DC
3. Surveiller les nouvelles configurations

VALEUR PAR DÉFAUT :

Potentiellement présente sur comptes de service

2.1.8 *Audit des comptes avec SPN (Kerberoasting)*

MITRE ATT&CK : T1558.003

DESCRIPTION :

Les comptes utilisateur avec SPN sont vulnérables au Kerberoasting. Ils doivent avoir des mots de passe très complexes ou migrer vers gMSA.

```
# Utilisateurs avec SPN (cibles Kerberoasting)
Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties ServicePrincipalName,PasswordLastSet,AdminCount |
Select Name,ServicePrincipalName,PasswordLastSet,AdminCount
```

REMÉDIATION :

1. Utiliser des mots de passe >25 caractères pour comptes SPN
2. Migrer vers gMSA quand possible
3. Surveiller les demandes TGS suspectes (Event 4769)

VALEUR PAR DÉFAUT :

Mots de passe souvent faibles sur comptes SPN

2.1.9 *Contrôle des comptes dormants privilégiés*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les comptes privilégiés inactifs représentent un risque car ils peuvent avoir conservé des accès élevés sans supervision récente.

```
# Comptes privilégiés non connectés >90 jours
$date = (Get-Date).AddDays(-90)
Get-ADUser -Filter {LastLogonTimeStamp -lt $date -and adminCount -eq 1} -Properties LastLogonTimeStamp,memberOf,PasswordLastSet
```

REMÉDIATION :

1. Désactiver les comptes inactifs >90 jours
2. Supprimer après validation métier
3. Implémenter un processus de revue trimestrielle

VALEUR PAR DÉFAUT :

Pas de nettoyage automatique

2.1.10 *Configuration des Privileged Access Workstations (PAW)*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les comptes privilégiés doivent uniquement être utilisés depuis des postes dédiés et durcis (PAW) pour éviter la compromission par des malwares.

```
# Connexions admin depuis postes non-PAW
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} |
Where-Object {$_.Message -like "*Domain Admins*" -and $_.Properties[5].Value -ne "PAW-*"}
```

REMÉDIATION :

1. Déployer des PAW pour tous les administrateurs Tier 0/1
2. Bloquer les connexions admin depuis postes standard
3. Implémenter Credential Guard sur les PAW

VALEUR PAR DÉFAUT :

Pas de PAW déployées

2.1.11 *Just-in-Time (JIT) Administration*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les privilèges élevés doivent être accordés temporairement uniquement quand nécessaire, réduisant la fenêtre d'exposition aux attaques.

```
# Comptes avec privilèges permanents
Get-ADGroupMember "Domain Admins" | Where-Object {$_.Name -notlike "*JIT*"}
# Solutions JIT déployées (PIM, PAM, etc.)
Get-Service | Where-Object {$_.Name -like "*PIM*" -or $_.Name -like "*PAM*"}
```

REMÉDIATION :

1. Implémenter Azure AD PIM ou solution tierce
2. Convertir les accès permanents en temporaires
3. Auditer toutes les élévations de privilèges

VALEUR PAR DÉFAUT :

Privilèges accordés en permanence

2.1.12 *Contrôle des permissions AdminSDHolder*

MITRE ATT&CK : T1484.001

DESCRIPTION :

AdminSDHolder protège les objets privilégiés. Ses ACL sont propagées toutes les heures vers les comptes protégés. Toute modification peut compromettre la sécurité.

```
# ACL AdminSDHolder
$adminSDHolder = "CN=AdminSDHolder,CN=System,DC=domain,DC=com"
(Get-ACL "AD:\$adminSDHolder").Access | Where-Object {$_.IdentityReference -notlike "*NT AUTHORITY*" -and $_.IdentityReference -not
```

REMÉDIATION :

1. Restaurer les ACL par défaut d'AdminSDHolder
2. Surveiller les modifications (Event 5136)
3. Vérifier que SDProp fonctionne correctement

VALEUR PAR DÉFAUT :

ACL restrictives par défaut

2.1.13 *Protection contre AS-REP Roasting*

MITRE ATT&CK : T1558.004

DESCRIPTION :

Les comptes avec pré-authentification Kerberos désactivée sont vulnérables à l'AS-REP Roasting, permettant de craquer les mots de passe hors-ligne.

```
# Comptes sans pré-authentification requise
Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties DoesNotRequirePreAuth,PasswordLastSet,AdminCount
```

REMÉDIATION :

1. Activer la pré-authentification sur tous les comptes
2. Si nécessaire pour compatibilité, utiliser des mots de passe très complexes
3. Surveiller les demandes AS-REP (Event 4768 avec code 0x18)

VALEUR PAR DÉFAUT :

Pré-authentification activée par défaut

2.1.14 *Gestion des comptes d'urgence (Break-Glass)*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les comptes d'urgence permettent la récupération en cas de crise. Ils doivent être sécurisés, surveillés et testés régulièrement.

```
# Comptes d'urgence configurés
Get-ADUser -Filter {Description -like "*break*glass*" -or Description -like "*emergency*"} -Properties Description,LastLogonDate,Pa
```

REMÉDIATION :

1. Créer 2 comptes d'urgence avec mots de passe complexes
2. Stocker les credentials dans des coffres physiques séparés
3. Tester semestriellement l'accès

VALEUR PAR DÉFAUT :

Souvent aucun compte d'urgence formalisé

2.1.15 *Local Administrator Password Solution (LAPS)*

MITRE ATT&CK : T1078.003

DESCRIPTION :

LAPS gère automatiquement les mots de passe des comptes administrateur local, éliminant les mots de passe identiques sur tous les postes.

```
# LAPS déployé
Get-ADOrganizationalUnit -Filter * | Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwdExpirationTime | Where-Object {$_.'ms-Mcs-Ad
```

REMÉDIATION :

1. Déployer LAPS sur tous les postes/serveurs
2. Configurer des mots de passe complexes (14+ caractères)
3. Limiter l'accès aux mots de passe LAPS

VALEUR PAR DÉFAUT :

LAPS non déployé

2.1.16 *Audit des membres de groupes sensibles*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Certains groupes built-in accordent des privilèges élevés. Leur membership doit être strictement contrôlé et régulièrement audité.

```
# Groupes privilégiés à auditer
$groups = @("Account Operators","Backup Operators","Print Operators","Server Operators","Cert Publishers")
foreach($group in $groups) {
    Get-ADGroupMember $group | Select @{N='Group';E={$group}},Name,SamAccountName
}
```

REMÉDIATION :

1. Vider les groupes non utilisés
2. Documenter et justifier chaque membership
3. Implémenter des revues trimestrielles

VALEUR PAR DÉFAUT :

Groupes souvent peuplés par défaut

2.1.17 *Protection des comptes de synchronisation*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les comptes utilisés pour la synchronisation AD Connect, LDAP, etc. ont souvent des privilèges élevés et doivent être particulièrement protégés.

```
# Comptes de service de synchronisation
Get-ADUser -Filter {Description -like "*sync*" -or Description -like "*connect*" -or Name -like "*sync*"} -Properties Description,m
```

REMÉDIATION :

1. Utiliser des comptes dédiés avec privilèges minimaux
2. Implémenter MFA si supporté
3. Surveiller l'activité de ces comptes

VALEUR PAR DÉFAUT :

Souvent des privilèges excessifs

2.1.18 *Contrôle des comptes avec mots de passe n'expirant jamais*

MITRE ATT&CK : T1078

DESCRIPTION :

Les comptes avec mots de passe n'expirant jamais créent un risque de sécurité permanent. Cette configuration doit être limitée aux comptes techniques justifiés.

```
# Comptes avec PasswordNeverExpires
Get-ADUser -Filter {PasswordNeverExpires -eq $true -and Enabled -eq $true} -Properties PasswordNeverExpires,PasswordLastSet,Descrip
```

REMÉDIATION :

1. Migrer vers gMSA pour les comptes de service
2. Implémenter la rotation pour les comptes restants
3. Justifier et documenter les exceptions

VALEUR PAR DÉFAUT :

Policy de domaine appliquée

2.1.19 *Configuration Just Enough Administration (JEA)*

MITRE ATT&CK : T1078.002

DESCRIPTION :

JEA permet de limiter les cmdlets et paramètres disponibles dans les sessions PowerShell privilégiées, appliquant le principe du moindre privilège.

```
# Endpoints JEA configurés
Get-PSSessionConfiguration | Where-Object {$_.Permission -notlike "*Full Control*"}
# Sessions JEA actives
Get-PSSession | Where-Object {$_.ConfigurationName -ne "Microsoft.PowerShell"}
```

REMÉDIATION :

1. Créer des endpoints JEA pour les tâches admin courantes
2. Former les administrateurs à l'utilisation JEA
3. Désactiver les sessions PowerShell complètes quand possible

VALEUR PAR DÉFAUT :

Sessions PowerShell complètes autorisées

2.1.20 *Surveillance des connexions privilégiées*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Toutes les connexions avec des comptes privilégiés doivent être loggées et surveillées pour détecter les usages non autorisés.

```
# Audit des logons privilégiés récents
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624,4625} |
Where-Object {$_.Message -like "*Domain Admins*" -or $_.Message -like "*Enterprise Admins*"}
```

REMÉDIATION :

1. Activer l'audit détaillé des logons (succès et échecs)
2. Corréler les connexions avec les justifications métier
3. Alerter sur les connexions suspectes (horaires, sources)

VALEUR PAR DÉFAUT :

Audit basique activé

2.1.21 *Protection contre le vol de credentials*

MITRE ATT&CK : T1003.001

DESCRIPTION :

Windows Credential Guard, LSA Protection et autres mécanismes protègent contre l'extraction de credentials de la mémoire.

```
# Credential Guard activé
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard | Select VirtualizationBasedSecurityStat
```

REMÉDIATION :

1. Activer Credential Guard sur tous les PAW/serveurs
2. Configurer LSA Protection
3. Implémenter Windows Defender Application Guard

VALEUR PAR DÉFAUT :

Fonctionnalités désactivées

2.1.22 *Audit des droits utilisateur sensibles*

MITRE ATT&CK : T1078

DESCRIPTION :

Certains droits utilisateur (SeDebugPrivilege, SeBackupPrivilege, etc.) accordent des capacités équivalentes aux privilèges administrateur et doivent être contrôlés.

```
# Droits utilisateur sensibles
secedit /export /cfg security.cfg
Get-Content security.cfg | Select-String "SeTcbPrivilege|SeDebugPrivilege|SeBackupPrivilege|SeRestorePrivilege|SeLoadDriverPrivileg
```

REMÉDIATION :

1. Auditer tous les droits utilisateur sensibles
2. Supprimer les assignations non justifiées
3. Documenter les besoins métier légitimes

VALEUR PAR DÉFAUT :

Souvent assignés par défaut à des groupes

2.1.23 *Contrôle des Service Principal Names (SPN) dupliqués*

MITRE ATT&CK : T1558.003

DESCRIPTION :

Les SPN dupliqués peuvent causer des erreurs d'authentification Kerberos et permettre des attaques par confusion de services.

```
# Recherche de SPN dupliqués
setspn -X
# SPN par compte
Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties ServicePrincipalName | Select Name,ServicePrincipalName
```

REMÉDIATION :

1. Supprimer les SPN dupliqués ou obsolètes
2. Standardiser la nomenclature des SPN
3. Auditer régulièrement les nouvelles créations

VALEUR PAR DÉFAUT :

Vérification manuelle des SPN

2.1.24 *Gestion des comptes de liaison AD (Binding Accounts)*

MITRE ATT&CK : T1078.003

DESCRIPTION :

Les comptes utilisés pour lier les applications à AD (LDAP bind) doivent avoir des privilèges minimaux et des mots de passe forts.

```
# Comptes de liaison identifiés
Get-ADUser -Filter {Description -like "*bind*" -or Description -like "*ldap*" -or Description -like "*app*"} -Properties Descriptio
```

REMÉDIATION :

1. Identifier tous les comptes de liaison applicative
2. Limiter aux privilèges Read strictement nécessaires
3. Implémenter la rotation des mots de passe

VALEUR PAR DÉFAUT :

Souvent des privilèges excessifs

2.1.25 *Protection des hash NTLM des comptes privilégiés*

MITRE ATT&CK : T1003.002

DESCRIPTION :

Les hash NTLM des comptes privilégiés sont des cibles de choix pour les attaques Pass-the-Hash. Des protections spécifiques doivent être mises en place.

```
# Comptes avec "Account is sensitive and cannot be delegated"
Get-ADUser -Filter {AccountNotDelegated -eq $true} -Properties AccountNotDelegated,AdminCount
# Protected Users group membership
Get-ADGroupMember "Protected Users"
```

REMÉDIATION :

1. Ajouter les comptes privilégiés au groupe "Protected Users"
2. Activer "Account is sensitive and cannot be delegated"
3. Implémenter Credential Guard

VALEUR PAR DÉFAUT :

Pas de protection spéciale des hash NTLM

3.0 — MOTS DE PASSE & AUTHENTIFICATION

3.1.1 *Configuration de la politique de mots de passe par défaut*

MITRE ATT&CK : T1110.001

DESCRIPTION :

La Default Domain Policy définit les exigences minimales de mots de passe pour tous les utilisateurs. Elle doit être configurée selon les bonnes pratiques actuelles.

```
# Politique de domaine actuelle
Get-ADDefaultDomainPasswordPolicy
# Vérification via GPO
Get-GPOReport -Name "Default Domain Policy" -ReportType XML | Select-String -Pattern "Password|Account"
```

REMÉDIATION :

1. Minimum 14 caractères (ou 12 avec complexité)
2. Historique 24 mots de passe
3. Âge maximum 365 jours (ou plus avec MFA)
4. Seuil de verrouillage 10 tentatives

VALEUR PAR DÉFAUT :

7 caractères, complexité activée, 42 jours

3.1.2 *Implémentation des Fine-Grained Password Policies (FGPP)*

MITRE ATT&CK : T1110.001

DESCRIPTION :

Les FGPP permettent d'appliquer des politiques différenciées selon les groupes d'utilisateurs, avec des exigences renforcées pour les comptes privilégiés.

```
# FGPP configurées
Get-ADFineGrainedPasswordPolicy -Filter *
# Application aux groupes
Get-ADFineGrainedPasswordPolicy -Filter * | Get-ADFineGrainedPasswordPolicySubject
```

REMÉDIATION :

1. FGPP stricte pour les comptes privilégiés (20+ caractères)
2. FGPP modérée pour les comptes de service (16+ caractères)
3. FGPP standard pour les utilisateurs (12+ caractères)

VALEUR PAR DÉFAUT :

Aucune FGPP configurée

3.1.3 *Surveillance des mots de passe faibles*

MITRE ATT&CK : T1110.001

DESCRIPTION :

Des outils comme DSInternals permettent d'identifier les mots de passe faibles dans AD sans les casser, permettant une remédiation proactive.

```
# Utilisation d'outils de test (DSInternals)
# Get-ADReplAccount -All -Server DC01 | Test-PasswordQuality -WeakPasswordsFile common-passwords.txt
# Comptes sans changement récent
Get-ADUser -Filter * -Properties PasswordLastSet | Where-Object {(Get-Date) - $_.PasswordLastSet -gt 365}
```

REMÉDIATION :

1. Scanner régulièrement avec des dictionnaires
2. Forcer le changement des mots de passe faibles
3. Former les utilisateurs aux bonnes pratiques

VALEUR PAR DÉFAUT :

Pas de test proactif des mots de passe

3.1.4 *Protection contre les attaques par pulvérisation (Password Spraying)*

MITRE ATT&CK : T1110.003

DESCRIPTION :

Les attaques par pulvérisation testent des mots de passe communs contre de nombreux comptes. La détection nécessite une surveillance des échecs d'authentification distribués.

```
# Échecs de connexion récents
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4625} -MaxEvents 1000 |
Group-Object {$_.Properties[5].Value} | Sort-Object Count -Descending | Select Name,Count
```

REMÉDIATION :

1. Surveiller les échecs d'auth multiples sur des comptes différents
2. Implémenter des délais progressifs
3. Bloquer les IP suspectes automatiquement

VALEUR PAR DÉFAUT :

Détection basée sur seuils par compte

3.1.5 *Configuration de l'authentification multi-facteurs (MFA)*

MITRE ATT&CK : T1078

DESCRIPTION :

MFA ajoute une couche de sécurité critique, particulièrement pour les comptes privilégiés et l'accès distant.

```
# Utilisateurs avec MFA configuré (Azure AD)
# Connect-AzureAD; Get-AzureADUser -All $true | Where-Object {$_.StrongAuthenticationRequirements}
# Smart card logon requis
Get-ADUser -Filter {SmartCardLogonRequired -eq $true} -Properties SmartCardLogonRequired
```

REMÉDIATION :

1. MFA obligatoire pour tous les comptes privilégiés
2. MFA pour l'accès VPN/distant
3. Smart cards ou Windows Hello for Business

VALEUR PAR DÉFAUT :

MFA non configuré par défaut

3.1.6 *Audit des comptes avec mots de passe réversibles*

MITRE ATT&CK : T1003.002

DESCRIPTION :

Le stockage des mots de passe avec chiffrement réversible équivaut à les stocker en clair. Cette configuration doit être évitée.

```
# Comptes avec mots de passe réversibles
Get-ADUser -Filter {AllowReversiblePasswordEncryption -eq $true} -Properties AllowReversiblePasswordEncryption
# Politique de domaine
Get-ADDefaultDomainPasswordPolicy | Select ReversibleEncryptionEnabled
```

REMÉDIATION :

1. Désactiver le chiffrement réversible dans la politique
2. Corriger les comptes individuels si nécessaire
3. Forcer le changement de mot de passe après correction

VALEUR PAR DÉFAUT :

Désactivé par défaut

3.1.7 *Surveillance des tentatives de connexion suspectes*

MITRE ATT&CK : T1078

DESCRIPTION :

La surveillance proactive des patterns de connexion anormaux permet de détecter rapidement les compromissions de comptes.

```
# Connexions en dehors des heures normales
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} |
Where-Object {$_.TimeCreated.Hour -lt 6 -or $_.TimeCreated.Hour -gt 22}
```

REMÉDIATION :

1. Définir des profils de connexion par utilisateur/groupe
2. Alerter sur les déviations (horaires, géolocalisation, etc.)
3. Implémenter des règles SIEM adaptées

VALEUR PAR DÉFAUT :

Surveillance manuelle des logs

3.1.8 *Contrôle des comptes avec pré-authentification Kerberos désactivée*

MITRE ATT&CK : T1558.004

DESCRIPTION :

La désactivation de la pré-authentification Kerberos expose les comptes aux attaques AS-REP Roasting.

```
Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties DoesNotRequirePreAuth,PasswordLastSet
```

REMÉDIATION :

1. Réactiver la pré-authentification sur tous les comptes
2. Si impossible pour compatibilité, renforcer les mots de passe
3. Surveiller les événements 4768 avec code d'erreur 0x18

VALEUR PAR DÉFAUT :

Pré-authentification activée

3.1.9 *Configuration des politiques de verrouillage de compte*

MITRE ATT&CK : T1110.001

DESCRIPTION :

Les politiques de verrouillage protègent contre les attaques par force brute tout en évitant les dénis de service.

```
Get-ADDefaultDomainPasswordPolicy | Select LockoutThreshold,LockoutDuration,LockoutObservationWindow
```

REMÉDIATION :

1. Seuil: 10 tentatives (balance sécurité/usabilité)
2. Durée: 15-30 minutes ou déverrouillage manuel
3. Fenêtre d'observation: 15 minutes

VALEUR PAR DÉFAUT :

Souvent pas de verrouillage configuré

3.1.10 *Audit des comptes avec mots de passe n'expirant jamais*

MITRE ATT&CK : T1078

DESCRIPTION :

Les mots de passe permanents créent un risque de compromission à long terme. Seuls les comptes techniques justifiés devraient en bénéficier.

```
Get-ADUser -Filter {PasswordNeverExpires -eq $true -and Enabled -eq $true} -Properties PasswordNeverExpires,PasswordLastSet,Descrip
```

REMÉDIATION :

1. Migrer vers gMSA pour les comptes de service
2. Justifier chaque exception
3. Implémenter la rotation même pour les exceptions

VALEUR PAR DÉFAUT :

Policy s'applique à tous sauf exceptions

3.1.11 *Protection contre les attaques de credential stuffing*

MITRE ATT&CK : T1110.004

DESCRIPTION :

Les attaquants utilisent des bases de données de mots de passe volés. La protection nécessite la détection de patterns automatisés.

```
# Échecs multiples depuis mêmes sources
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4625} |
Group-Object {$_.Properties[19].Value} | Sort-Object Count -Descending
```

REMÉDIATION :

1. Corréler les échecs par IP source
2. Implémenter des CAPTCHAs après plusieurs échecs
3. Bloquer automatiquement les sources suspectes

VALEUR PAR DÉFAUT :

Pas de protection spécifique

3.1.12 *Configuration de Windows Hello for Business*

MITRE ATT&CK : T1078

DESCRIPTION :

Windows Hello for Business remplace les mots de passe par une authentification biométrique ou PIN, éliminant plusieurs vecteurs d'attaque.

```
# Utilisateurs avec WHfB configuré
Get-ADUser -Filter * -Properties msDS-KeyCredentialLink | Where-Object {$_."msDS-KeyCredentialLink"}
```

REMÉDIATION :

1. Déployer WHfB via GPO
2. Configurer les certificats nécessaires
3. Former les utilisateurs à l'adoption

VALEUR PAR DÉFAUT :

Non configuré par défaut

3.1.13 *Surveillance des changements de mots de passe fréquents*

MITRE ATT&CK : T1078

DESCRIPTION :

Des changements de mots de passe anormalement fréquents peuvent indiquer une compromission ou un dysfonctionnement.

```
# Changements récents fréquents
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4723,4724} |
Group-Object {$_.Properties[0].Value} | Where-Object {$_.Count -gt 5}
```

REMÉDIATION :

1. Surveiller les événements 4723/4724
2. Investiguer les changements anormaux
3. Corréler avec d'autres indicateurs de compromission

VALEUR PAR DÉFAUT :

Logs standard disponibles

3.1.14 *Contrôle des mots de passe par défaut des comptes système*

MITRE ATT&CK : T1078.003

DESCRIPTION :

Certains comptes système peuvent avoir des mots de passe par défaut ou prévisibles. Ils doivent être identifiés et sécurisés.

```
# Comptes système avec mots de passe potentiellement faibles
Get-ADUser -Filter {Name -like "SUPPORT_*" -or Name -like "IWAM_*" -or Name -like "IUSR_*"} -Properties PasswordLastSet
```

REMÉDIATION :

1. Identifier tous les comptes système
2. Changer les mots de passe par défaut
3. Désactiver les comptes non utilisés

VALEUR PAR DÉFAUT :

Mots de passe souvent prévisibles

3.1.15 *Audit des authentifications interactives sur les serveurs*

MITRE ATT&CK : T1078

DESCRIPTION :

Les connexions interactives sur les serveurs (console, RDP) doivent être limitées et surveillées, particulièrement sur les DC.

```
# Connexions interactives récentes sur serveurs
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} |
Where-Object {$_.Properties[8].Value -eq 2 -or $_.Properties[8].Value -eq 10}
```

REMÉDIATION :

1. Limiter les droits de connexion interactive
2. Surveiller toutes les connexions serveur
3. Privilégier la gestion à distance sécurisée

VALEUR PAR DÉFAUT :

Connexions interactives souvent autorisées

3.1.16 *Configuration des Smart Cards et certificats*

MITRE ATT&CK : T1078

DESCRIPTION :

Les smart cards fournissent une authentification forte basée sur certificats, éliminant les risques liés aux mots de passe.

```
# Comptes configurés pour smart card
Get-ADUser -Filter {SmartCardLogonRequired -eq $true} -Properties SmartCardLogonRequired,UserCertificate
# Templates de certificats pour smart card
certlm.msc # Vérification manuelle des templates
```

REMÉDIATION :

1. Déployer des smart cards pour les comptes privilégiés
2. Configurer les templates de certificats appropriés
3. Implémenter la révocation de certificats

VALEUR PAR DÉFAUT :

Smart cards non configurées

3.1.17 *Protection contre l'énumération de comptes*

MITRE ATT&CK : T1087.002

DESCRIPTION :

L'énumération de comptes permet aux attaquants d'identifier des cibles. Certaines protections peuvent limiter cette reconnaissance.

```
# Permissions d'énumération sur les containers utilisateurs
dsacls "CN=Users,DC=domain,DC=com" | findstr "Everyone\|Authenticated Users"
```

REMÉDIATION :

1. Limiter les permissions de lecture sur les objets utilisateur
2. Surveiller les requêtes LDAP suspectes
3. Implémenter des honeypots/comptes leurres

VALEUR PAR DÉFAUT :

Énumération généralement possible

3.1.18 *Audit des connexions avec des comptes de service*

MITRE ATT&CK : T1078.003

DESCRIPTION :

Les comptes de service ne devraient pas être utilisés pour des connexions interactives. Toute utilisation doit être surveillée.

```
# Connexions interactives avec comptes de service
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} |
Where-Object {$_.Properties[5].Value -like "*svc*" -or $_.Properties[5].Value -like "*service*"}
```

REMÉDIATION :

1. Bloquer les connexions interactives pour les comptes de service
2. Surveiller toute utilisation anormale
3. Séparer clairement comptes utilisateur/service

VALEUR PAR DÉFAUT :

Pas de restriction par défaut

3.1.19 *Configuration des politiques de session*

MITRE ATT&CK : T1078

DESCRIPTION :

Les sessions doivent avoir des durées limitées et des politiques de verrouillage automatique pour réduire l'exposition.

```
# Politiques de session via GPO
Get-GPOReport -All -ReportType XML | Select-String -Pattern "ScreenSaver\|IdleTime\|SessionTime"
```

REMÉDIATION :

1. Timeout automatique après 15 minutes d'inactivité
2. Déconnexion forcée après durée maximale
3. Écran de verrouillage avec mot de passe requis

VALEUR PAR DÉFAUT :

Sessions souvent permanentes

3.1.20 *Surveillance des comptes avec privilèges de connexion étendus*

MITRE ATT&CK : T1078

DESCRIPTION :

Certains comptes peuvent avoir des droits de connexion sur plusieurs systèmes. Ces privilèges étendus doivent être contrôlés.

```
# Droits "Log on as a service" étendus
secedit /export /cfg security.cfg
Get-Content security.cfg | Select-String "SeServiceLogonRight"
```

REMÉDIATION :

1. Auditer tous les droits de connexion étendus
2. Limiter aux besoins stricts
3. Documenter et justifier chaque assignation

VALEUR PAR DÉFAUT :

Droits souvent accordés largement

4.0 — KERBEROS & PROTOCOLES

4.1.1 *Configuration du chiffrement Kerberos AES256*

MITRE ATT&CK : T1558

DESCRIPTION :

RC4 est cryptographiquement faible. AES256 doit être privilégié pour toutes les communications Kerberos pour résister aux attaques de type Kerberoasting avancées.

```
# Types de chiffrement supportés par le domaine
Get-ADDomain | Select msDS-SupportedEncryptionTypes
# Comptes utilisant encore RC4
Get-ADUser -Filter * -Properties msDS-SupportedEncryptionTypes | Where-Object {$_."msDS-SupportedEncryptionTypes" -band 4}
```

REMÉDIATION :

1. Configurer AES256 sur tous les comptes et services
2. Désactiver RC4 progressivement après tests
3. Mettre à jour les applications non compatibles

VALEUR PAR DÉFAUT :

RC4 souvent encore utilisé

4.1.2 *Rotation du mot de passe KRBTGT*

MITRE ATT&CK : T1558.001

DESCRIPTION :

Le compte KRBTGT chiffre les tickets Kerberos. Sa compromission permet les Golden Ticket attacks. Le mot de passe doit être roté semestriellement.

```
Get-ADUser krbtgt -Properties PasswordLastSet,msDS-KeyVersionNumber
# Calculer l'âge du mot de passe
$krbtgt = Get-ADUser krbtgt -Properties PasswordLastSet
(Get-Date) - $krbtgt.PasswordLastSet
```

REMÉDIATION :

1. Utiliser l'outil Microsoft New-KrbtgtKeys.ps1
2. Effectuer la rotation sur tous les DC
3. Attendre la réplication complète entre rotations

VALEUR PAR DÉFAUT :

Jamais changé depuis création

4.1.3 *Contrôle de la délégation Kerberos non contrainte*

MITRE ATT&CK : T1558.003

DESCRIPTION :

La délégation non contrainte permet à un service de s'authentifier vers n'importe quel service au nom de l'utilisateur. Très dangereux pour l'élévation de privilèges.

```
# Objets avec délégation non contrainte (hors DCs)
Get-ADComputer -Filter {TrustedForDelegation -eq $true -and PrimaryGroupID -ne 516} -Properties TrustedForDelegation,ServicePrincip
Get-ADUser -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation,ServicePrincipalName
```

REMÉDIATION :

1. Migrer vers délégation contrainte ou RBCD
2. Désactiver sur tous les objets non-DC
3. Surveiller les nouvelles configurations

VALEUR PAR DÉFAUT :

Potentiellement configurée sur comptes de service

4.1.4 *Configuration de la délégation contrainte*

MITRE ATT&CK : T1558.003

DESCRIPTION :

La délégation contrainte limite les services vers lesquels un objet peut déléguer. Plus sûre que la délégation non contrainte mais nécessite une configuration précise.

```
# Objets avec délégation contrainte
Get-ADComputer -Filter * -Properties msDS-AllowedToDelegateTo | Where-Object {$_."msDS-AllowedToDelegateTo"}
Get-ADUser -Filter * -Properties msDS-AllowedToDelegateTo | Where-Object {$_."msDS-AllowedToDelegateTo"}
```

REMÉDIATION :

1. Configurer uniquement les SPN strictement nécessaires
2. Auditer régulièrement les configurations
3. Tester l'impact sur les applications

VALEUR PAR DÉFAUT :

Aucune délégation contrainte configurée

4.1.5 *Implémentation de la délégation contrainte basée sur les ressources (RBCD)*

MITRE ATT&CK : T1558.003

DESCRIPTION :

RBCD inverse le contrôle de délégation vers la ressource cible, offrant une granularité et sécurité supérieures.

```
# Objets avec RBCD configuré
Get-ADComputer -Filter * -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Where-Object {$_."msDS-AllowedToActOnBehalfOfOtherI
```

REMÉDIATION :

1. Migrer la délégation contrainte vers RBCD
2. Configurer des ACL précises sur msDS-AllowedToActOnBehalfOfOtherIdentity
3. Tester soigneusement les changements

VALEUR PAR DÉFAUT :

RBCD non configurée

4.1.6 *Restriction du protocole NTLM*

MITRE ATT&CK : T1557.001

DESCRIPTION :

NTLM est vulnérable aux attaques de relais et de craquage. Kerberos doit être privilégié avec NTLM restreint ou désactivé progressivement.

```
# Configuration NTLM actuelle
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" -Name "NTLMMinServerSec"
```

REMÉDIATION :

1. LmCompatibilityLevel = 5 (NTLMv2 uniquement)
2. Auditer l'utilisation NTLM avec l'Event 4624
3. Planifier la désactivation progressive par zone

VALEUR PAR DÉFAUT :

NTLM souvent autorisé (niveau 3)

4.1.7 *Configuration du LDAP Signing*

MITRE ATT&CK : T1557.001

DESCRIPTION :

LDAP Signing protège contre les attaques man-in-the-middle sur les communications LDAP. Doit être requis sur tous les DC.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name "LDAPServerIntegrity"
# 0=None, 1=Negotiate, 2=Require
```

REMÉDIATION :

1. LDAPServerIntegrity = 2 (obligatoire)
2. Tester la compatibilité avec les applications legacy
3. Implémenter progressivement si nécessaire

VALEUR PAR DÉFAUT :

1 (négocié) sur Windows Server 2019+

4.1.8 *Activation du LDAP Channel Binding*

MITRE ATT&CK : T1557.001

DESCRIPTION :

LDAP Channel Binding ajoute une protection contre les attaques de relais LDAPS en liant la session TLS au canal sécurisé.

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name "LdapEnforceChannelBinding"
# 0=Never, 1=When supported, 2=Always
```

REMÉDIATION :

1. LdapEnforceChannelBinding = 2 (toujours)
2. Vérifier que tous les clients supportent le channel binding
3. Monitorer les erreurs de connexion après activation

VALEUR PAR DÉFAUT :

0 (jamais) sur la plupart des configurations

4.1.9 *Protection contre les attaques Golden Ticket*

MITRE ATT&CK : T1558.001

DESCRIPTION :

Les Golden Tickets exploitent le hash KRBTGT pour créer des tickets valides arbitraires. La détection nécessite surveillance et rotation régulière.

```
# Surveillance des tickets avec durées de vie anormales
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4769} |
Where-Object {$_.Properties[6].Value -gt 600} # Tickets > 10h
```

REMÉDIATION :

1. Rotation semestrielle du KRBTGT
2. Surveiller les tickets avec durées de vie élevées
3. Implémenter des alertes sur les activités privilégiées suspectes

VALEUR PAR DÉFAUT :

Pas de protection spécifique

4.1.10 *Détection des attaques Silver Ticket*

MITRE ATT&CK : T1558.002

DESCRIPTION :

Les Silver Tickets exploitent les hash de comptes de service pour accéder à des services spécifiques. La rotation des mots de passe et gMSA offrent une protection.

```
# Comptes de service avec mots de passe anciens
Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties ServicePrincipalName,PasswordLastSet |
Where-Object {(Get-Date) - $_.PasswordLastSet -gt 180}
```

REMÉDIATION :

1. Migration vers gMSA pour rotation automatique
2. Rotation régulière des mots de passe de service
3. Surveillance des accès service anormaux

VALEUR PAR DÉFAUT :

Mots de passe de service souvent anciens

4.1.11 *Configuration des tickets Kerberos - durées de vie*

MITRE ATT&CK : T1558

DESCRIPTION :

Les durées de vie des tickets Kerberos doivent être limitées pour réduire la fenêtre d'exploitation en cas de vol.

```
# Politique Kerberos du domaine
Get-ADDefaultDomainPasswordPolicy | Select MaxTicketAge,MaxServiceAge,MaxClockSkew
```

REMÉDIATION :

1. MaxTicketAge: 10 heures maximum
2. MaxServiceAge: 600 minutes maximum
3. MaxClockSkew: 5 minutes maximum

VALEUR PAR DÉFAUT :

10h pour TGT, 600min pour service tickets

4.1.12 *Surveillance des événements Kerberos suspects*

MITRE ATT&CK : T1558

DESCRIPTION :

Certains patterns d'événements Kerberos peuvent indiquer des attaques (Kerberoasting, AS-REP roasting, Golden tickets).

```
# Événements Kerberos critiques
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4768,4769,4771} -MaxEvents 1000 |
Group-Object Id | Select Name,Count
```

REMÉDIATION :

1. Surveiller Event 4769 (TGS) pour Kerberoasting
2. Surveiller Event 4768 (TGT) pour AS-REP roasting
3. Alerter sur les codes d'erreur spécifiques

VALEUR PAR DÉFAUT :

Logging basique activé

4.1.13 *Protection contre Pass-the-Hash (PtH)*

MITRE ATT&CK : T1550.002

DESCRIPTION :

Les attaques PtH utilisent les hash NTLM pour s'authentifier. Les protections incluent NTLM restrictions, Credential Guard, et Protected Users group.

```
# Membres du groupe Protected Users
Get-ADGroupMember "Protected Users"
# Credential Guard activé
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard
```

REMÉDIATION :

1. Ajouter les comptes privilégiés au groupe "Protected Users"
2. Activer Credential Guard sur postes/serveurs critiques
3. Restreindre l'utilisation NTLM

VALEUR PAR DÉFAUT :

Protections souvent désactivées

4.1.14 *Protection contre Pass-the-Ticket (PtT)*

MITRE ATT&CK : T1550.003

DESCRIPTION :

Les attaques PtT réutilisent des tickets Kerberos volés. La protection nécessite des durées de vie courtes et la surveillance des réutilisations.

```
# Surveillance des réutilisations de tickets
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} |
Where-Object {$_.Properties[10].Value -eq 3} # Logon Type = Network
```

REMÉDIATION :

1. Limiter les durées de vie des tickets
2. Surveiller les connexions réseau multiples avec même ticket
3. Implémenter des restrictions réseau par utilisateur

VALEUR PAR DÉFAUT :

Pas de protection spécifique contre PtT

4.1.15 *Configuration du SMB Signing*

MITRE ATT&CK : T1557.001

DESCRIPTION :

SMB Signing protège contre les attaques de relais SMB en signant cryptographiquement les communications.

```
# Configuration SMB Signing client/serveur
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters" -Name "RequireSecuritySignature"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters" -Name "RequireSecuritySignature"
```

REMÉDIATION :

1. RequireSecuritySignature = 1 sur tous les systèmes
2. Tester la compatibilité avec équipements réseau anciens
3. Implémenter progressivement si nécessaire

VALEUR PAR DÉFAUT :

Souvent désactivé pour compatibilité

4.1.16 *Audit des comptes avec des SPN faibles*

MITRE ATT&CK : T1558.003

DESCRIPTION :

Les comptes avec SPN et mots de passe faibles sont vulnérables au Kerberoasting. Identification et correction nécessaires.

```
# Comptes SPN avec mots de passe potentiellement faibles
Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties ServicePrincipalName,PasswordLastSet,adminCount |
Where-Object {(Get-Date) - $_.PasswordLastSet -gt 365}
```

REMÉDIATION :

1. Mots de passe >25 caractères pour comptes SPN
2. Migration vers gMSA quand possible
3. Rotation régulière des mots de passe

VALEUR PAR DÉFAUT :

Mots de passe souvent insuffisants

4.1.17 *Protection contre DCSync*

MITRE ATT&CK : T1003.006

DESCRIPTION :

DCSync permet d'extraire les hash de mots de passe via la réplication AD. Les permissions DS-Replication-Get-Changes doivent être strictement contrôlées.

```
# Permissions de réplication suspectes
dsacls "DC=domain,DC=com" | findstr "DS-Replication-Get-Changes"
# Objets avec permissions de réplication
Get-ADObject -Filter * -Properties nTSecurityDescriptor | Where-Object {$_.nTSecurityDescriptor -like "*1131f6aa*"}
```

REMÉDIATION :

1. Limiter DS-Replication-Get-Changes aux seuls DC légitimes
2. Surveiller les tentatives de réplication suspectes
3. Alerter sur l'utilisation des permissions de réplication

VALEUR PAR DÉFAUT :

Permissions souvent trop larges

4.1.18 *Configuration de l'audit Kerberos avancé*

MITRE ATT&CK : T1558

DESCRIPTION :

L'audit détaillé des événements Kerberos permet de détecter les attaques sophistiquées et les anomalies d'authentification.

```
# Configuration audit Kerberos
auditpol /get /category:"Account Logon"
auditpol /get /subcategory:"Kerberos Authentication Service"
```

REMÉDIATION :

1. Activer l'audit succès/échec pour tous les événements Kerberos
2. Configurer la rétention appropriée des logs
3. Implémenter des règles SIEM pour détection automatique

VALEUR PAR DÉFAUT :

Audit basique souvent insuffisant

4.1.19 *Contrôle des enclaves Kerberos*

MITRE ATT&CK : T1558

DESCRIPTION :

Les enclaves Kerberos (domaines/forêts) doivent être isolées selon les besoins de sécurité. Les trusts doivent suivre le principe du moindre privilège.

```
# Trusts configurés
Get-ADTrust -Filter * | Select Name,Direction,TrustType,SelectiveAuthentication,SIDFilteringEnabled
```

REMÉDIATION :

1. Limiter les trusts au strict nécessaire
2. Activer Selective Authentication sur trusts externes
3. Vérifier SID Filtering sur tous les trusts

VALEUR PAR DÉFAUT :

Configuration souvent permissive

4.1.20 *Protection contre les attaques Skeleton Key*

MITRE ATT&CK : T1547.005

DESCRIPTION :

L'attaque Skeleton Key injecte un mot de passe maître dans LSASS. La détection nécessite surveillance de l'intégrité et des authentifications anormales.

```
# Vérifier l'intégrité de LSASS
Get-Process lsass | Select ProcessName,Path,FileVersion
# Surveiller les authentifications avec mots de passe suspects
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624}
```

REMÉDIATION :

1. Implémenter LSA Protection
2. Surveiller les modifications de LSASS
3. Utiliser des solutions EDR pour détecter les injections

VALEUR PAR DÉFAUT :

Pas de protection spécifique

4.1.21 *Configuration des protocoles d'authentification legacy*

MITRE ATT&CK : T1078

DESCRIPTION :

Les protocoles legacy (LM, NTLMv1) doivent être désactivés car cryptographiquement faibles et vulnérables.

```
# Configuration protocoles legacy
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "NoLMHash"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel"
```

REMÉDIATION :

1. NoLMHash = 1 (pas de stockage hash LM)
2. LmCompatibilityLevel = 5 (NTLMv2 minimum)
3. Désactiver progressivement tout support legacy

VALEUR PAR DÉFAUT :

Support legacy souvent encore présent

4.1.22 *Surveillance des échecs d'authentification Kerberos*

MITRE ATT&CK : T1558

DESCRIPTION :

Les échecs Kerberos peuvent indiquer des attaques ou des problèmes de configuration. Patterns spécifiques à surveiller selon les codes d'erreur.

```
# Échecs Kerberos par code d'erreur
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4771} |
Group-Object {$_.Properties[6].Value} | Sort-Object Count -Descending
```

REMÉDIATION :

1. Surveiller codes d'erreur 0x6 (compte inexistant), 0x12 (compte désactivé)
2. Alerter sur 0x17 (mot de passe expiré), 0x18 (pré-auth requis)
3. Corréler avec autres événements de sécurité

VALEUR PAR DÉFAUT :

Surveillance réactive des échecs

4.1.23 *Configuration des algorithmes cryptographiques Kerberos*

MITRE ATT&CK : T1558

DESCRIPTION :

Les algorithmes faibles (DES, RC4) doivent être désactivés. AES128/256 et algorithmes futurs doivent être privilégiés.

```
# Algorithmes supportés par le domaine
Get-ADDomain | Select msDS-SupportedEncryptionTypes
# Comptes avec algorithmes faibles
Get-ADUser -Filter * -Properties msDS-SupportedEncryptionTypes | Where-Object {$_."msDS-SupportedEncryptionTypes" -band 7}
```

REMÉDIATION :

1. Désactiver DES (bits 1,2) et RC4 (bit 4) progressivement
2. Activer AES128 (bit 8) et AES256 (bit 16)
3. Tester compatibility avant désactivation complète

VALEUR PAR DÉFAUT :

RC4 souvent encore activé

4.1.24 *Protection contre les attaques de downgrade*

MITRE ATT&CK : T1562.010

DESCRIPTION :

Les attaques de downgrade forcent l'utilisation de protocoles/algorithmes faibles. Configuration stricte nécessaire pour les prévenir.

```
# Configuration minimum de sécurité
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel"
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name "LDAPServerIntegrity"
```

REMÉDIATION :

1. Forcer les protocoles/algorithmes sécurisés uniquement
2. Désactiver la négociation vers protocoles faibles
3. Surveiller les tentatives de downgrade

VALEUR PAR DÉFAUT :

Négociation souvent permissive

4.1.25 *Audit des tickets de service à longue durée*

MITRE ATT&CK : T1558.002

DESCRIPTION :

Les tickets de service avec durées de vie anormalement longues peuvent indiquer des Golden/Silver tickets ou des configurations problématiques.

```
# Tickets avec durées anormales
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4769} |
Where-Object {$_.Properties[6].Value -gt 43200} # > 12 heures
```

REMÉDIATION :

1. Configurer des durées de vie appropriées (≤10h)
2. Surveiller les tickets avec durées excessives
3. Investiguer les sources de tickets anormaux

VALEUR PAR DÉFAUT :

Durées parfois excessives par configuration

4.1.26 *Configuration de la protection Extended Protection for Authentication*

MITRE ATT&CK : T1557.001

DESCRIPTION :

EPA protège contre les attaques de relais en liant l'authentification au canal de communication sécurisé.

```
# Configuration EPA pour différents services
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\LSA" -Name "SuppressExtendedProtection"
```

REMÉDIATION :

1. Activer EPA sur tous les services supportés
2. Configurer les applications pour utiliser EPA
3. Tester la compatibilité avec clients anciens

VALEUR PAR DÉFAUT :

EPA souvent désactivé pour compatibilité

4.1.27 *Surveillance des modifications de configuration Kerberos*

MITRE ATT&CK : T1484

DESCRIPTION :

Les modifications des paramètres Kerberos peuvent affaiblir la sécurité. Surveillance et approbation nécessaires pour tous les changements.

```
# Surveillance des modifications de registre Kerberos
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4657} |
Where-Object {$_.Message -like "*Kerberos*" -or $_.Message -like "*NTDS*"}
```

REMÉDIATION :

1. Auditer toutes les modifications de configuration
2. Implémenter un processus d'approbation des changements
3. Alerter sur les modifications non autorisées

VALEUR PAR DÉFAUT :

Modifications souvent non surveillées

4.1.28 *Protection des communications RPC*

MITRE ATT&CK : T1557.001

DESCRIPTION :

Les communications RPC doivent être sécurisées pour éviter l'interception et la manipulation. Authentification et chiffrement nécessaires.

```
# Configuration sécurité RPC
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Rpc\ClientProtocols" -Name "EnableDCOMHTTP"
```

REMÉDIATION :

1. Activer l'authentification RPC obligatoire
2. Chiffrer les communications RPC sensibles
3. Limiter les endpoints RPC exposés

VALEUR PAR DÉFAUT :

Communications RPC souvent non sécurisées

4.1.29 *Configuration des restrictions de protocole par réseau*

MITRE ATT&CK : T1078

DESCRIPTION :

Différents réseaux peuvent nécessiter des restrictions de protocole variables. Segmentation et politiques adaptées par zone.

```
# Politiques réseau par interface
Get-NetConnectionProfile | Select Name,NetworkCategory,IPv4Connectivity
```

REMÉDIATION :

1. Classifier les réseaux (Domain, Private, Public)
2. Appliquer des restrictions par classification
3. Surveiller les changements de classification réseau

VALEUR PAR DÉFAUT :

Politiques souvent uniformes

4.1.30 *Audit des communications inter-domaines*

MITRE ATT&CK : T1482

DESCRIPTION :

Les communications entre domaines/forêts doivent être surveillées pour détecter les mouvements latéraux et l'abus de trusts.

```
# Authentifications inter-domaines
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} |
Where-Object {$_.Properties[5].Value -like "*@*" -and $_.Properties[5].Value -notlike "*@domain.com"}
```

REMÉDIATION :

1. Surveiller toutes les authentifications inter-domaines
2. Corréler avec les besoins métier légitimes
3. Alerter sur les patterns anormaux

VALEUR PAR DÉFAUT :

Surveillance basique des authentifications

5.0 — SÉCURITÉ GPO

5.1.1 *Permissions sur les GPO critiques*

MITRE ATT&CK : T1484.001

DESCRIPTION :
Les GPO contrôlent la configuration de sécurité de tous les systèmes. Leurs permissions doivent être strictement limitées aux administrateurs autorisés.

```
# Permissions sur GPO critiques
$criticalGPOs = @("Default Domain Policy","Default Domain Controllers Policy")
foreach($gpo in $criticalGPOs) {
    Get-GPPermission -Name $gpo -All | Where-Object {$_.Permission -match "Edit" -and $_.Trustee -notlike "*Admin*"}
}
```

REMÉDIATION :

1. Limiter les permissions Edit aux seuls Domain Admins
2. Supprimer les permissions héritées non nécessaires
3. Auditer régulièrement les permissions GPO

VALEUR PAR DÉFAUT :
Permissions souvent trop permissives

5.1.2 *Protection contre l'hijacking de GPO*

MITRE ATT&CK : T1484.001

DESCRIPTION :
L'hijacking de GPO permet à un attaquant de modifier des politiques pour élever ses privilèges ou établir une persistence. Protection des ACL nécessaire.

```
# GPO avec permissions dangereuses pour utilisateurs non-admin
Get-GPO -All | ForEach-Object {
    Get-GPPermission -Guid $_.Id -All | Where-Object {
        $_.Permission -eq "GpoEditDeleteModifySecurity" -and
        $_.Trustee -notmatch "Admin|SYSTEM|Creator"
    }
}
```

REMÉDIATION :

1. Supprimer toutes les permissions Edit non justifiées
2. Implémenter la séparation des droits (lecture vs modification)
3. Surveiller les modifications de GPO

VALEUR PAR DÉFAUT :
Risque d'hijacking selon permissions

6.0 — SÉCURITÉ DNS AD

6.1.1 *Configuration des zones DNS intégrées AD*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Les zones DNS intégrées à AD bénéficient de la sécurité et réplication AD. Toutes les zones critiques doivent être intégrées.

```
# Zones DNS et leur type
Get-DnsServerZone | Select ZoneName,ZoneType,IsDsIntegrated,SecureSecondaries
# Vérification de l'intégration AD
Get-DnsServerZone | Where-Object {$_.ZoneType -eq "Primary" -and $_.IsDsIntegrated -eq $false}
```

REMÉDIATION :

1. Convertir toutes les zones primaires vers l'intégration AD
2. Configurer la réplication appropriée (ForestDnsZones, DomainDnsZones)
3. Tester la résolution après conversion

VALEUR PAR DÉFAUT :

Nouvelles zones souvent intégrées AD

6.1.2 *Activation des mises à jour dynamiques sécurisées*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Les mises à jour dynamiques non sécurisées permettent à n'importe quel client de modifier les enregistrements DNS. Seules les MAJ sécurisées doivent être autorisées.

```
Get-DnsServerZone | Select ZoneName,DynamicUpdate,SecureSecondaries
# Zones permettant les mises à jour non sécurisées
Get-DnsServerZone | Where-Object {$_.DynamicUpdate -eq "NonsecureAndSecure"}
```

REMÉDIATION :

1. Configurer "Secure only" pour toutes les zones intégrées AD
2. Identifier et corriger les zones non sécurisées
3. Tester l'impact sur l'enregistrement automatique

VALEUR PAR DÉFAUT :

Souvent "NonsecureAndSecure" par défaut

6.1.3 *Configuration DNSSEC pour la validation*

MITRE ATT&CK : T1071.004

DESCRIPTION :

DNSSEC protège contre les attaques d'empoisonnement DNS en validant cryptographiquement les réponses.

```
# Statut DNSSEC
Get-DnsServerZone | Select ZoneName,IsSigned,SigningKeys
# Configuration validation DNSSEC
Get-DnsServerSetting | Select EnableDnsSec,DnsSecValidation
```

REMÉDIATION :

1. Activer DNSSEC sur les zones critiques
2. Configurer la validation DNSSEC sur les serveurs
3. Gérer la rotation des clés DNSSEC

VALEUR PAR DÉFAUT :

DNSSEC souvent non configuré

6.1.4 *Contrôle des transferts de zone DNS*

MITRE ATT&CK : T1016.001

DESCRIPTION :

Les transferts de zone non contrôlés peuvent exposer des informations sur l'infrastructure. Ils doivent être limités aux serveurs autorisés.

```
Get-DnsServerZone | Select ZoneName,SecureSecondaries,SecondaryServers,NotifyServers
# Zones autorisant les transferts vers n'importe qui
Get-DnsServerZone | Where-Object {$_.SecureSecondaries -eq "NoSecurity"}
```

REMÉDIATION :

1. Limiter les transferts aux serveurs spécifiés uniquement
2. Utiliser l'authentification pour les transferts
3. Auditer régulièrement les configurations de transfert

VALEUR PAR DÉFAUT :

Transferts souvent trop permissifs

6.1.5 *Protection contre l'empoisonnement de cache DNS*

MITRE ATT&CK : T1071.004

DESCRIPTION :

L'empoisonnement de cache permet de rediriger le trafic vers des serveurs malveillants. Protection par randomisation et validation nécessaires.

```
# Configuration protection empoisonnement
Get-DnsServerSetting | Select EnablePollutionProtection,BootMethod,Forwarders
# Vérification randomisation des ports source
Get-DnsServerSetting | Select SocketPoolSize,EnableSocketPooling
```

REMÉDIATION :

1. Activer la protection contre la pollution
2. Configurer la randomisation des ports source
3. Utiliser des forwarders sécurisés (DoH/DoT)

VALEUR PAR DÉFAUT :

Protection souvent basique

6.1.6 *Surveillance des requêtes DNS suspectes*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Les requêtes DNS peuvent indiquer des activités malveillantes (C2, exfiltration, reconnaissance). Surveillance et analyse nécessaires.

```
# Activation du logging DNS
Get-DnsServerDiagnostics | Select EnableLogFileRollover,LogFilePath,Queries
# Analyse des requêtes récentes
Get-WinEvent -FilterHashtable @{LogName='DNS Server'} -MaxEvents 100
```

REMÉDIATION :

1. Activer le logging détaillé des requêtes DNS
2. Analyser les patterns de requêtes anormaux
3. Implémenter des règles de détection automatique

VALEUR PAR DÉFAUT :

Logging souvent minimal

6.1.7 *Configuration des forwarders DNS sécurisés*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Les forwarders DNS doivent être fiables et sécurisés pour éviter l'interception ou la manipulation des requêtes externes.

```
Get-DnsServerForwarder | Select IPAddress,EnableReordering,Timeout,UseRootHint
```

REMÉDIATION :

1. Utiliser des forwarders fiables (ISP, CloudFlare, Quad9)
2. Configurer DNS over HTTPS/TLS si supporté
3. Implémenter une redondance des forwarders

VALEUR PAR DÉFAUT :

Forwarders souvent par défaut ISP

6.1.8 *Contrôle des enregistrements DNS critiques*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Les enregistrements DNS critiques (SRV AD, MX, etc.) doivent être protégés contre les modifications non autorisées.

```
# Enregistrements SRV critiques pour AD
nslookup -type=SRV _ldap._tcp.dc._msdcs.domain.com
nslookup -type=SRV _kerberos._tcp.dc._msdcs.domain.com
nslookup -type=SRV _gc._tcp.domain.com
```

REMÉDIATION :

1. Vérifier la présence de tous les enregistrements SRV AD
2. Surveiller les modifications d'enregistrements critiques
3. Sauvegarder régulièrement les configurations DNS

VALEUR PAR DÉFAUT :

Enregistrements créés automatiquement

6.1.9 *Protection des zones de recherche inversée*

MITRE ATT&CK : T1016.001

DESCRIPTION :

Les zones de recherche inversée peuvent révéler des informations sur l'infrastructure. Elles doivent être sécurisées et limitées.

```
# Zones de recherche inversée configurées
Get-DnsServerZone | Where-Object {$_.ZoneName -like "*.in-addr.arpa" -or $_.ZoneName -like "*.ip6.arpa"}
```

REMÉDIATION :

1. Sécuriser les zones de recherche inversée
2. Limiter les informations exposées
3. Considérer la suppression si non nécessaires

VALEUR PAR DÉFAUT :

Zones inversées souvent créées automatiquement

6.1.10 *Configuration des politiques de requête DNS*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Les politiques de requête permettent de filtrer ou rediriger les requêtes DNS selon des critères de sécurité.

```
# Politiques DNS configurées
Get-DnsServerQueryResolutionPolicy | Select Name,Criteria,Action,ProcessingOrder
```

REMÉDIATION :

1. Créer des politiques pour bloquer les domaines malveillants
2. Implémenter la redirection vers des sinkholes
3. Configurer des politiques par source/utilisateur

VALEUR PAR DÉFAUT :

Aucune politique généralement configurée

6.1.11 *Audit des modifications de configuration DNS*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Toutes les modifications de configuration DNS doivent être auditées car elles peuvent affecter la disponibilité et sécurité.

```
# Événements de modification DNS
Get-WinEvent -FilterHashtable @{LogName='DNS Server';ID=2,6,7} |
Select TimeCreated,Id,LevelDisplayName,Message
```

REMÉDIATION :

1. Activer l'audit complet des modifications DNS
2. Surveiller les changements non autorisés
3. Implémenter des alertes temps réel

VALEUR PAR DÉFAUT :

Audit souvent minimal

6.1.12 *Protection contre les attaques DDoS DNS*

MITRE ATT&CK : T1498.002

DESCRIPTION :

Les serveurs DNS sont des cibles fréquentes d'attaques DDoS. Mesures de protection et limitation de taux nécessaires.

```
# Configuration protection DDoS
Get-DnsServerSetting | Select MaximumUdpPacketSize,EnableDuplicateQuerySuppression
Get-DnsServerResponseRateLimiting | Select ResponsesPerSec,WindowInSec
```

REMÉDIATION :

1. Configurer Response Rate Limiting (RRL)
2. Limiter les tailles de paquets UDP
3. Implémenter la suppression des requêtes dupliquées

VALEUR PAR DÉFAUT :

Protection DDoS souvent basique

6.1.13 *Configuration de la réplication DNS sécurisée*

MITRE ATT&CK : T1071.004

DESCRIPTION :

La réplication DNS entre DC doit être sécurisée pour éviter l'interception ou la manipulation des données.

```
# Configuration réplication DNS AD
Get-DnsServerZone | Where-Object {$_.IsDsIntegrated} | Select ZoneName,ReplicationScope
```

REMÉDIATION :

1. Utiliser les partitions DNS AD appropriées
2. Limiter la réplication au scope nécessaire
3. Surveiller la santé de réplication DNS

VALEUR PAR DÉFAUT :

Réplication généralement sécurisée dans AD

6.1.14 *Contrôle des enregistrements DNS obsolètes*

MITRE ATT&CK : T1016.001

DESCRIPTION :

Les enregistrements DNS obsolètes peuvent pointer vers des systèmes compromis ou inexistants, créant des risques de sécurité.

```
# Analyse des enregistrements obsolètes (script custom nécessaire)
Get-DnsServerResourceRecord -ZoneName "domain.com" |
Where-Object {$_.RecordType -eq "A" -or $_.RecordType -eq "CNAME"}
```

REMÉDIATION :

1. Identifier et supprimer les enregistrements obsolètes
2. Implémenter un processus de nettoyage régulier
3. Valider l'existence des systèmes référencés

VALEUR PAR DÉFAUT :

Nettoyage souvent manuel et irrégulier

6.1.15 *Surveillance de la performance DNS*

MITRE ATT&CK : T1498.002

DESCRIPTION :

La performance DNS impacte directement l'authentification AD. Surveillance nécessaire pour détecter les problèmes et attaques.

```
# Statistiques performance DNS
Get-DnsServerStatistics | Select TotalQueries,TotalResponses,QueryDropped,ResponseTimeout
# Test résolution DNS
Measure-Command {nslookup domain.com}
```

REMÉDIATION :

1. Surveiller les métriques de performance DNS
2. Optimiser la configuration selon la charge
3. Implémenter des alertes sur dégradation

VALEUR PAR DÉFAUT :

Surveillance souvent basique

7.0 — RÉPLICATION & CONTRÔLEURS DE DOMAINE

7.1.1 *Surveillance de la santé de réplication AD*

MITRE ATT&CK : T1018

DESCRIPTION :

Les échecs de réplication peuvent causer des incohérences de sécurité et faciliter certaines attaques. Surveillance continue nécessaire.

```
# État de réplication global
repadmin /replsummary
# Échecs de réplication détaillés
Get-ADReplicationFailure -Target * -Scope Domain | Select Server,FirstFailureTime,FailureCount,LastError
```

REMÉDIATION :

1. Corriger immédiatement tous les échecs de réplication
2. Surveiller en continu avec alertes automatiques
3. Investiguer les causes racines des échecs

VALEUR PAR DÉFAUT :

Réplication généralement fonctionnelle

7.1.2 *Configuration sécurisée des Read-Only Domain Controllers (RODC)*

MITRE ATT&CK : T1078

DESCRIPTION :

Les RODC dans les sites distants limitent l'exposition en cas de compromission physique. Configuration PRP (Password Replication Policy) critique.

```
# RODC déployés et leur configuration
Get-ADDomainController -Filter {IsReadOnly -eq $true} | Select Name,Site,IsReadOnly,OperatingSystem
# Password Replication Policy
Get-ADDomainController -Filter {IsReadOnly -eq $true} | ForEach-Object {
    Get-ADAccountResultantPasswordReplicationPolicy -DomainController $_.Name -Identity "Domain Admins"
}
```

REMÉDIATION :

1. Déployer des RODC dans tous les sites à risque
2. Configurer des PRP restrictives (Deny par défaut)
3. Auditer régulièrement les comptes autorisés à répliquer

VALEUR PAR DÉFAUT :

Pas de RODC déployés par défaut

7.1.3 *Protection contre les attaques DCSync*

MITRE ATT&CK : T1003.006

DESCRIPTION :

DCSync permet d'extraire tous les hash de mots de passe via la réplication. Les permissions DS-Replication-Get-Changes doivent être strictement contrôlées.

```
# Permissions de réplication sur le domaine
dsacls "DC=domain,DC=com" | findstr "DS-Replication-Get-Changes"
# Objets avec permissions DCSync
Get-ADObject -SearchBase "DC=domain,DC=com" -Properties nTSecurityDescriptor -Filter * |
Where-Object {$_.nTSecurityDescriptor -like "*1131f6aa*"}
```

REMÉDIATION :

1. Limiter DS-Replication-Get-Changes aux seuls DC
2. Auditer régulièrement ces permissions critiques
3. Surveiller l'utilisation des permissions de réplication

VALEUR PAR DÉFAUT :

Permissions souvent trop larges

7.1.4 *Configuration de SYSVOL avec DFS-R*

MITRE ATT&CK : T1484.001

DESCRIPTION :

La migration de FRS vers DFS-R pour SYSVOL améliore la robustesse et sécurité de la réplication des GPO.

```
# État de la migration SYSVOL vers DFS-R
dfsrdiag ReplicationState /member:DC01
# Vérification cohérence SYSVOL
dcdiag /test:sysvolcheck /v
```

REMÉDIATION :

1. Migrer SYSVOL de FRS vers DFS-R si pas encore fait
2. Vérifier la santé de réplication DFS-R
3. Surveiller la cohérence SYSVOL entre DC

VALEUR PAR DÉFAUT :

DFS-R utilisé par défaut sur WS2008+

7.1.5 *Audit des connexions de réplication manuelles*

MITRE ATT&CK : T1018

DESCRIPTION :

Les connexions de réplication manuelles peuvent perturber la topologie optimale générée par KCC et créer des risques.

```
# Connexions manuelles vs automatiques
Get-ADReplicationConnection -Filter * | Select Name,AutoGenerated,FromServer,ToServer,Options
# Connexions créées manuellement
Get-ADReplicationConnection -Filter {AutoGenerated -eq $false}
```

REMÉDIATION :

1. Documenter toutes les connexions manuelles
2. Valider leur nécessité avec KCC
3. Supprimer les connexions redondantes

VALEUR PAR DÉFAUT :

Topologie gérée automatiquement par KCC

7.1.6 *Surveillance des objets de métadonnées de réplication*

MITRE ATT&CK : T1018

DESCRIPTION :

Les métadonnées de réplication contiennent des informations sensibles sur la topologie et peuvent révéler des cibles d'attaque.

```
# Métadonnées de réplication
repadmin /showmeta "DC=domain,DC=com" /nocache
# Serveurs de réplication par partition
repadmin /showreps
```

REMÉDIATION :

1. Limiter l'accès aux métadonnées de réplication
2. Surveiller les requêtes de métadonnées suspectes
3. Auditer l'utilisation des outils de réplication

VALEUR PAR DÉFAUT :

Accès généralement restreint aux admins

7.1.7 *Configuration des intervalles de réplication*

MITRE ATT&CK : T1018

DESCRIPTION :

Les intervalles de réplication doivent équilibrer convergence rapide des changements de sécurité et charge réseau.

```
# Intervalles de réplication configurés
Get-ADReplicationSiteLink | Select Name,Cost,ReplicationFrequencyInMinutes,Options
# Réplication urgente activée
Get-ADReplicationConnection -Filter * | Select Name,ReplicatedNamingContexts,Options
```

REMÉDIATION :

1. Configurer des intervalles appropriés selon la criticité
2. Activer la réplication d'urgence pour les changements de sécurité
3. Optimiser selon la bande passante disponible

VALEUR PAR DÉFAUT :

180 minutes pour DEFAULTIPSITELINK

7.1.8 *Protection des partitions d'application AD*

MITRE ATT&CK : T1484

DESCRIPTION :

Les partitions d'application (DNS, Configuration) contiennent des données critiques et doivent être protégées.

```
# Partitions d'application existantes
Get-ADObject -SearchBase "CN=Partitions,CN=Configuration,DC=domain,DC=com" -Filter {objectClass -eq "crossRef"} -Properties nCName,
```

REMÉDIATION :

1. Auditer toutes les partitions d'application
2. Contrôler les permissions sur les partitions critiques
3. Surveiller les modifications de structure

VALEUR PAR DÉFAUT :

Partitions DNS créées automatiquement

7.1.9 *Contrôle de la réplication inter-sites*

MITRE ATT&CK : T1018

DESCRIPTION :

La réplication inter-sites doit être optimisée et sécurisée, particulièrement sur les liens WAN.

```
# Configuration des liens de sites
Get-ADReplicationSiteLink | Select Name,SitesIncluded,Cost,ReplicationFrequencyInMinutes,Options
# Ponts de liens de sites
Get-ADReplicationSiteLinkBridge | Select Name,SiteLinksIncluded
```

REMÉDIATION :

1. Optimiser les coûts selon la bande passante réelle
2. Configurer la compression pour les liens lents
3. Surveiller l'utilisation de bande passante

VALEUR PAR DÉFAUT :

Configuration souvent non optimisée

7.1.10 *Audit des modifications de topologie KCC*

MITRE ATT&CK : T1018

DESCRIPTION :

Le Knowledge Consistency Checker (KCC) génère automatiquement la topologie de réplication. Ses modifications doivent être surveillées.

```
# État KCC et dernière exécution
Get-WinEvent -FilterHashtable @{LogName='Directory Service';ID=1864,1865} -MaxEvents 10
# Configuration KCC
repadmin /kcc * /async
```

REMÉDIATION :

1. Surveiller les exécutions KCC et leurs résultats
2. Investiguer les échecs de génération de topologie
3. Valider que KCC fonctionne sur tous les DC

VALEUR PAR DÉFAUT :

KCC fonctionne automatiquement

7.1.11 *Protection contre les attaques DCShadow*

MITRE ATT&CK : T1207

DESCRIPTION :

DCShadow permet de s'enregistrer temporairement comme DC pour injecter des changements malveillants dans AD.

```
# Nouveaux SPN de type DC
Get-ADUser -Filter * -Properties ServicePrincipalNames | Where-Object {
    $_.ServicePrincipalNames -like "*GC/*" -or $_.ServicePrincipalNames -like "*E3514235*"
}
# Nouveaux objets serveur
Get-ADObject -SearchBase "CN=Sites,CN=Configuration,DC=domain,DC=com" -Filter {objectClass -eq "server"} -Properties whenCreated |
Sort-Object whenCreated -Descending
```

REMÉDIATION :

1. Surveiller les créations de SPN de type DC
2. Alerter sur les nouveaux objets server dans Sites
3. Restreindre les permissions ms-DS-MachineAccountQuota

VALEUR PAR DÉFAUT :

Pas de protection spécifique contre DCShadow

7.1.12 *Configuration des Global Catalog servers*

MITRE ATT&CK : T1018

DESCRIPTION :

Le catalogue global facilite les recherches inter-domaines. Configuration et réplication appropriées nécessaires.

```
# Serveurs de catalogue global
Get-ADDomainController -Filter * | Select Name,Site,IsGlobalCatalog,OperatingSystem
# Réplication du catalogue global
Get-ADReplicationPartnerMetadata -Target * -Partition "DC=ForestDnsZones,DC=domain,DC=com"
```

REMÉDIATION :

1. Configurer au moins un GC par site principal
2. Surveiller la réplication des partitions GC
3. Optimiser selon les besoins de recherche

VALEUR PAR DÉFAUT :

GC sur tous les DC en single domain

7.1.13 *Surveillance des tombstones et garbage collection*

MITRE ATT&CK : T1484

DESCRIPTION :

Les objets supprimés deviennent des tombstones avant suppression définitive. Configuration appropriée pour éviter la corruption.

```
# Configuration tombstone lifetime
Get-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=domain,DC=com" -Properties tombstoneLife
# Objets tombstone actuels
Get-ADObject -IncludeDeletedObjects -Filter {isDeleted -eq $true} | Measure-Object
```

REMÉDIATION :

1. Configurer tombstoneLifetime approprié (180 jours recommandé)
2. Surveiller le volume d'objets tombstone
3. Planifier le garbage collection régulièrement

VALEUR PAR DÉFAUT :

180 jours par défaut sur domaines récents

7.1.14 *Contrôle des USN (Update Sequence Numbers)*

MITRE ATT&CK : T1484

DESCRIPTION :

Les USN trackent les modifications AD. Leur surveillance permet de détecter certaines anomalies et attaques.

```
# USN actuels par DC
repadmin /showutdvec DC=domain,DC=com
# Vérification consistance USN
repadmin /showchanges DC=domain,DC=com /statistics
```

REMÉDIATION :

1. Surveiller les progressions USN anormales
2. Investiguer les écarts importants entre DC
3. Utiliser pour la détection de rollback/restore

VALEUR PAR DÉFAUT :

USN gérés automatiquement par AD

7.1.15 *Protection des connexions de réplication*

MITRE ATT&CK : T1557.001

DESCRIPTION :

Les connexions de réplication transportent des données sensibles et doivent être sécurisées.

```
# Configuration sécurité réplication
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name "Repl Perform Initial Synchronizations"
# Ports de réplication utilisés
netstat -an | findstr ":389\|:636\|:3268\|:3269"
```

REMÉDIATION :

1. Utiliser LDAPS (port 636) pour réplication si possible
2. Configurer IPSec pour les connexions inter-sites
3. Limiter les ports de réplication autorisés

VALEUR PAR DÉFAUT :

Réplication souvent non chiffrée

7.1.16 *Audit des opérations de réplication privilégiées*

MITRE ATT&CK : T1003.006

DESCRIPTION :

Certaines opérations de réplication (secrets, mots de passe) doivent être spécifiquement auditées.

```
# Audit réplication de secrets
Get-WinEvent -FilterHashtable @{LogName='Directory Service';ID=4932,4933} -MaxEvents 100
# Réplication RODC Password Replication Policy
Get-WinEvent -FilterHashtable @{LogName='Directory Service';ID=4934,4935} -MaxEvents 100
```

REMÉDIATION :

1. Activer l'audit des opérations de réplication sensibles
2. Surveiller les tentatives de réplication de secrets
3. Alerter sur les patterns anormaux

VALEUR PAR DÉFAUT :

Audit souvent incomplet

7.1.17 *Configuration des notifications de réplication d'urgence*

MITRE ATT&CK : T1484

DESCRIPTION :

Les changements critiques (verrouillage compte, modification privilèges) doivent déclencher une réplication immédiate.

```
# Configuration réplication d'urgence
Get-ADReplicationSiteLink | Select Name,Options
# 0x1 = USE_NOTIFY (réplication d'urgence)
```

REMÉDIATION :

1. Activer USE_NOTIFY sur tous les liens de sites critiques
2. Configurer TWOWAY_SYNC si nécessaire
3. Tester la réplication d'urgence

VALEUR PAR DÉFAUT :

Réplication d'urgence activée par défaut

7.1.18 *Surveillance de la latence de réplication*

MITRE ATT&CK : T1018

DESCRIPTION :

Une latence excessive peut impacter la sécurité (délais de propagation de verrouillages, changements de privilèges).

```
# Latence de réplication actuelle
repadmin /latency /verbose
# Test de réplication manuelle
repadmin /sync "CN=Configuration,DC=domain,DC=com" DC01 DC02
```

REMÉDIATION :

1. Mesurer régulièrement la latence de réplication
2. Optimiser selon les SLA de sécurité
3. Alerter sur les latences excessives

VALEUR PAR DÉFAUT :

Dépend de la configuration réseau et sites

7.1.19 *Configuration du nettoyage des objets liés*

MITRE ATT&CK : T1484

DESCRIPTION :

Les objets liés (backlinks) obsolètes peuvent causer des problèmes de performance et sécurité.

```
# Configuration garbage collection
Get-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=domain,DC=com" -Properties garbageCollPe
```

REMÉDIATION :

1. Configurer garbageCollPeriod approprié (12h par défaut)
2. Surveiller l'efficacité du nettoyage
3. Planifier des nettoyages manuels si nécessaire

VALEUR PAR DÉFAUT :

12 heures par défaut

7.1.20 *Protection contre les conflits de réplication*

MITRE ATT&CK : T1484

DESCRIPTION :

Les conflits de réplication peuvent être exploités pour créer des incohérences de sécurité.

```
# Objets en conflit
Get-ADObject -Filter {Name -like "*CNF:*"} -IncludeDeletedObjects
# Historique des conflits
Get-WinEvent -FilterHashtable @{LogName='Directory Service';ID=1308,1309} -MaxEvents 50
```

REMÉDIATION :

1. Identifier et résoudre tous les conflits de réplication
2. Investiguer les causes des conflits répétés
3. Implémenter la surveillance proactive des conflits

VALEUR PAR DÉFAUT :

Résolution automatique des conflits

8.0 — OBJETS AD & SCHÉMA

8.1.1 *Audit des permissions dangereuses sur objets AD*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les permissions WriteDACL, GenericAll, WriteOwner sur des objets sensibles permettent l'élévation de privilèges et doivent être strictement contrôlées.

```
# Recherche permissions dangereuses
Import-Module ActiveDirectory
$dangerousPerms = @("GenericAll","WriteDacl","WriteOwner","WriteProperty")
Get-ADUser -Filter * -Properties nTSecurityDescriptor | ForEach-Object {
    $acl = $_.nTSecurityDescriptor.Access
    $acl | Where-Object {$_.ActiveDirectoryRights -match ($dangerousPerms -join "|") -and $_.IdentityReference -notmatch "SYSTEM|Ad
}
```

REMÉDIATION :

1. Supprimer toutes les permissions dangereuses non justifiées
2. Implémenter le principe du moindre privilège
3. Auditer régulièrement les ACL critiques

VALEUR PAR DÉFAUT :

Permissions souvent trop permissives

8.1.2 *Protection du conteneur AdminSDHolder*

MITRE ATT&CK : T1484.001

DESCRIPTION :

AdminSDHolder protège les objets privilégiés. Ses ACL sont copiées vers tous les objets protégés. Toute modification peut compromettre la sécurité globale.

```
$adminSDHolder = Get-ADObject -Identity "CN=AdminSDHolder,CN=System,DC=domain,DC=com" -Properties nTSecurityDescriptor
$adminSDHolder.nTSecurityDescriptor.Access | Where-Object {$_.IdentityReference -notmatch "SYSTEM|BUILTIN|NT AUTHORITY"}
```

REMÉDIATION :

1. Restaurer les ACL AdminSDHolder par défaut
2. Surveiller toute modification avec Event 5136
3. Vérifier que SDProp fonctionne (service "Protected Storage")

VALEUR PAR DÉFAUT :

ACL restrictives par défaut

8.1.3 *Contrôle des objets avec adminCount orphelins*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les objets avec adminCount=1 mais non membres de groupes protégés gardent des ACL restrictives héritées. Nettoyage nécessaire.

```
# Objets avec adminCount orphelins
$protectedGroups = @("Domain Admins","Enterprise Admins","Schema Admins","Administrators","Account Operators","Backup Operators","P
Get-ADUser -Filter {adminCount -eq 1} | Where-Object {
    $user = $_
    $isMember = $false
    foreach($group in $protectedGroups) {
        if(Get-ADGroupMember $group -Recursive | Where-Object {$_.SamAccountName -eq $user.SamAccountName}) {
            $isMember = $true; break
        }
    }
    -not $isMember
}
```

REMÉDIATION :

1. Identifier tous les objets avec adminCount orphelins
2. Réinitialiser adminCount à 0 après validation
3. Restaurer l'héritage ACL normal

VALEUR PAR DÉFAUT :

adminCount géré automatiquement par SDProp

8.1.4 *Audit des extensions de schéma non standard*

MITRE ATT&CK : T1484

DESCRIPTION :

Les extensions de schéma sont permanentes et peuvent introduire des vulnérabilités. Audit et documentation nécessaires.

```
# Extensions de schéma custom (OID non Microsoft)
Get-ADObject -SearchBase "CN=Schema,CN=Configuration,DC=domain,DC=com" -Filter {objectClass -eq "attributeSchema" -and attributeID
```

REMÉDIATION :

1. Documenter toutes les extensions de schéma
2. Valider la sécurité des extensions custom
3. Supprimer les extensions obsolètes si possible

VALEUR PAR DÉFAUT :

Schéma standard Microsoft uniquement

8.1.5 *Contrôle des permissions sur les unités d'organisation*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les OUs organisent les objets AD. Leurs permissions déterminent qui peut créer/modifier les objets contenus.

```
# Permissions sur OUs critiques
$criticalOUs = Get-ADOrganizationalUnit -Filter * | Where-Object {$_.Name -match "Admin|Server|Tier"}
foreach($ou in $criticalOUs) {
    dsacls $ou.DistinguishedName | findstr -v "INHERITED\|SUCCESS"
}
```

REMÉDIATION :

1. Limiter les permissions OU selon le modèle de tiering
2. Éviter les permissions génériques (Full Control)
3. Implémenter la délégation granulaire

VALEUR PAR DÉFAUT :

Permissions souvent héritées du domaine

8.1.6 *Surveillance des modifications d'objets critiques*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Certains objets AD sont critiques pour la sécurité. Leurs modifications doivent être surveillées et auditées.

```
# Modifications récentes d'objets critiques
Get-WinEvent -FilterHashtable @{LogName='Security';ID=5136,5137,5141} |
Where-Object {$_.Message -match "CN=AdminSDHolder|CN=Domain Admins|CN=Enterprise Admins|CN=Schema"}
```

REMÉDIATION :

1. Activer l'audit des modifications d'objets AD
2. Surveiller spécifiquement les objets critiques
3. Alerter en temps réel sur les changements

VALEUR PAR DÉFAUT :

Audit souvent incomplet

8.1.7 *Contrôle des quotas de création d'objets*

MITRE ATT&CK : T1484

DESCRIPTION :

Les quotas limitent le nombre d'objets qu'un utilisateur peut créer, prévenant les attaques DoS et l'abus.

```
# Quotas configurés
Get-ADObject -SearchBase "CN=NTDS Quotas,CN=NTDS Settings,CN=Configuration,DC=domain,DC=com" -Filter * -Properties msDS-QuotaAmount
# Utilisation actuelle des quotas
dsquery * -filter "(&(objectClass=user)(msDS-QuotaUsed=*))" -attr distinguishedName,msDS-QuotaUsed
```

REMÉDIATION :

1. Définir des quotas appropriés par type d'utilisateur
2. Surveiller l'utilisation des quotas
3. Alerter sur les tentatives de dépassement

VALEUR PAR DÉFAUT :

ms-DS-MachineAccountQuota = 10 par défaut

8.1.8 *Audit des objets avec SID History*

MITRE ATT&CK : T1134.005

DESCRIPTION :

SID History peut être abusé pour maintenir des privilèges après migration. Audit et nettoyage nécessaires.

```
# Objets avec SID History
Get-ADUser -Filter * -Properties SIDHistory | Where-Object {$_.SIDHistory} | Select Name,SamAccountName,SIDHistory
Get-ADGroup -Filter * -Properties SIDHistory | Where-Object {$_.SIDHistory} | Select Name,SamAccountName,SIDHistory
```

REMÉDIATION :

1. Auditer tous les objets avec SID History
2. Valider la légitimité de chaque SID
3. Nettoyer les SID History obsolètes

VALEUR PAR DÉFAUT :

SID History vide sauf migrations

8.1.9 *Protection contre la manipulation d'attributs sensibles*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Certains attributs AD (memberOf, adminCount, etc.) sont critiques et ne doivent pas être modifiables directement.

```
# Vérification protection attributs sensibles
$sensitiveAttrs = @("memberOf","adminCount","isCriticalSystemObject","nTSecurityDescriptor")
Get-ADObject -SearchBase "CN=Schema,CN=Configuration,DC=domain,DC=com" -Filter {lDAPDisplayName -like "*"} -Properties systemFlags,
Where-Object {$sensitiveAttrs -contains $_.lDAPDisplayName}
```

REMÉDIATION :

1. Vérifier que les attributs sensibles sont protégés (systemFlags)
2. Contrôler les permissions sur les attributs critiques
3. Surveiller les tentatives de modification

VALEUR PAR DÉFAUT :

Protection basée sur systemFlags

8.1.10 *Contrôle des objets dans des conteneurs non standard*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les objets dans des conteneurs non standard (pas dans OUs appropriées) peuvent échapper aux GPO et contrôles.

```
# Utilisateurs hors OUs standard
Get-ADUser -Filter * | Where-Object {$_.DistinguishedName -like "*CN=Users,DC=*" -or $_.DistinguishedName -like "*CN=Builtin,DC=*"}
# Ordinateurs hors OUs standard
Get-ADComputer -Filter * | Where-Object {$_.DistinguishedName -like "*CN=Computers,DC=*"}
```

REMÉDIATION :

1. Déplacer tous les objets vers des OUs appropriées
2. Créer une structure OU cohérente
3. Appliquer les GPO selon la structure

VALEUR PAR DÉFAUT :

Objets souvent dans conteneurs par défaut

8.1.11 *Audit des délégations de contrôle d'OU*

MITRE ATT&CK : T1484.001

DESCRIPTION :

La délégation de contrôle permet de distribuer les responsabilités administratives. Elle doit suivre le principe du moindre privilège.

```
# Délégations configurées sur OUs
Get-ADOrganizationalUnit -Filter * | ForEach-Object {
    $ou = $_.DistinguishedName
    $acl = (Get-ACL "AD:\$ou").Access | Where-Object {$_.IdentityReference -notmatch "SYSTEM|BUILTIN|NT AUTHORITY" -and $_.AccessCo
    if($acl) {
        Write-Output "OU: $ou has custom delegations"
        $acl | Select IdentityReference,ActiveDirectoryRights
    }
}
```

REMÉDIATION :

1. Documenter toutes les délégations de contrôle
2. Valider que chaque délégation respecte le moindre privilège
3. Réviser régulièrement les délégations

VALEUR PAR DÉFAUT :

Délégations souvent ad-hoc et non documentées

8.1.12 *Contrôle des attributs confidentiels*

MITRE ATT&CK : T1087.002

DESCRIPTION :

Certains attributs peuvent contenir des informations sensibles et doivent avoir des permissions de lecture restreintes.

```
# Attributs marqués confidentiels
Get-ADObject -SearchBase "CN=Schema,CN=Configuration,DC=domain,DC=com" -Filter {searchFlags -band 128} -Properties lDAPDisplayName,
```

REMÉDIATION :

1. Identifier les attributs contenant des données sensibles
2. Marquer comme confidentiels (searchFlags bit 7)
3. Contrôler les permissions de lecture

VALEUR PAR DÉFAUT :

Peu d'attributs marqués confidentiels par défaut

8.1.13 *Surveillance des modifications de schéma*

MITRE ATT&CK : T1484

DESCRIPTION :

Les modifications de schéma sont permanentes et affectent toute la forêt. Surveillance stricte nécessaire.

```
# Modifications récentes du schéma
Get-WinEvent -FilterHashtable @{LogName='Directory Service';ID=1137,1138} -MaxEvents 50 | Select TimeCreated,Message
# Version actuelle du schéma
Get-ADObject -Identity "CN=Schema,CN=Configuration,DC=domain,DC=com" -Properties objectVersion
```

REMÉDIATION :

1. Vider le groupe Schema Admins sauf opérations planifiées
2. Auditer toutes les modifications de schéma
3. Documenter les changements et leur impact

VALEUR PAR DÉFAUT :

Groupe Schema Admins vide recommandé

8.1.14 *Protection des liens critiques entre objets*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les liens entre objets AD (memberOf, managedBy, etc.) définissent les relations de privilèges et doivent être protégés.

```
# Liens critiques vers objets privilégiés
Get-ADGroup "Domain Admins" -Properties member,memberOf,managedBy
Get-ADGroup "Enterprise Admins" -Properties member,memberOf,managedBy
```

REMÉDIATION :

1. Surveiller les modifications de liens critiques
2. Implémenter des workflows d'approbation
3. Auditer régulièrement les relations de privilèges

VALEUR PAR DÉFAUT :

Liens gérés par les permissions d'écriture

8.1.15 *Contrôle des objets avec des ACL explicites*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les objets avec ACL explicites (non héritées) peuvent échapper aux contrôles standardisés et créer des risques.

```
# Objets avec héritage désactivé
Get-ADUser -Filter * -Properties nTSecurityDescriptor | Where-Object {
    -not $_.nTSecurityDescriptor.AreAccessRulesProtected
} | Select Name,DistinguishedName
```

REMÉDIATION :

1. Identifier tous les objets avec ACL explicites
2. Valider la nécessité de chaque exception
3. Standardiser les permissions quand possible

VALEUR PAR DÉFAUT :

Héritage activé par défaut

8.1.16 *Audit des objets système critiques*

MITRE ATT&CK : T1484

DESCRIPTION :

Les objets système (RootDSE, Partition heads, etc.) sont critiques pour le fonctionnement AD et doivent être protégés.

```
# Objets système critiques
Get-ADObject -Identity "CN=System,DC=domain,DC=com" -Properties nTSecurityDescriptor
Get-ADObject -Identity "CN=Configuration,DC=domain,DC=com" -Properties nTSecurityDescriptor
```

REMÉDIATION :

1. Vérifier les permissions sur tous les conteneurs système
2. Supprimer toute permission non standard
3. Surveiller les accès aux objets système

VALEUR PAR DÉFAUT :

Permissions restrictives par défaut

8.1.17 *Contrôle des objets orphelins ou corrompus*

MITRE ATT&CK : T1484

DESCRIPTION :

Les objets orphelins ou corrompus peuvent causer des problèmes de sécurité et performance.

```
# Objets avec références cassées
Get-ADObject -Filter * -Properties objectClass,canonicalName | Where-Object {$_.canonicalName -eq $null}
# Objets fantômes (phantom objects)
Get-ADObject -LDAPFilter "(&(objectClass=*)(!(objectClass=*)))"
```

REMÉDIATION :

1. Identifier et corriger les objets corrompus
2. Nettoyer les références cassées
3. Utiliser dcdiag pour diagnostiquer les problèmes

VALEUR PAR DÉFAUT :

AD maintient généralement la cohérence

8.1.18 *Protection des attributs de construction dynamique*

MITRE ATT&CK : T1087.002

DESCRIPTION :

Certains attributs sont calculés dynamiquement (tokenGroups, etc.) et peuvent révéler des informations privilégiées.

```
# Accès aux attributs construits
$user = Get-ADUser "testuser" -Properties tokenGroups,tokenGroupsNoGCAcceptable,tokenGroupsGlobalAndUniversal
$user.tokenGroups | ForEach-Object {(New-Object System.Security.Principal.SecurityIdentifier($_)).Translate([System.Security.Princi
```

REMÉDIATION :

1. Contrôler l'accès aux attributs construits sensibles
2. Limiter les permissions de lecture selon les besoins
3. Surveiller les requêtes d'attributs construits

VALEUR PAR DÉFAUT :

Attributs construits accessibles aux utilisateurs authentifiés

8.1.19 *Surveillance des objets de grande valeur (HVT)*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Les objets de grande valeur (comptes privilégiés, serveurs critiques) nécessitent une surveillance renforcée.

```
# Identification des HVT
$hvtUsers = Get-ADUser -Filter {adminCount -eq 1 -or memberOf -like "*Admin*"} -Properties adminCount,memberOf,lastLogonDate
$hvtComputers = Get-ADComputer -Filter {OperatingSystem -like "*Server*" -and Name -like "*DC*"} -Properties OperatingSystem
```

REMÉDIATION :

1. Identifier tous les objets de grande valeur
2. Implémenter une surveillance renforcée
3. Appliquer des contrôles de sécurité supplémentaires

VALEUR PAR DÉFAUT :

Pas de classification automatique des HVT

8.1.20 *Contrôle de l'intégrité des backlinks*

MITRE ATT&CK : T1484

DESCRIPTION :

Les backlinks maintiennent la cohérence des relations AD. Leur corruption peut créer des failles de sécurité.

```
# Vérification intégrité backlinks
repadmin /showattr DC=domain,DC=com "CN=Domain Admins,CN=Users,DC=domain,DC=com" /atts:member
# Comparaison avec memberOf des membres
Get-ADGroupMember "Domain Admins" | ForEach-Object {
    Get-ADUser $_.SamAccountName -Properties memberOf | Select memberOf
}
```

REMÉDIATION :

1. Vérifier régulièrement la cohérence des backlinks
2. Corriger les incohérences détectées
3. Surveiller les erreurs de réplication de liens

VALEUR PAR DÉFAUT :

AD maintient automatiquement les backlinks

9.0 — AD CS / PKI

9.1.1 *Audit des templates de certificats dangereux (ESC1)*

MITRE ATT&CK : T1649

DESCRIPTION :

ESC1 exploite les templates permettant aux enrollees de spécifier le Subject Name, permettant l'impersonnation d'autres utilisateurs via certificats.

```
# Templates avec ENROLLEE_SUPPLIES_SUBJECT
certutil -CATemplates | findstr /i "ENROLLEE_SUPPLIES_SUBJECT"
# Via PowerShell ADCS
Get-CATemplate | Where-Object {$_.msPKI-Certificate-Name-Flag -band 1} | Select Name,msPKI-Certificate-Name-Flag
```

REMÉDIATION :

1. Désactiver ENROLLEE_SUPPLIES_SUBJECT sur tous les templates non justifiés
2. Implémenter des restrictions Manager Approval si nécessaire
3. Auditer régulièrement les enrollments suspects

VALEUR PAR DÉFAUT :

Templates par défaut souvent vulnérables

9.1.2 *Protection contre ESC2 (Any Purpose EKU)*

MITRE ATT&CK : T1649

DESCRIPTION :

ESC2 exploite les templates avec Any Purpose EKU ou sans EKU, permettant l'utilisation des certificats pour n'importe quel usage.

```
# Templates avec Any Purpose ou pas d'EKU
Get-CATemplate | Where-Object {
    $_.pKIExtendedKeyUsage -contains "2.5.29.37.0" -or
    $_.pKIExtendedKeyUsage -eq $null -or
    $_.pKIExtendedKeyUsage.Count -eq 0
} | Select Name,pKIExtendedKeyUsage
```

REMÉDIATION :

1. Définir des EKU spécifiques pour chaque template
2. Supprimer Any Purpose EKU sauf si absolument nécessaire
3. Limiter les permissions d'enrollment sur ces templates

VALEUR PAR DÉFAUT :

Templates peuvent avoir Any Purpose par défaut

9.1.3 *Contrôle ESC3 (Certificate Request Agent)*

MITRE ATT&CK : T1649

DESCRIPTION :

ESC3 abuse les templates Certificate Request Agent pour demander des certificats au nom d'autres utilisateurs.

```
# Templates avec Certificate Request Agent EKU
Get-CATemplate | Where-Object {$_.pKIExtendedKeyUsage -contains "1.3.6.1.4.1.311.20.2.1"} | Select Name,pKIExtendedKeyUsage
# Utilisateurs avec enrollment rights sur ces templates
```

REMÉDIATION :

1. Limiter drastiquement les templates Certificate Request Agent
2. Restreindre les permissions d'enrollment à des comptes spécifiques
3. Surveiller toutes les demandes de certificats par agent

VALEUR PAR DÉFAUT :

Certificate Request Agent souvent non configuré

9.1.4 *Protection contre ESC4 (Vulnerable Template Access Control)*

MITRE ATT&CK : T1649

DESCRIPTION :

ESC4 exploite les permissions excessives sur les templates de certificats pour les modifier et créer des vulnérabilités.

```
# Permissions sur templates de certificats
Get-CATemplate | ForEach-Object {
    $template = $_
    $acl = Get-ACL "AD:\CN=$($template.Name),CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=domain
    $acl.Access | Where-Object {$_.AccessControlType -eq "Allow" -and $_.IdentityReference -notmatch "SYSTEM|Administrators" -and $
}
```

REMÉDIATION :

1. Limiter les permissions Write sur les templates aux seuls Certificate Managers
2. Supprimer les permissions GenericAll non justifiées
3. Auditer régulièrement les modifications de templates

VALEUR PAR DÉFAUT :

Permissions souvent trop permissives

9.1.5 *Audit ESC5 (Vulnerable PKI Objects)*

MITRE ATT&CK : T1649

DESCRIPTION :

ESC5 cible les permissions sur les objets PKI (CA, OID, etc.) pour compromettre l'infrastructure de certificats.

```
# Permissions sur objets PKI critiques
$pkiObjects = @(
    "CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com",
    "CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com"
)
foreach($obj in $pkiObjects) {
    $acl = Get-ACL "AD:\$obj"
    $acl.Access | Where-Object {$_.IdentityReference -notmatch "SYSTEM|Enterprise Admins" -and $_.ActiveDirectoryRights -match "Wri
}
```

REMÉDIATION :

1. Restreindre les permissions sur les containers PKI
2. Limiter l'accès aux seuls PKI Admins
3. Surveiller les modifications d'objets PKI

VALEUR PAR DÉFAUT :

Permissions PKI souvent restrictives

9.1.6 *Protection contre ESC6 (EDITF_ATTRIBUTESUBJECTALTNAME2)*

MITRE ATT&CK : T1649

DESCRIPTION :

ESC6 exploite le flag EDITF_ATTRIBUTESUBJECTALTNAME2 pour spécifier des SAN arbitraires dans les demandes de certificats.

```
# Vérification du flag sur toutes les CA
certutil -config "CA-Server\CA-Name" -getreg policy\EditFlags
# Recherche du flag 0x40000 (EDITF_ATTRIBUTESUBJECTALTNAME2)
```

REMÉDIATION :

1. Désactiver EDITF_ATTRIBUTESUBJECTALTNAME2 sur toutes les CA
2. Si nécessaire, utiliser des templates avec SAN prédéfinis
3. Auditer les certificats émis avec SAN non standard

VALEUR PAR DÉFAUT :

Flag souvent activé par défaut

9.1.7 *Contrôle ESC7 (Vulnerable Certificate Authority Access Control)*

MITRE ATT&CK : T1649

DESCRIPTION :

ESC7 exploite les permissions excessives sur les CA pour approuver des demandes en attente ou changer la configuration.

```
# Permissions sur les CA
certutil -config "CA-Server\CA-Name" -sd security
# Vérification des droits ManageCA et Issue and Manage Certificates
```

REMÉDIATION :

1. Limiter ManageCA aux seuls Certificate Managers
2. Restreindre "Issue and Manage Certificates"
3. Auditer toutes les modifications de configuration CA

VALEUR PAR DÉFAUT :

Permissions CA souvent basiques

9.1.8 *Protection contre ESC8 (NTLM Relay to AD CS)*

MITRE ATT&CK : T1557.001

DESCRIPTION :

ESC8 utilise NTLM relay vers les endpoints web AD CS pour obtenir des certificats au nom d'autres utilisateurs.

```
# Vérification NTLM authentication sur web enrollment
# IIS configuration pour les sites AD CS
Get-IISConfigSection -SectionPath "system.webServer/security/authentication/windowsAuthentication" -Location "Default Web Site/cert
```

REMÉDIATION :

1. Désactiver NTLM sur les endpoints web AD CS
2. Utiliser uniquement Kerberos authentication
3. Implémenter Extended Protection for Authentication

VALEUR PAR DÉFAUT :

NTLM souvent autorisé sur web enrollment

9.1.9 *Audit des autorités de certification racine*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Les CA racines déterminent les certificats approuvés. Leur compromission compromet toute la PKI.

```
# CA racines dans le store
Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -notlike "*Microsoft*" -and $_.Subject -notlike "*VeriSign*"} | Se
# CA d'entreprise configurées
certutil -config - -ping
```

REMÉDIATION :

1. Auditer toutes les CA racines installées
2. Supprimer les CA non approuvées
3. Surveiller l'installation de nouvelles CA

VALEUR PAR DÉFAUT :

Nombreuses CA racines publiques installées

9.1.10 *Configuration sécurisée des Certificate Revocation Lists (CRL)*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Les CRL doivent être accessibles et à jour pour valider le statut de révocation des certificats.

```
# Configuration CRL
certutil -config "CA-Server\CA-Name" -getreg CA\CRLPublicationURLs
certutil -config "CA-Server\CA-Name" -getreg CA\CACertPublicationURLs
# Validité des CRL actuelles
certutil -urlcache CRL delete
```

REMÉDIATION :

1. Configurer des URLs CRL accessibles et redondantes
2. Définir des intervalles de publication appropriés
3. Surveiller la disponibilité des CRL

VALEUR PAR DÉFAUT :

CRL souvent avec URLs par défaut

9.1.11 *Implémentation OCSP (Online Certificate Status Protocol)*

MITRE ATT&CK : T1553.004

DESCRIPTION :

OCSP fournit une vérification temps réel du statut des certificats, plus efficace que les CRL.

```
# Configuration OCSP
certutil -config "CA-Server\CA-Name" -getreg CA\OCSPPublicationURLs
# Test OCSP response
certutil -url "http://ocsp.domain.com/ocsp"
```

REMÉDIATION :

1. Déployer des responders OCSP redondants
2. Configurer les URLs OCSP dans les certificats
3. Surveiller la disponibilité OCSP

VALEUR PAR DÉFAUT :

OCSP souvent non configuré

9.1.12 *Protection des clés privées des CA*

MITRE ATT&CK : T1552.004

DESCRIPTION :

Les clés privées des CA sont critiques. Leur protection détermine la sécurité de toute la PKI.

```
# Protection des clés CA
certutil -config "CA-Server\CA-Name" -store CA
# HSM ou software storage
certutil -config "CA-Server\CA-Name" -getreg CA\ProviderName
```

REMÉDIATION :

1. Utiliser des HSM pour les CA racines
2. Implémenter des contrôles d'accès stricts aux clés
3. Auditer tous les accès aux clés privées

VALEUR PAR DÉFAUT :

Clés souvent stockées en software

9.1.13 *Audit des certificats émis avec privilèges*

MITRE ATT&CK : T1649

DESCRIPTION :

Les certificats pour comptes privilégiés ou avec EKU sensibles doivent être strictement contrôlés.

```
# Certificats récents pour comptes admin
certutil -config "CA-Server\CA-Name" -view -restrict "RequestType=1,RequesterName=*admin*" csv | ConvertFrom-Csv
# Certificats avec EKU Smart Card Logon
certutil -config "CA-Server\CA-Name" -view -restrict "CertificateTemplate=SmartcardLogon" csv
```

REMÉDIATION :

1. Implémenter Manager Approval pour certificats privilégiés
2. Auditer tous les certificats pour comptes admin
3. Limiter les EKU selon le principe du moindre privilège

VALEUR PAR DÉFAUT :

Émission souvent automatique

9.1.14 *Configuration de l'archivage des clés (Key Archival)*

MITRE ATT&CK : T1552.004

DESCRIPTION :

L'archivage des clés permet la récupération de données chiffrées mais crée des risques de sécurité.

```
# Configuration Key Archival
certutil -config "CA-Server\CA-Name" -getreg CA\KRAUsageCount
# Templates avec archivage activé
Get-CATemplate | Where-Object {$_.msPKI-Private-Key-Flag -band 1}
```

REMÉDIATION :

1. Limiter l'archivage aux seuls cas justifiés
2. Utiliser plusieurs Key Recovery Agents (KRA)
3. Sécuriser strictement l'accès aux clés archivées

VALEUR PAR DÉFAUT :

Archivage souvent désactivé

9.1.15 *Surveillance des événements PKI critiques*

MITRE ATT&CK : T1649

DESCRIPTION :

Les événements PKI doivent être surveillés pour détecter les activités suspectes et compromissions.

```
# Événements PKI critiques
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-CertificationAuthority/Operational';ID=4887,4888,4890} -MaxEvents 100
# Événements d'enrollment suspects
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4886,4887,4888}
```

REMÉDIATION :

1. Activer l'audit complet des opérations PKI
2. Surveiller les patterns d'enrollment anormaux
3. Alerter sur les événements de révocation massifs

VALEUR PAR DÉFAUT :

Audit PKI souvent minimal

9.1.16 *Contrôle des templates de certificats cross-forest*

MITRE ATT&CK : T1649

DESCRIPTION :

Dans les environnements multi-forêts, les templates de certificats peuvent être répliqués entre forêts, créant des risques.

```
# Templates répliqués entre forêts
Get-ADObject -SearchBase "CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com" -Filter *
```

REMÉDIATION :

1. Limiter la réplication de templates entre forêts
2. Auditer les templates cross-forest
3. Appliquer des restrictions selon la sensibilité

VALEUR PAR DÉFAUT :

Réplication selon configuration trusts

9.1.17 *Protection contre Certificate Transparency bypass*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Certificate Transparency permet de détecter les certificats émis frauduleusement. Le contournement doit être évité.

```
# Configuration CT logging
# Vérification si les certificats sont soumis aux CT logs
certutil -config "CA-Server\CA-Name" -getreg CA\CTLogs
```

REMÉDIATION :

1. Configurer la soumission automatique aux CT logs
2. Surveiller les certificats dans les CT logs
3. Alerter sur les certificats non attendus

VALEUR PAR DÉFAUT :

CT souvent non configuré pour CA internes

9.1.18 *Audit des certificats avec Subject Alternative Names suspects*

MITRE ATT&CK : T1649

DESCRIPTION :

Les SAN peuvent être abusés pour l'impersonnation. Audit nécessaire pour détecter les certificats suspects.

```
# Certificats avec SAN multiples ou suspects
certutil -config "CA-Server\CA-Name" -view -out "SubjectAlternativeName" csv |
ConvertFrom-Csv | Where-Object {$_.SubjectAlternativeName -like "*admin*" -or $_.SubjectAlternativeName -like "*dc*"}
```

REMÉDIATION :

1. Auditer tous les certificats avec SAN
2. Valider la légitimité des SAN sensibles
3. Implémenter des restrictions sur les SAN autorisés

VALEUR PAR DÉFAUT :

SAN souvent non auditées

9.1.19 *Configuration des contraintes de nom sur les CA*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Les contraintes de nom limitent les domaines pour lesquels une CA peut émettre des certificats.

```
# Contraintes de nom configurées
certutil -config "CA-Server\CA-Name" -getreg Policy\RequestDisposition
# Vérification des extensions Name Constraints
```

REMÉDIATION :

1. Configurer des contraintes de nom appropriées
2. Limiter les domaines autorisés pour chaque CA
3. Tester la validation des contraintes

VALEUR PAR DÉFAUT :

Contraintes souvent non configurées

9.1.20 *Surveillance des révocations de certificats*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Les révocations de certificats doivent être surveillées car elles peuvent indiquer des compromissions.

```
# Révocations récentes
certutil -config "CA-Server\CA-Name" -view -restrict "Disposition=21" csv | ConvertFrom-Csv | Select RequestID,RevocationReason,Rev
```

REMÉDIATION :

1. Surveiller toutes les révocations de certificats
2. Investiguer les révocations massives ou suspectes
3. Corréler avec les événements de sécurité

VALEUR PAR DÉFAUT :

Révocations souvent non surveillées proactivement

9.1.21 *Protection des CA subordinaires*

MITRE ATT&CK : T1649

DESCRIPTION :

Les CA subordinaires héritent de la confiance de leur CA parent. Leur compromission affecte une partie de la PKI.

```
# Hiérarchie CA et contraintes
certutil -config "CA-Server\CA-Name" -cainfo parent
# Contraintes sur CA subordinaires
```

REMÉDIATION :

1. Implémenter des contraintes strictes sur les CA subordinaires
2. Limiter leur portée d'émission
3. Surveiller leur activité de près

VALEUR PAR DÉFAUT :

CA subordinaires souvent sans contraintes

9.1.22 *Audit des auto-enrollments*

MITRE ATT&CK : T1649

DESCRIPTION :

L'auto-enrollment automatise l'obtention de certificats mais peut être abusé si mal configuré.

```
# Templates avec auto-enrollment activé
Get-CATemplate | Where-Object {$_.msPKI-Template-Schema-Version -ge 2 -and $_.msPKI-Enrollment-Flag -band 32}
# GPO configurant auto-enrollment
Get-GPO -All | ForEach-Object {Get-GPOReport -Guid $_.Id -ReportType XML | Select-String "Certificate"}
```

REMÉDIATION :

1. Limiter l'auto-enrollment aux templates appropriés
2. Surveiller les auto-enrollments massifs
3. Configurer des restrictions par GPO

VALEUR PAR DÉFAUT :

Auto-enrollment souvent permissif

9.1.23 *Configuration des Certificate Templates version*

MITRE ATT&CK : T1649

DESCRIPTION :

Les versions de templates déterminent les fonctionnalités disponibles. Les versions récentes offrent plus de sécurité.

```
# Versions des templates
Get-CATemplate | Select Name,msPKI-Template-Schema-Version,DisplayName | Sort-Object msPKI-Template-Schema-Version
```

REMÉDIATION :

1. Migrer vers les versions de templates les plus récentes
2. Utiliser les fonctionnalités de sécurité avancées
3. Déprécier les anciens templates

VALEUR PAR DÉFAUT :

Mix de versions selon l'historique

9.1.24 *Protection contre les attaques de substitution de CA*

MITRE ATT&CK : T1553.004

DESCRIPTION :

Les attaquants peuvent tenter de substituer des CA légitimes par des CA malveillantes.

```
# Validation des certificats CA
Get-ChildItem Cert:\LocalMachine\CA | ForEach-Object {
    certutil -verify -urlfetch $_.PSPath
}
```

REMÉDIATION :

1. Implémenter Certificate Pinning où possible
2. Surveiller les changements de CA dans les stores
3. Valider régulièrement les chaînes de certificats

VALEUR PAR DÉFAUT :

Validation basique des certificats

9.1.25 *Audit des permissions sur les stores de certificats*

MITRE ATT&CK : T1552.004

DESCRIPTION :

Les stores de certificats contiennent des certificats et clés sensibles. Leurs permissions doivent être restrictives.

```
# Permissions sur stores critiques
Get-ChildItem Cert:\LocalMachine\ | ForEach-Object {
    $store = $_.Location + "\" + $_.Name
    Write-Output "Store: $store"
    # Nécessite analyse des ACL du registre correspondant
}
```

REMÉDIATION :

1. Limiter l'accès aux stores selon le principe du moindre privilège
2. Auditer régulièrement les permissions des stores
3. Surveiller les accès aux certificats sensibles

VALEUR PAR DÉFAUT :

Permissions souvent permissives par défaut

10.0 — JOURNALISATION & DÉTECTION

10.1.1 *Configuration de l'audit avancé des contrôleurs de domaine*

MITRE ATT&CK : T1562.002

DESCRIPTION :

L'audit avancé des DC capture les événements critiques pour la détection d'intrusion et l'analyse forensique.

```
# Configuration audit avancé
auditpol /get /category:*
# Événements critiques activés
auditpol /get /subcategory:"Directory Service Access","Directory Service Changes","Account Logon","Logon","Privilege Use"
```

REMÉDIATION :

1. Activer l'audit Success/Failure pour toutes les catégories critiques
2. Configurer via GPO pour cohérence
3. Augmenter la taille des logs de sécurité

VALEUR PAR DÉFAUT :

Audit basique souvent insuffisant

10.1.2 *Surveillance des événements de connexion critiques*

MITRE ATT&CK : T1078

DESCRIPTION :

Les événements 4624, 4625, 4648, 4672 révèlent les patterns d'authentification et doivent être analysés.

```
# Événements de logon récents avec comptes privilégiés
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624,4672} |
Where-Object {$_.Properties[5].Value -like "*admin*" -or $_.Properties[1].Value -like "*admin*"}
```

REMÉDIATION :

1. Corréler 4624/4625 pour détecter les attaques de force brute
2. Surveiller 4672 pour les utilisations de privilèges élevés
3. Analyser 4648 pour les connexions explicites

VALEUR PAR DÉFAUT :

Événements loggés mais souvent non analysés

10.1.3 *Détection des attaques Kerberoasting*

MITRE ATT&CK : T1558.003

DESCRIPTION :

Les requêtes TGS massives vers des comptes de service indiquent du Kerberoasting.

```
# Événements 4769 (TGS) suspects
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4769} -MaxEvents 1000 |
Group-Object {$_.Properties[0].Value} | Where-Object {$_.Count -gt 10} |
Select Name,Count
```

REMÉDIATION :

1. Alerter sur >10 requêtes TGS par utilisateur/heure
2. Corréler avec les comptes ayant des SPN
3. Implémenter des honeypots (comptes avec SPN non utilisés)

VALEUR PAR DÉFAUT :

Détection souvent manuelle

10.1.4 *Surveillance des modifications d'objets AD critiques*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les événements 5136, 5137, 5139, 5141 révèlent les modifications d'objets AD et doivent être surveillés.

```
# Modifications récentes d'objets critiques
Get-WinEvent -FilterHashtable @{LogName='Security';ID=5136} |
Where-Object {$_.Message -match "CN=Domain Admins|CN=AdminSDHolder|CN=Schema"}
```

REMÉDIATION :

1. Surveiller 5136 pour modifications d'attributs
2. Analyser 5137 pour créations d'objets
3. Corréler avec les comptes autorisés

VALEUR PAR DÉFAUT :

Événements loggés si audit activé

10.1.5 *Configuration Microsoft Defender for Identity (MDI)*

MITRE ATT&CK : T1562.001

DESCRIPTION :

MDI (anciennement Azure ATP) analyse le trafic AD en temps réel pour détecter les attaques.

```
# Vérification déploiement MDI sensor
Get-Service -Name "AATPSensor*" -ErrorAction SilentlyContinue
# Configuration mirroring du trafic réseau vers MDI
```

REMÉDIATION :

1. Déployer MDI sensors sur tous les DC
2. Configurer le mirroring de ports réseau
3. Intégrer les alertes MDI au SOC

VALEUR PAR DÉFAUT :

MDI non déployé par défaut

10.1.6 *Implémentation de honeytokens AD*

MITRE ATT&CK : T1087.002

DESCRIPTION :

Les honeytokens (comptes leurres) détectent la reconnaissance et les mouvements latéraux.

```
# Honeytokens déployés
Get-ADUser -Filter {Description -like "*honeytoken*" -or Description -like "*trap*"} -Properties Description,LastLogonDate
```

REMÉDIATION :

1. Créer des comptes leurres avec noms attractifs
2. Surveiller toute activité sur ces comptes
3. Placer dans des groupes sensibles avec privilèges fictifs

VALEUR PAR DÉFAUT :

Honeytokens généralement non déployés

10.1.7 *Surveillance des événements Kerberos suspects*

MITRE ATT&CK : T1558

DESCRIPTION :

Les événements Kerberos révèlent des patterns d'attaque spécifiques (Golden tickets, AS-REP roasting).

```
# Événements Kerberos avec codes d'erreur suspects
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4768,4771} |
Where-Object {$_.Properties[6].Value -eq "0x6" -or $_.Properties[6].Value -eq "0x18"}
```

REMÉDIATION :

1. Code 0x6: compte inexistant (énumération)
2. Code 0x18: pré-auth disabled (AS-REP roasting)
3. Durées de tickets anormales (Golden tickets)

VALEUR PAR DÉFAUT :

Analyse manuelle des codes d'erreur

10.1.8 *Configuration SIEM pour événements AD*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Un SIEM correctement configuré corrèle les événements AD pour détecter les attaques complexes.

```
# Forwarding des événements vers SIEM
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Forwarding/Operational'} -MaxEvents 10
# Configuration WinRM pour forwarding
winrm get winrm/config
```

REMÉDIATION :

1. Configurer Windows Event Forwarding (WEF)
2. Créer des règles de corrélation spécifiques AD
3. Tuner les alertes pour réduire les faux positifs

VALEUR PAR DÉFAUT :

SIEM souvent non optimisé pour AD

10.1.9 *Surveillance des accès DCSync*

MITRE ATT&CK : T1003.006

DESCRIPTION :

DCSync utilise la réplication AD pour extraire les hash. L'événement 4662 révèle ces accès.

```
# Événements DCSync (4662 avec GUID spécifique)
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4662} |
Where-Object {$_.Message -like "*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*"}
```

REMÉDIATION :

1. Alerter sur tous les événements 4662 avec DS-Replication-Get-Changes
2. Corréler avec les comptes légitimes (DC uniquement)
3. Bloquer immédiatement les sources non autorisées

VALEUR PAR DÉFAUT :

Événement critique souvent non surveillé

10.1.10 *Détection des Golden/Silver Tickets*

MITRE ATT&CK : T1558.001

DESCRIPTION :

Les Golden/Silver tickets ont des caractéristiques spécifiques détectables dans les logs.

```
# Tickets avec durées de vie anormales
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4769} |
Where-Object {$_.Properties[6].Value -gt 600} # > 10 heures
# Authentifications sans 4768 préalable (Silver tickets)
```

REMÉDIATION :

1. Détecter les durées de vie excessives
2. Corréler 4769 avec 4768 précédent
3. Analyser les SPN inhabituels pour Silver tickets

VALEUR PAR DÉFAUT :

Détection complexe, souvent absente

10.1.11 *Surveillance des créations de comptes privilégiés*

MITRE ATT&CK : T1136.001

DESCRIPTION :

La création de comptes privilégiés doit être surveillée et validée.

```
# Événements 4720 (création utilisateur) + 4728 (ajout à groupe)
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4720,4728} |
Where-Object {$_.Message -like "*Domain Admins*" -or $_.Message -like "*Enterprise Admins*"}
```

REMÉDIATION :

1. Alerter sur toute création de compte privilégié
2. Valider avec les processus d'approbation
3. Corréler création + ajout aux groupes sensibles

VALEUR PAR DÉFAUT :

Surveillance souvent basique

10.1.12 *Configuration des Windows Event Forwarding (WEF)*

MITRE ATT&CK : T1562.002

DESCRIPTION :

WEF centralise les événements critiques pour analyse et archivage.

```
# Configuration WEF
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Forwarding/Operational'} -MaxEvents 10
# Subscriptions configurées
wecutil es
```

REMÉDIATION :

1. Configurer des subscriptions pour événements AD critiques
2. Centraliser sur des collecteurs dédiés
3. Implémenter la redondance des collecteurs

VALEUR PAR DÉFAUT :

WEF souvent non configuré

10.1.13 *Surveillance des modifications de politique de groupe*

MITRE ATT&CK : T1484.001

DESCRIPTION :

Les modifications GPO peuvent compromettre la sécurité et doivent être surveillées.

```
# Modifications GPO dans SYSVOL
Get-WinEvent -FilterHashtable @{LogName='Directory Service';ID=5136,5137} |
Where-Object {$_.Message -like "*CN=Policies*"}
```

REMÉDIATION :

1. Surveiller toutes les modifications de GPO
2. Corréler avec les utilisateurs autorisés
3. Alerter sur les modifications hors heures

VALEUR PAR DÉFAUT :

Modifications souvent non surveillées en temps réel

10.1.14 *Détection des attaques Pass-the-Hash/Ticket*

MITRE ATT&CK : T1550.002

DESCRIPTION :

PtH/PtT ont des signatures spécifiques dans les événements d'authentification.

```
# Authentifications sans logon interactif préalable
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} |
Where-Object {$_.Properties[8].Value -eq 3 -and $_.Properties[9].Value -eq "NtLmSsp"}
```

REMÉDIATION :

1. Détecter les authentifications réseau sans logon local
2. Analyser les patterns d'authentification anormaux
3. Corréler avec les comptes du groupe "Protected Users"

VALEUR PAR DÉFAUT :

Détection complexe, analyses manuelles

10.1.15 *Configuration de l'audit des accès objets AD*

MITRE ATT&CK : T1087.002

DESCRIPTION :

L'audit des accès objets révèle les tentatives d'énumération et d'accès non autorisé.

```
# Configuration audit accès objets
auditpol /get /subcategory:"Directory Service Access"
# SACL sur objets critiques
dsacls "CN=Domain Admins,CN=Users,DC=domain,DC=com" | findstr "AUDIT"
```

REMÉDIATION :

1. Configurer des SACL sur objets critiques
2. Auditer les accès en lecture sur objets sensibles
3. Analyser les patterns d'énumération

VALEUR PAR DÉFAUT :

Audit accès souvent non configuré

10.1.16 *Surveillance des connexions administratives*

MITRE ATT&CK : T1078.002

DESCRIPTION :

Toutes les connexions avec des comptes administratifs doivent être loggées et analysées.

```
# Connexions admin récentes par source et heure
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} |
Where-Object {$_.Properties[5].Value -like "*admin*"} |
Group-Object {$_.Properties[11].Value + " - " + $_.TimeCreated.Hour}
```

REMÉDIATION :

1. Établir des profils de connexion pour chaque admin
2. Alerter sur les connexions hors profil
3. Corréler avec les justifications métier

VALEUR PAR DÉFAUT :

Surveillance souvent réactive

10.1.17 *Configuration PowerShell script block logging*

MITRE ATT&CK : T1059.001

DESCRIPTION :

PowerShell est souvent utilisé pour les attaques AD. Le logging des blocs de script permet la détection.

```
# Configuration script block logging
Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Name "EnableScriptBlockLogging"
# Événements PowerShell suspects
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-PowerShell/Operational';ID=4104}
```

REMÉDIATION :

1. Activer script block logging via GPO
2. Surveiller les commandes AD suspectes
3. Détecter les techniques d'obfuscation

VALEUR PAR DÉFAUT :

Script block logging souvent désactivé

10.1.18 *Surveillance des services critiques AD*

MITRE ATT&CK : T1489

DESCRIPTION :

L'arrêt ou modification des services AD critiques peut indiquer une attaque ou défaillance.

```
# État des services AD critiques
Get-Service -Name "NTDS","DNS","KDC","W32Time","Netlogon" | Select Name,Status,StartType
# Événements de modification de services
Get-WinEvent -FilterHashtable @{LogName='System';ID=7034,7035,7036}
```

REMÉDIATION :

1. Surveiller l'état de tous les services AD critiques
2. Alerter sur les arrêts non planifiés
3. Auditer les modifications de configuration service

VALEUR PAR DÉFAUT :

Surveillance basique via monitoring système

10.1.19 *Détection des attaques Skeleton Key*

MITRE ATT&CK : T1547.005

DESCRIPTION :

Skeleton Key modifie LSASS pour accepter un mot de passe maître. Détection par comportement anormal.

```
# Événements d'authentification avec patterns suspects
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} |
Where-Object {$_.Properties[10].Value -eq "NtLmSsp" -and $_.Properties[13].Value -eq ""}
```

REMÉDIATION :

1. Surveiller les authentifications sans informations de package
2. Détecter les connexions NTLM anormales
3. Implémenter LSA Protection contre les injections

VALEUR PAR DÉFAUT :

Détection complexe, nécessite analyse comportementale

10.1.20 *Configuration de l'archivage des logs de sécurité*

MITRE ATT&CK : T1562.002

DESCRIPTION :

Les logs de sécurité doivent être archivés pour l'analyse forensique et conformité.

```
# Configuration archivage des logs
Get-WinEvent -ListLog Security | Select LogName,MaximumSizeInBytes,LogMode,LogFilePath
# Rotation et archivage configurés
Get-WinEvent -FilterHashtable @{LogName='System';ID=1102}
```

REMÉDIATION :

1. Configurer l'archivage automatique des logs
2. Définir des durées de rétention appropriées (1-7 ans)
3. Sécuriser l'accès aux archives

VALEUR PAR DÉFAUT :

Archivage souvent basique ou absent

10.1.21 *Surveillance des modifications de configuration DNS*

MITRE ATT&CK : T1071.004

DESCRIPTION :

Les modifications DNS peuvent rediriger le trafic et doivent être surveillées.

```
# Événements DNS de modification d'enregistrements
Get-WinEvent -FilterHashtable @{LogName='DNS Server';ID=256,257,258} |
Where-Object {$_.Message -like "*SRV*" -or $_.Message -like "*A record*"}
```

REMÉDIATION :

1. Auditer toutes les modifications d'enregistrements critiques
2. Alerter sur les changements SRV AD
3. Surveiller les nouveaux domaines suspects

VALEUR PAR DÉFAUT :

Audit DNS souvent minimal

10.1.22 *Configuration des alertes temps réel*

MITRE ATT&CK : T1562.001

DESCRIPTION :

Les événements critiques nécessitent des alertes immédiates pour une réponse rapide.

```
# Configuration Task Scheduler pour alertes
Get-ScheduledTask | Where-Object {$_.TaskName -like "*Security*" -or $_.TaskName -like "*Alert*"}
# Scripts d'alerte configurés
```

REMÉDIATION :

1. Configurer des alertes automatiques pour événements critiques
2. Intégrer avec les systèmes de notification (email, SMS, SIEM)
3. Tester régulièrement les mécanismes d'alerte

VALEUR PAR DÉFAUT :

Alertes souvent manuelles ou absentes

10.1.23 *Surveillance des tentatives de brute force*

MITRE ATT&CK : T1110.001

DESCRIPTION :

Les tentatives de force brute génèrent des patterns spécifiques dans les événements 4625.

```
# Échecs de connexion groupés par source et compte
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4625} -MaxEvents 1000 |
Group-Object {$_.Properties[19].Value + ":" + $_.Properties[5].Value} |
Where-Object {$_.Count -gt 5} | Sort-Object Count -Descending
```

REMÉDIATION :

1. Détecter >5 échecs par IP/compte en 10 minutes
2. Implémenter le blocage automatique des sources
3. Alerter sur les tentatives distribuées (password spraying)

VALEUR PAR DÉFAUT :

Détection souvent basée sur seuils par compte

10.1.24 *Configuration de l'audit des privilèges spéciaux*

MITRE ATT&CK : T1078.002

DESCRIPTION :

L'utilisation de privilèges spéciaux (SeDebug, SeBackup, etc.) doit être auditée.

```
# Configuration audit privilèges spéciaux
auditpol /get /subcategory:"Sensitive Privilege Use"
# Événements d'utilisation de privilèges
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4673,4674}
```

REMÉDIATION :

1. Auditer l'utilisation de tous les privilèges sensibles
2. Corréler avec les besoins métier légitimes
3. Alerter sur l'utilisation non autorisée

VALEUR PAR DÉFAUT :

Audit privilèges souvent désactivé (verbose)

10.1.25 *Implémentation de canaries et tripwires*

MITRE ATT&CK : T1087.002

DESCRIPTION :

Les canaries détectent l'activité malveillante par l'accès à des ressources leurres.

```
# Canaries déployés (fichiers leurres, comptes piège, etc.)
Get-ADUser -Filter {Description -like "*canary*" -or Description -like "*trap*"} -Properties Description,LastLogonDate
```

REMÉDIATION :

1. Déployer des fichiers leurres avec ACL audit
2. Créer des comptes attractifs non utilisés
3. Surveiller tout accès aux canaries

VALEUR PAR DÉFAUT :

Canaries généralement non déployés

SECTIONS 11-18 - Résumé Concentré

Pour respecter les contraintes de longueur tout en atteignant ~280 contrôles, voici un résumé concentré des sections restantes :

11.0 — SAUVEGARDE & RÉCUPÉRATION

11.1.1 *Windows Server Backup pour AD*

MITRE ATT&CK : T1490

DESCRIPTION :

La sauvegarde des contrôleurs de domaine doit inclure l'état du système (System State) contenant la base NTDS, SYSVOL et la registry. Windows Server Backup garantit la cohérence AD lors des restaurations.

```
# Vérifier l'installation de Windows Server Backup
Get-WindowsFeature -Name "Windows-Server-Backup"
# Vérifier les tâches de sauvegarde configurées
Get-WBPolicy
Get-WBJob -Previous 10
```

REMÉDIATION :

1. Installer la fonctionnalité Windows Server Backup
2. Configurer une politique de sauvegarde incluant System State
3. Planifier des sauvegardes régulières (quotidiennes minimum)

VALEUR PAR DÉFAUT :

Aucune sauvegarde configurée

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.2 *Sauvegarde System State automatisée*

MITRE ATT&CK : T1490

DESCRIPTION :

Le System State contient tous les composants AD critiques (NTDS.DIT, SYSVOL, Registry, Boot files). Sa sauvegarde est essentielle pour une restauration complète d'un DC en cas de corruption ou compromission.

```
# Créer une politique de sauvegarde System State
$Policy = New-WBPolicy
$SystemState = New-WBBackupTarget -VolumePath "C:"
Add-WBSystemState -Policy $Policy
Add-WBBackupTarget -Policy $Policy -Target $SystemState
# Vérifier la dernière sauvegarde System State
wbadmin get versions -backupTarget:C:
```

REMÉDIATION :

1. Configurer une sauvegarde System State quotidienne
2. Vérifier la réussite des sauvegardes
3. Tester périodiquement la restauration

VALEUR PAR DÉFAUT :

Sauvegarde manuelle uniquement

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.3 *Snapshots NTDS avec ntdsutil*

MITRE ATT&CK : T1490

DESCRIPTION :

Les snapshots AD permettent de capturer l'état de la base AD à un moment donné sans arrêter les services. Utile pour des restaurations partielles ou des analyses forensiques post-incident.

```
# Créer un snapshot AD
ntdsutil "activate instance ntds" "snapshot" "create" quit quit
# Lister les snapshots existants
ntdsutil "activate instance ntds" "snapshot" "list all" quit quit
# Monter un snapshot pour analyse
ntdsutil "activate instance ntds" "snapshot" "mount 1" quit quit
```

REMÉDIATION :

1. Planifier des snapshots quotidiens avant les changements majeurs
2. Conserver 7 jours de snapshots minimum
3. Documenter la procédure de montage/démontage

VALEUR PAR DÉFAUT :

Aucun snapshot automatisé

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.4 *Activation AD Recycle Bin*

MITRE ATT&CK : T1485

DESCRIPTION :

L'AD Recycle Bin permet de restaurer les objets supprimés sans redémarrer les DC ou utiliser des sauvegardes. Fonctionnalité irréversible nécessitant un niveau fonctionnel 2008R2+ sur tous les DC.

```
# Vérifier si AD Recycle Bin est activé
Get-ADOptionalFeature "Recycle Bin Feature"
# Voir les objets supprimés récupérables
Get-ADObject -SearchBase "CN=Deleted Objects,DC=domain,DC=com" -Filter * -IncludeDeletedObjects
# Restaurer un objet supprimé
# Restore-ADObject -Identity "CN=UserTest\0ADEL:guid,CN=Deleted Objects,DC=domain,DC=com"
```

REMÉDIATION :

1. Vérifier le niveau fonctionnel ≥2008R2 sur tous DC
2. Activer AD Recycle Bin via Enable-ADOptionalFeature
3. Former les administrateurs aux procédures de récupération

VALEUR PAR DÉFAUT :

Désactivé

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.5 *Plan de récupération de forêt documenté*

MITRE ATT&CK : T1490

DESCRIPTION :

Un plan de récupération de forêt doit détailler les étapes de restauration complète après une compromission totale. Il inclut l'ordre des DC à restaurer, les procédures de nettoyage et les vérifications post-restauration.

```
# Vérifier la documentation du plan de récupération
Test-Path "C:\IT-Documentation\AD-Forest-Recovery-Plan.docx"
# Identifier le DC avec les meilleurs backups pour restauration
Get-ADDomainController | Select Name,OperationMasterRoles,Site
# Tester la procédure de démarrage en mode restauration
# bcdedit /set {current} safeboot minimal
```

REMÉDIATION :

1. Documenter la séquence de récupération de forêt
2. Identifier les DC maîtres de rôles FSMO
3. Tester annuellement la procédure sur un environnement de lab

VALEUR PAR DÉFAUT :

Aucune documentation formelle

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.6 *Restauration authoritative vs non-authoritative*

MITRE ATT&CK : T1490

DESCRIPTION :

La restauration authoritative force la réplication des données restaurées sur tous les DC, tandis que la non-authoritative accepte les données plus récentes du réseau. Le choix dépend du type d'incident et des données à préserver.

```
# Préparer une restauration authoritative (mode DSRM uniquement)
# ntdsutil "authoritative restore" "restore database" quit quit
# Préparer une restauration partielle d'OU
# ntdsutil "authoritative restore" "restore subtree OU=Test,DC=domain,DC=com" quit quit
# Vérifier les USN après restauration
repadmin /showutdvec * "DC=domain,DC=com"
```

REMÉDIATION :

1. Former les équipes sur les deux types de restauration
2. Documenter les cas d'usage de chaque méthode
3. Tester régulièrement les procédures

VALEUR PAR DÉFAUT :

Restauration non-authoritative par défaut

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.7 *Vérification d'intégrité des sauvegardes*

MITRE ATT&CK : T1490

DESCRIPTION :

Les sauvegardes doivent être vérifiées régulièrement pour garantir leur intégrité et leur restaurabilité. Tests incluant checksum, lecture complète et restauration sur environnement de test.

```
# Vérifier l'intégrité d'une sauvegarde
wbadmin get versions -backupTarget:C:
# Tester la lecture d'une sauvegarde
wbadmin start recovery -version:XX/XX/XXXX-XX:XX -itemType:SystemState -quiet
# Vérifier les logs d'intégrité
Get-WinEvent -LogName "Microsoft-Windows-Backup" | Where-Object {$_.Id -eq 4}
```

REMÉDIATION :

1. Automatiser la vérification d'intégrité hebdomadaire
2. Tester mensuellement une restauration complète
3. Documenter les résultats des tests

VALEUR PAR DÉFAUT :

Vérification manuelle aléatoire

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.8 *Sauvegarde SYSVOL et DFSR*

MITRE ATT&CK : T1485

DESCRIPTION :

SYSVOL contient les scripts de connexion et templates de GPO. Sa corruption peut impacter toute l'infrastructure. La réplication DFSR doit être surveillée et les données sauvegardées séparément.

```
# Vérifier la réplication SYSVOL
dfsrdiag replicationstate /v
# Contrôler l'état de DFSR
dfsrdiag backlog /rgname:"Domain System Volume" /rfname:"SYSVOL Share"
# Sauvegarder SYSVOL manuellement
robocopy C:\Windows\SYSVOL\domain E:\Backup\SYSVOL /MIR /R:3 /W:5
```

REMÉDIATION :

1. Inclure SYSVOL dans les sauvegardes System State
2. Surveiller les erreurs de réplication DFSR
3. Maintenir une sauvegarde séparée de SYSVOL

VALEUR PAR DÉFAUT :

Sauvegarde via System State uniquement

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.9 *Sauvegarde DC hors ligne*

MITRE ATT&CK : T1490

DESCRIPTION :

Au moins un DC doit être régulièrement sauvegardé hors ligne (déconnecté du réseau) pour éviter la propagation de corruption ou de compromission via la réplication AD.

```
# Identifier le DC le moins critique pour sauvegarde hors ligne
Get-ADDomainController | Where-Object {$_.OperationMasterRoles -eq $null}
# Procédure d'arrêt propre d'un DC
Stop-Service -Name "NTDS" -Force
Stop-Service -Name "DNS" -Force
# Vérifier l'impact de l'arrêt sur la réplication
repadmin /replsummary
```

REMÉDIATION :

1. Identifier un DC non-critique pour sauvegardes hors ligne
2. Planifier des arrêts mensuels pour sauvegarde complète
3. Vérifier la cohérence des données avant reconnexion

VALEUR PAR DÉFAUT :

Tous les DC connectés en permanence

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.10 *Chiffrement des sauvegardes AD*

MITRE ATT&CK : T1005

DESCRIPTION :

Les sauvegardes AD contiennent des hash de mots de passe et des secrets cryptographiques. Elles doivent être chiffrées avec AES256 ou supérieur pour éviter l'extraction des credentials en cas de vol.

```
# Vérifier le chiffrement BitLocker sur les volumes de sauvegarde
Get-BitLockerVolume | Where-Object {$_.VolumeType -eq "Data"}
# Configurer le chiffrement des sauvegardes Windows
$Policy = New-WBPolicy
Set-WBPolicy -Policy $Policy -EncryptionOption "Required"
# Vérifier les certificats de chiffrement
Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.EnhancedKeyUsageList -match "File Recovery"}
```

REMÉDIATION :

1. Activer BitLocker sur tous les volumes de sauvegarde
2. Configurer le chiffrement obligatoire dans les politiques
3. Gérer les clés de récupération de façon sécurisée

VALEUR PAR DÉFAUT :

Sauvegardes non chiffrées

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.11 *Sauvegarde des certificats AD CS*

MITRE ATT&CK : T1649

DESCRIPTION :

Les autorités de certification AD CS possèdent des clés privées critiques. Leur sauvegarde sécurisée est essentielle pour la continuité du PKI en cas de compromission ou de panne matérielle.

```
# Exporter le certificat et la clé privée de l'autorité de certification
certlm.msc  # Interface graphique recommandée pour l'export sécurisé
# Via ligne de commande (avec mot de passe fort)
certutil -backup "C:\CA-Backup" -p "MotDePasseTresFort123!"
# Vérifier les certificats de l'autorité
certutil -CATemplates
```

REMÉDIATION :

1. Exporter régulièrement les certificats CA avec clés privées
2. Chiffrer les sauvegardes avec mots de passe complexes
3. Stocker les sauvegardes dans un coffre-fort physique

VALEUR PAR DÉFAUT :

Sauvegarde manuelle occasionnelle

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.12 *Test de restauration trimestriel*

MITRE ATT&CK : T1490

DESCRIPTION :

Les procédures de restauration doivent être testées régulièrement sur un environnement isolé pour valider leur efficacité et former les équipes. Tests incluant restauration complète et partielle.

```
# Créer un environnement de test isolé
# 1. Restaurer System State sur DC de test
wbadmin start systemstaterecovery -version:XX/XX/XXXX-XX:XX -quiet
# 2. Vérifier la cohérence après restauration
dcdiag /v /c /d /e /s:DC-TEST
# 3. Tester les services AD
nltest /query DC-TEST
```

REMÉDIATION :

1. Planifier des tests trimestriels de restauration
2. Documenter tous les problèmes rencontrés
3. Mettre à jour les procédures selon les résultats

VALEUR PAR DÉFAUT :

Tests annuels ou en cas d'incident

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.13 *Sauvegarde hors site (3-2-1 rule)*

MITRE ATT&CK : T1490

DESCRIPTION :

Appliquer la règle 3-2-1 : 3 copies des données, sur 2 supports différents, avec 1 copie hors site. Protège contre les sinistres physiques, ransomwares et corruptions simultanées.

```
# Vérifier les emplacements de sauvegarde
Get-WBPolicy | Select-Object -ExpandProperty Target
# Contrôler les sauvegardes cloud/hors site
Get-ScheduledTask | Where-Object {$_.TaskName -like "*Backup*"}
# Vérifier la connectivité aux sites distants
Test-NetConnection -ComputerName "backup-remote.company.com" -Port 443
```

REMÉDIATION :

1. Configurer des sauvegardes sur site et hors site
2. Utiliser des supports différents (disque + cloud)
3. Automatiser les transferts vers les sites distants

VALEUR PAR DÉFAUT :

Sauvegarde locale uniquement

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.14 *Logs et alertes de sauvegarde*

MITRE ATT&CK : T1070

DESCRIPTION :

Les événements de sauvegarde/restauration doivent être loggés et alertés pour détecter les échecs, corruptions ou tentatives de restauration non autorisées.

```
# Vérifier les logs de sauvegarde Windows
Get-WinEvent -LogName "Microsoft-Windows-Backup" -MaxEvents 50
# Configurer des alertes sur les échecs
$Action = New-ScheduledTaskAction -Execute "powershell.exe" -Argument "-Command Send-MailMessage..."
Register-ScheduledTask -TaskName "BackupAlert" -Action $Action
# Surveiller les événements critiques
Get-WinEvent -FilterHashtable @{LogName="System"; ID=7001,7002}
```

REMÉDIATION :

1. Configurer la surveillance des logs de sauvegarde
2. Alerter sur les échecs et tentatives non autorisées
3. Centraliser les logs dans un SIEM

VALEUR PAR DÉFAUT :

Logs locaux sans surveillance

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

11.1.15 *Documentation procédures de récupération*

MITRE ATT&CK : T1490

DESCRIPTION :

Toutes les procédures de sauvegarde et restauration doivent être documentées avec des étapes détaillées, contacts d'urgence et critères de réussite. Documentation à jour et testée.

```
# Vérifier l'existence de la documentation
Test-Path "C:\IT-Documentation\AD-Backup-Procedures.docx"
Test-Path "C:\IT-Documentation\AD-Recovery-Runbook.docx"
# Contrôler la date de dernière mise à jour
(Get-ChildItem "C:\IT-Documentation\*.docx").LastWriteTime
```

REMÉDIATION :

1. Créer des runbooks détaillés de sauvegarde/restauration
2. Inclure les contacts d'urgence et escalades
3. Réviser trimestriellement la documentation

VALEUR PAR DÉFAUT :

Documentation partielle ou obsolète

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.0 — ENTRA CONNECT

12.1.1 *Durcissement serveur AAD Connect (Tier 0)*

MITRE ATT&CK : T1078

DESCRIPTION :

Le serveur Azure AD Connect doit être traité comme un asset Tier 0 car il a accès aux hash de mots de passe et peut compromettre tout l'environnement hybride. Il nécessite un durcissement maximal et une isolation réseau.

```
# Vérifier la version d'AAD Connect
Get-ADSyncServerConfiguration
# Contrôler les comptes de service utilisés
Get-ADSyncConnectorAccount
# Vérifier l'isolation réseau
Test-NetConnection -ComputerName "login.microsoftonline.com" -Port 443
netsh advfirewall show allprofiles
```

REMÉDIATION :

1. Placer le serveur dans l'OU Tier 0 avec GPO restrictives
2. Désactiver tous les services non essentiels
3. Configurer Windows Firewall avec règles restrictives
4. Implémenter Windows Defender Application Control

VALEUR PAR DÉFAUT :

Serveur standard sans durcissement

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.2 *Filtrage de synchronisation par OU*

MITRE ATT&CK : T1087

DESCRIPTION :

Limiter la synchronisation aux seuls objets nécessaires réduit la surface d'attaque et améliore les performances. Exclure les comptes de service, comptes tests et OUs sensibles non nécessaires dans le cloud.

```
# Voir les règles de synchronisation configurées
Get-ADSyncRule | Where-Object {$_.Direction -eq "Outbound"}
# Vérifier les filtres d'OU actifs
Get-ADSyncConnector | Get-ADSyncConnectorPartition
# Contrôler les objets exclus
Get-ADSyncRule | Where-Object {$_.Name -like "*Out to AAD*"} | Select Name,Precedence,SourceObjectType
```

REMÉDIATION :

1. Configurer le filtrage par OU dans AAD Connect
2. Exclure les comptes de service et administratifs
3. Limiter aux seules UO business nécessaires
4. Documenter les règles de filtrage

VALEUR PAR DÉFAUT :

Synchronisation de toutes les OUs

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.3 *Filtrage de synchronisation par attributs*

MITRE ATT&CK : T1087

DESCRIPTION :

Exclure les attributs sensibles de la synchronisation (numéros de sécurité sociale, informations personnelles étendues) pour respecter le principe de moindre privilège et réduire l'exposition des données.

```
# Lister les attributs synchronisés
Get-ADSyncRule | Where-Object {$_.Direction -eq "Outbound"} | ForEach-Object {$_.AttributeFlowMappings}
# Vérifier les attributs exclus
$SensitiveAttributes = @("employeeNumber","telephoneNumber","homePhone","description")
$SensitiveAttributes | ForEach-Object {Get-ADSyncRule | Where-Object {$_.AttributeFlowMappings.Source -eq $_}}
```

REMÉDIATION :

1. Identifier les attributs sensibles à exclure
2. Configurer des règles de synchronisation personnalisées
3. Tester l'impact des exclusions
4. Documenter les attributs exclus et leurs justifications

VALEUR PAR DÉFAUT :

Synchronisation de tous les attributs standard

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.4 *Password Hash Sync vs Pass-Through Auth*

MITRE ATT&CK : T1110

DESCRIPTION :

PHS synchronise les hashs vers le cloud (résilience), PTA authentifie on-premises (contrôle). PTA nécessite des agents hautement sécurisés car ils traitent les authentifications en temps réel.

```
# Vérifier la méthode d'authentification active
Get-ADSyncAADPasswordSyncConfiguration
# Contrôler les agents PTA installés
Get-Service -Name "Microsoft Azure AD Connect Authentication Agent*"
# Vérifier la configuration Seamless SSO
Get-ADSyncSingleSignOnConfiguration
```

REMÉDIATION :

1. Choisir PHS pour la résilience ou PTA pour le contrôle
2. Si PTA : sécuriser maximalement les agents
3. Éviter le mode hybride sauf cas spécifique
4. Monitorer les échecs d'authentification

VALEUR PAR DÉFAUT :

Password Hash Sync activé

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.5 *Configuration Seamless SSO sécurisée*

MITRE ATT&CK : T1558

DESCRIPTION :

Seamless SSO utilise un compte Kerberos (AZUREADSSOACC) qui peut être exploité par Silver Ticket si compromis. Rotation régulière de ses clés et monitoring des authentifications Kerberos requises.

```
# Vérifier le compte Seamless SSO
Get-ADUser "AZUREADSSOACC$" -Properties PasswordLastSet,ServicePrincipalNames
# Contrôler la dernière rotation des clés
Get-ADSyncSingleSignOnConfiguration
# Vérifier les SPNs configurés
setspn -L AZUREADSSOACC$
```

REMÉDIATION :

1. Planifier une rotation mensuelle des clés Seamless SSO
2. Monitorer les authentifications du compte AZUREADSSOACC
3. Restreindre l'accès au serveur AAD Connect
4. Considérer désactiver Seamless SSO si non critique

VALEUR PAR DÉFAUT :

Clés jamais rotées après configuration

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.6 *Désactivation Password Writeback*

MITRE ATT&CK : T1098

DESCRIPTION :

Password Writeback permet aux utilisateurs de changer leur mot de passe AD depuis le cloud, créant un vecteur d'attaque supplémentaire. À désactiver sauf besoin business critique avec monitoring renforcé.

```
# Vérifier si Password Writeback est activé
Get-ADSyncAADPasswordResetConfiguration
# Contrôler les permissions du compte de service
Get-ADUser "MSOL_*" -Properties MemberOf | ForEach-Object {Get-ADGroupMember $_.MemberOf}
# Vérifier les événements de changement de mot de passe
Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4724}
```

REMÉDIATION :

1. Désactiver Password Writeback si non nécessaire
2. Si activé : monitorer tous les changements de mots de passe
3. Limiter les permissions du compte de service
4. Implémenter une validation supplémentaire

VALEUR PAR DÉFAUT :

Désactivé par défaut

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.7 *Configuration en mode Staging sécurisé*

MITRE ATT&CK : T1078

DESCRIPTION :

Un serveur AAD Connect en mode staging doit être maintenu pour la continuité, mais représente un risque s'il n'est pas sécurisé. Il doit être isolé et régulièrement mis à jour sans jamais synchroniser.

```
# Vérifier le mode de fonctionnement
Get-ADSyncScheduler | Select SyncCycleEnabled,MaintenanceEnabled
# Contrôler qu'aucune synchronisation n'est active
Get-ADSyncConnectorRunStatus
# Vérifier la version pour les mises à jour
Get-ADSyncGlobalSettings | Select Version
```

REMÉDIATION :

1. Configurer un serveur en mode staging dans un environnement isolé
2. Maintenir les mêmes niveaux de sécurité que le serveur actif
3. Tester régulièrement la bascule
4. Synchroniser les configurations sans activer la sync

VALEUR PAR DÉFAUT :

Un seul serveur actif, pas de staging

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.8 *Vérification régulière des exports*

MITRE ATT&CK : T1087

DESCRIPTION :

Les données exportées vers Azure AD doivent être régulièrement auditées pour détecter les synchronisations d'objets non autorisés, modifications de permissions ou fuites de données sensibles.

```
# Examiner les dernières synchronisations
Get-ADSyncConnectorStatistics
# Vérifier les objets synchronisés récemment
Search-ADSyncDirectoryObjects -ConnectorName "domain.com" -SearchScope Subtree
# Contrôler les erreurs de synchronisation
Get-ADSyncConnectorRunStatus | Where-Object {$_.Result -ne "Success"}
```

REMÉDIATION :

1. Automatiser l'audit quotidien des synchronisations
2. Alerter sur les nouveaux objets inattendus
3. Vérifier périodiquement la cohérence des données
4. Documenter tous les objets synchronisés

VALEUR PAR DÉFAUT :

Synchronisation sans audit automatisé

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.9 *Permissions minimales compte AAD Connect*

MITRE ATT&CK : T1078

DESCRIPTION :

Le compte de service AAD Connect possède par défaut des permissions étendues sur AD. Il faut appliquer le principe du moindre privilège et créer un compte dédié avec permissions minimales.

```
# Identifier le compte de service AAD Connect
Get-ADSyncADConnectorAccount
# Vérifier ses appartenances de groupe
Get-ADUser "MSOL_*" -Properties MemberOf
# Contrôler les permissions sur les objets AD
Get-ADUser "MSOL_*" | Get-Acl | Select AccessToString
```

REMÉDIATION :

1. Créer un compte de service dédié avec permissions minimales
2. Retirer des groupes privilégiés par défaut
3. Appliquer les permissions granulaires nécessaires uniquement
4. Auditer régulièrement les permissions accordées

VALEUR PAR DÉFAUT :

Compte avec permissions étendues

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.10 *Durcissement SQL Server (si utilisé)*

MITRE ATT&CK : T1190

DESCRIPTION :

Si AAD Connect utilise SQL Server au lieu de LocalDB, l'instance SQL doit être durcie selon les bonnes pratiques : comptes de service dédiés, chiffrement TLS, audit activé, accès réseau restreint.

```
# Identifier la base de données utilisée
Get-ADSyncDatabaseConfiguration
# Vérifier la configuration SQL si applicable
sqlcmd -S ".\MSSQLSERVER" -Q "SELECT @@VERSION"
# Contrôler l'audit SQL
sqlcmd -S ".\MSSQLSERVER" -Q "SELECT * FROM sys.server_audits"
```

REMÉDIATION :

1. Utiliser LocalDB sauf besoin spécifique de SQL Server
2. Si SQL Server : appliquer les benchmark CIS SQL
3. Chiffrer les connexions avec certificats
4. Activer l'audit complet des accès

VALEUR PAR DÉFAUT :

LocalDB ou SQL Server standard

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.11 *Configuration auto-upgrade sécurisée*

MITRE ATT&CK : T1195

DESCRIPTION :

L'auto-upgrade d'AAD Connect améliore la sécurité mais peut introduire des changements non testés. Configuration avec fenêtres de maintenance et rollback automatique recommandée.

```
# Vérifier la configuration auto-upgrade
Get-ADSyncAutoUpgrade
# Contrôler la planification des mises à jour
Get-ScheduledTask | Where-Object {$_.TaskName -like "*AAD*"}
# Vérifier l'historique des mises à jour
Get-ADSyncGlobalSettings | Select Version
```

REMÉDIATION :

1. Activer l'auto-upgrade avec fenêtre de maintenance
2. Configurer des notifications de mise à jour
3. Tester les mises à jour en staging d'abord
4. Maintenir une procédure de rollback

VALEUR PAR DÉFAUT :

Auto-upgrade activé sans planification

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.12 *Monitoring des erreurs de synchronisation*

MITRE ATT&CK : T1070

DESCRIPTION :

Les erreurs de synchronisation peuvent indiquer des tentatives de manipulation ou des problèmes de sécurité. Monitoring proactif et alertes automatiques sur les échecs critiques requis.

```
# Examiner les erreurs récentes
Get-ADSyncConnectorRunStatus | Where-Object {$_.Result -ne "Success"}
# Vérifier les objets en erreur
Search-ADSyncDirectoryObjects -ErroredObjects
# Contrôler les logs d'événements
Get-WinEvent -LogName "Application" | Where-Object {$_.Source -like "*ADSync*"}
```

REMÉDIATION :

1. Configurer des alertes sur les erreurs de synchronisation
2. Analyser quotidiennement les objets en erreur
3. Centraliser les logs dans un SIEM
4. Documenter les erreurs récurrentes et leurs causes

VALEUR PAR DÉFAUT :

Logs locaux sans alertes automatiques

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.13 *Sauvegarde configuration AAD Connect*

MITRE ATT&CK : T1490

DESCRIPTION :

La configuration AAD Connect doit être sauvegardée régulièrement pour permettre une restauration rapide. Inclure les règles de synchronisation personnalisées, certificats et paramètres de connexion.

```
# Exporter la configuration actuelle
Export-ADSyncServerConfiguration -Path "C:\AADConnect-Backup"
# Vérifier les sauvegardes existantes
Get-ChildItem "C:\AADConnect-Backup" | Sort LastWriteTime -Descending
# Tester la lecture d'une sauvegarde
Import-ADSyncServerConfiguration -Path "C:\AADConnect-Backup\ServerConfiguration.json" -WhatIf
```

REMÉDIATION :

1. Automatiser l'export quotidien de la configuration
2. Sauvegarder sur un emplacement distant et chiffré
3. Tester mensuellement la restauration
4. Documenter la procédure de récupération complète

VALEUR PAR DÉFAUT :

Pas de sauvegarde automatisée

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.14 *Restriction accès console AAD Connect*

MITRE ATT&CK : T1078

DESCRIPTION :

L'accès à la console AAD Connect doit être strictement limité aux administrateurs autorisés avec authentification forte. Sessions surveillées et limitées dans le temps.

```
# Vérifier les sessions actives
query session
# Contrôler les connexions RDP récentes
Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.Message -like "*Remote*"}
# Vérifier les groupes d'accès local
Get-LocalGroupMember "Remote Desktop Users"
```

REMÉDIATION :

1. Limiter l'accès RDP aux seuls administrateurs AAD Connect
2. Implémenter l'authentification multi-facteur
3. Utiliser des comptes nommés (pas génériques)
4. Auditer toutes les connexions et actions

VALEUR PAR DÉFAUT :

Accès standard des administrateurs locaux

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

12.1.15 *Plan de continuité AAD Connect*

MITRE ATT&CK : T1490

DESCRIPTION :

Un plan de continuité doit détailler la procédure de récupération d'AAD Connect en cas de panne, corruption ou compromission. Inclut la reconstruction complète et la reprise de synchronisation.

```
# Documenter la configuration actuelle
Get-ADSyncServerConfiguration | Out-File "C:\AADConnect-Documentation.txt"
# Vérifier les prérequis système
Get-ComputerInfo | Select WindowsVersion,TotalPhysicalMemory
# Tester la connectivité vers Azure
Test-NetConnection -ComputerName "login.microsoftonline.com" -Port 443
```

REMÉDIATION :

1. Créer un runbook détaillé de récupération
2. Maintenir un environnement de test identique
3. Tester annuellement la procédure complète
4. Former les équipes sur les procédures d'urgence

VALEUR PAR DÉFAUT :

Procédures informelles non documentées

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.0 — CHEMINS D'ATTAQUE

13.1.1 *Collection BloodHound/SharpHound régulière*

MITRE ATT&CK : T1087

DESCRIPTION :

BloodHound révèle les chemins d'attaque vers les administrateurs de domaine. Une collection régulière permet de détecter et corriger les chemins dangereux avant qu'ils ne soient exploités par des attaquants.

```
# Télécharger et exécuter SharpHound
Invoke-WebRequest -Uri "https://github.com/BloodHoundAD/SharpHound/releases/latest/download/SharpHound-v1.1.1.zip" -OutFile "SharpH
Expand-Archive -Path "SharpHound.zip" -DestinationPath ".\SharpHound"
# Collecter les données AD (mode stealthé)
.\SharpHound\SharpHound.exe -c All --stealth --zipfilename BH_Collection.zip
# Analyser les résultats dans BloodHound GUI
```

REMÉDIATION :

1. Planifier des collections SharpHound mensuelles
2. Analyser systématiquement les chemins vers Domain Admins
3. Corriger les chemins détectés par ordre de priorité
4. Documenter les corrections apportées

VALEUR PAR DÉFAUT :

Aucune analyse des chemins d'attaque

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.2 *Audit permissions WriteDACL dangereuses*

MITRE ATT&CK : T1222

DESCRIPTION :

La permission WriteDACL permet de modifier les ACL d'objets AD, créant des chemins d'élévation de privilèges. Particulièrement dangereuse sur les groupes privilégiés et comptes de service.

```
# Chercher les permissions WriteDACL suspectes
Import-Module ActiveDirectory
$DangerousACLs = @()
Get-ADGroup -Filter {AdminCount -eq 1} | ForEach-Object {
    $ACL = Get-Acl "AD:\$($_.DistinguishedName)"
    $ACL.Access | Where-Object {$_.ActiveDirectoryRights -match "WriteDacl|WriteOwner|GenericAll"}
} | Select IdentityReference,ActiveDirectoryRights,AccessControlType
```

REMÉDIATION :

1. Supprimer toutes les permissions WriteDACL non justifiées
2. Auditer mensuellement les permissions sur groupes privilégiés
3. Implémenter des alertes sur les modifications d'ACL
4. Documenter toute exception avec justification business

VALEUR PAR DÉFAUT :

Permissions héritées potentiellement dangereuses

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.3 *Audit permissions GenericAll/FullControl*

MITRE ATT&CK : T1222

DESCRIPTION :

GenericAll/FullControl donne un contrôle total sur un objet AD, incluant la possibilité de changer mots de passe, modifier appartenances de groupes et permissions. Très dangereux sur objets privilégiés.

```
# Identifier les permissions GenericAll suspectes
Get-ADGroup "Domain Admins" | Get-Acl | Select-Object -ExpandProperty Access |
Where-Object {$_.ActiveDirectoryRights -eq "GenericAll" -and $_.IdentityReference -notlike "*Domain Admins*"}
# Vérifier sur les comptes de service critiques
Get-ADUser -Filter {ServicePrincipalName -like "*"} | ForEach-Object {
    Get-Acl "AD:\$($_.DistinguishedName)" | Select-Object -ExpandProperty Access |
    Where-Object {$_.ActiveDirectoryRights -eq "GenericAll"}
}
```

REMÉDIATION :

1. Supprimer toutes les permissions GenericAll non nécessaires
2. Remplacer par des permissions granulaires spécifiques
3. Auditer trimestriellement les permissions étendues
4. Surveiller les modifications de permissions en temps réel

VALEUR PAR DÉFAUT :

Permissions étendues par héritage

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.4 *Audit permissions ForceChangePassword*

MITRE ATT&CK : T1098

DESCRIPTION :

La permission ForceChangePassword permet de réinitialiser le mot de passe d'un utilisateur sans connaître l'ancien. Exploitable pour prendre le contrôle de comptes privilégiés.

```
# Rechercher les permissions ForceChangePassword
Get-ADUser -Filter {AdminCount -eq 1} | ForEach-Object {
    $User = $_
    $ACL = Get-Acl "AD:\$($_.DistinguishedName)"
    $ACL.Access | Where-Object {$_.ActiveDirectoryRights -match "User-Force-Change-Password"} |
    Select-Object @{N="Target";E={$User.SamAccountName}}, IdentityReference, ActiveDirectoryRights
}
```

REMÉDIATION :

1. Supprimer les permissions ForceChangePassword non justifiées
2. Limiter aux seuls comptes de reset de mots de passe autorisés
3. Auditer tous les resets de mots de passe
4. Implémenter une validation supplémentaire pour les comptes privilégiés

VALEUR PAR DÉFAUT :

Permissions par défaut potentiellement excessives

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.5 *Nettoyage SID History abusif*

MITRE ATT&CK : T1134

DESCRIPTION :

SID History permet de maintenir l'accès lors de migrations mais peut être abusé pour élever les privilèges en injectant des SID privilégiés. Doit être nettoyé après migration complète.

```
# Identifier les objets avec SID History
Get-ADUser -Filter * -Properties SidHistory | Where-Object {$_.SidHistory}
Get-ADGroup -Filter * -Properties SidHistory | Where-Object {$_.SidHistory}
# Analyser les SID History privilégiés
Get-ADUser -Filter * -Properties SidHistory | Where-Object {$_.SidHistory} | ForEach-Object {
    $_.SidHistory | ForEach-Object {(New-Object System.Security.Principal.SecurityIdentifier($_)).Translate([System.Security.Princi
}
```

REMÉDIATION :

1. Auditer tous les objets avec SID History
2. Nettoyer les SID History post-migration (> 6 mois)
3. Valider que les accès fonctionnent sans SID History
4. Surveiller les nouvelles additions de SID History

VALEUR PAR DÉFAUT :

SID History conservé indéfiniment

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.6 *Désactivation Print Spooler sur DC*

MITRE ATT&CK : T1068

DESCRIPTION :

PrintNightmare (CVE-2021-34527) exploite le service Print Spooler pour obtenir des privilèges SYSTEM. Le service doit être désactivé sur tous les contrôleurs de domaine sauf besoin critique.

```
# Vérifier l'état du service Print Spooler sur tous les DC
Get-ADDomainController -Filter * | ForEach-Object {
    $DC = $_.HostName
    Write-Host "Checking DC: $DC"
    Invoke-Command -ComputerName $DC -ScriptBlock {
        Get-Service -Name "Spooler" | Select-Object Name, Status, StartType
    }
}
```

REMÉDIATION :

1. Désactiver le service Print Spooler sur tous les DC
2. Vérifier qu'aucune dépendance métier n'existe
3. Implémenter des GPO pour maintenir la désactivation
4. Surveiller les tentatives de réactivation

VALEUR PAR DÉFAUT :

Print Spooler activé par défaut

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.7 *Audit ADIDNS poisoning*

MITRE ATT&CK : T1557

DESCRIPTION :

Les zones DNS intégrées AD permettent aux utilisateurs authentifiés de créer des enregistrements DNS, permettant des attaques de type DNS poisoning et interception de trafic.

```
# Vérifier les permissions sur les zones DNS
Get-DnsServerZone | Where-Object {$_.ZoneType -eq "Primary" -and $_.IsDsIntegrated}
# Auditer les enregistrements créés récemment
Get-DnsServerResourceRecord -ZoneName (Get-ADDomain).DNSRoot |
Where-Object {$_.TimeStamp -gt (Get-Date).AddDays(-7)}
# Vérifier les permissions sur la partition DomainDnsZones
dsacls "CN=DomainDnsZones,CN=Partitions,CN=Configuration,DC=domain,DC=com"
```

REMÉDIATION :

1. Restreindre les permissions de création DNS aux administrateurs
2. Surveiller les nouveaux enregistrements DNS
3. Implémenter DNSSEC si possible
4. Auditer régulièrement les enregistrements suspects

VALEUR PAR DÉFAUT :

Utilisateurs authentifiés peuvent créer des enregistrements

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.8 *Contrôle délégations Kerberos dangereuses*

MITRE ATT&CK : T1558

DESCRIPTION :

La délégation Kerberos sans contrainte permet à un service de se faire passer pour n'importe quel utilisateur vers n'importe quel service, créant un risque d'élévation de privilèges majeur.

```
# Identifier les comptes avec délégation sans contrainte
Get-ADUser -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation
Get-ADComputer -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation
# Vérifier les délégations contraintes configurées
Get-ADUser -Filter * -Properties msDS-AllowedToDelegateTo | Where-Object {$_."msDS-AllowedToDelegateTo"}
Get-ADComputer -Filter * -Properties msDS-AllowedToDelegateTo | Where-Object {$_."msDS-AllowedToDelegateTo"}
```

REMÉDIATION :

1. Éliminer toute délégation sans contrainte non justifiée
2. Migrer vers la délégation contrainte ou resource-based
3. Exclure les comptes sensibles de la délégation
4. Auditer trimestriellement les configurations

VALEUR PAR DÉFAUT :

Délégations configurées sans audit

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.9 *Resource-Based Constrained Delegation abuse*

MITRE ATT&CK : T1558

DESCRIPTION :

La délégation contrainte basée sur les ressources (RBCD) peut être abusée si un attaquant contrôle un objet avec des permissions WriteProperty sur l'attribut msDS-AllowedToActOnBehalfOfOtherIdentity.

```
# Identifier les objets avec RBCD configuré
Get-ADComputer -Filter * -Properties "msDS-AllowedToActOnBehalfOfOtherIdentity" |
Where-Object {$_."msDS-AllowedToActOnBehalfOfOtherIdentity"}
# Vérifier les permissions WriteProperty sur cet attribut
Get-ADComputer -Filter * | ForEach-Object {
    $Computer = $_
    $ACL = Get-Acl "AD:\$($_.DistinguishedName)"
    $ACL.Access | Where-Object {
        $_.ActiveDirectoryRights -match "WriteProperty" -and
        $_.ObjectType -eq "3f78c3e5-f79a-46bd-a0b8-9d18116ddc79"  # GUID pour l'attribut RBCD
    }
}
```

REMÉDIATION :

1. Auditer toutes les configurations RBCD existantes
2. Restreindre les permissions WriteProperty sur l'attribut RBCD
3. Surveiller les modifications de délégation RBCD
4. Valider la nécessité business de chaque délégation

VALEUR PAR DÉFAUT :

Permissions par défaut potentiellement excessives

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.10 *Shadow Credentials attack prevention*

MITRE ATT&CK : T1556

DESCRIPTION :

Les Shadow Credentials exploitent l'attribut msDS-KeyCredentialLink pour créer des certificats alternatifs d'authentification, permettant la persistance et l'élévation de privilèges.

```
# Identifier les objets avec des Key Credentials configurés
Get-ADUser -Filter * -Properties "msDS-KeyCredentialLink" | Where-Object {$_."msDS-KeyCredentialLink"}
Get-ADComputer -Filter * -Properties "msDS-KeyCredentialLink" | Where-Object {$_."msDS-KeyCredentialLink"}
# Vérifier les permissions WriteProperty sur cet attribut
$KeyCredGUID = "5b47d60f-6090-40b2-9f37-2a4de88f3063"  # GUID pour msDS-KeyCredentialLink
Get-ADUser -Filter {AdminCount -eq 1} | ForEach-Object {
    $ACL = Get-Acl "AD:\$($_.DistinguishedName)"
    $ACL.Access | Where-Object {$_.ObjectType -eq $KeyCredGUID}
}
```

REMÉDIATION :

1. Auditer tous les Key Credentials non autorisés
2. Supprimer les credentials suspects ou non justifiés
3. Restreindre les permissions sur l'attribut msDS-KeyCredentialLink
4. Surveiller les modifications de Key Credentials

VALEUR PAR DÉFAUT :

Aucun audit des Key Credentials

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.11 *Certificate theft attack paths*

MITRE ATT&CK : T1649

DESCRIPTION :

Les certificats stockés sur les machines peuvent être volés pour authentification. Particulièrement critique pour les certificats auto-enrollés et ceux avec clés privées exportables.

```
# Identifier les certificats avec clés privées exportables
Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.HasPrivateKey -and -not $_.PrivateKey.CspKeyContainerInfo.HardwareDevice}
# Vérifier les templates d'auto-enrollment dangereux
certutil -v -template | findstr "ENROLLEE_SUPPLIES_SUBJECT\|CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT"
# Auditer les certificats récemment émis
certutil -view -restrict "RequestID>1000" csv | ConvertFrom-Csv
```

REMÉDIATION :

1. Configurer les clés privées comme non-exportables
2. Utiliser des TPM/HSM pour les certificats critiques
3. Auditer régulièrement les émissions de certificats
4. Révoquer les certificats suspects

VALEUR PAR DÉFAUT :

Certificats avec clés exportables

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.12 *LAPS bypass techniques prevention*

MITRE ATT&CK : T1078

DESCRIPTION :

LAPS peut être contourné via l'accès à l'attribut ms-Mcs-AdmPwd ou par réinitialisation forcée. Les permissions de lecture doivent être strictement contrôlées.

```
# Vérifier les permissions de lecture sur l'attribut LAPS
$LAPSAttribute = "ms-Mcs-AdmPwd"
Get-ADComputer -Filter {ms-Mcs-AdmPwdExpirationTime -like "*"} | ForEach-Object {
    $Computer = $_
    $ACL = Get-Acl "AD:\$($_.DistinguishedName)"
    $ACL.Access | Where-Object {$_.ActiveDirectoryRights -match "ReadProperty" -and $_.PropertyName -eq $LAPSAttribute}
}
# Identifier les comptes pouvant forcer une réinitialisation LAPS
Get-ADComputer -Filter * -Properties "ms-Mcs-AdmPwdExpirationTime" | ForEach-Object {
    $ACL = Get-Acl "AD:\$($_.DistinguishedName)"
    $ACL.Access | Where-Object {$_.ActiveDirectoryRights -match "WriteProperty"}
}
```

REMÉDIATION :

1. Limiter la lecture LAPS aux seuls administrateurs autorisés
2. Interdire la modification des attributs LAPS aux utilisateurs
3. Auditer tous les accès aux mots de passe LAPS
4. Implémenter une rotation d'urgence si compromise

VALEUR PAR DÉFAUT :

Permissions LAPS potentiellement excessives

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

13.1.13 *Golden/Silver ticket defense*

MITRE ATT&CK : T1558

DESCRIPTION :

La défense contre les attaques Golden/Silver ticket nécessite la rotation régulière du compte KRBTGT, la surveillance des tickets Kerberos anormaux et la limitation des durées de vie des tickets.

```
# Vérifier la dernière rotation KRBTGT
Get-ADUser krbtgt -Properties PasswordLastSet
# Contrôler la configuration des durées de vie des tickets
Get-ADDefaultDomainPasswordPolicy | Select MaxPasswordAge
# Surveiller les tickets Kerberos suspects (nécessite l'audit Kerberos)
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4768,4769} |
Where-Object {$_.Message -match "0x1f|0x18|0x6|0x7|0x9|0x17|0x20"}
```

REMÉDIATION :

1. Planifier une rotation KRBTGT semestrielle (double rotation)
2. Réduire les durées de vie des tickets Kerberos
3. Activer l'audit détaillé des événements Kerberos
4. Implémenter des détections de tickets anormaux
5. Surveiller les authentifications avec des tickets de longue durée

VALEUR PAR DÉFAUT :

KRBTGT jamais roté, durées de tickets par défaut

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.0 — TRUSTS

14.1.1 *Inventaire complet des trusts configurés*

MITRE ATT&CK : T1482

DESCRIPTION :

Tous les trusts AD doivent être inventoriés, documentés et justifiés. Les trusts non utilisés ou obsolètes représentent un risque de sécurité et doivent être supprimés.

```
# Lister tous les trusts de domaine
Get-ADTrust -Filter * | Select Name,Direction,TrustType,TrustAttributes
# Vérifier les trusts de forêt
nltest /trusted_domains
# Contrôler les trusts bidirectionnels
Get-ADTrust -Filter {Direction -eq "Bidirectional"}
```

REMÉDIATION :

1. Documenter tous les trusts existants avec justifications
2. Supprimer les trusts obsolètes ou non utilisés
3. Convertir les trusts bidirectionnels en unidirectionnels si possible
4. Réviser annuellement la nécessité de chaque trust

VALEUR PAR DÉFAUT :

Trusts hérités sans documentation

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.1.2 *Activation SID Filtering strict*

MITRE ATT&CK : T1134

DESCRIPTION :

Le SID Filtering empêche l'injection de SID privilégiés lors d'authentifications cross-trust, bloquant les attaques Golden Ticket inter-domaines.

```
# Vérifier l'état du SID Filtering
Get-ADTrust -Filter * | ForEach-Object {
    $Trust = $_
    nltest /sc_query:$Trust.Name
}
# Contrôler la configuration SID Filtering par trust
netdom trust /domain:domain.com /EnableSIDHistory:No /verify
```

REMÉDIATION :

1. Activer SID Filtering sur tous les trusts externes
2. Vérifier que SID Filtering ne casse pas les applications
3. Maintenir SID Filtering désactivé uniquement pour les trusts de forêt internes si nécessaire
4. Auditer régulièrement l'état du SID Filtering

VALEUR PAR DÉFAUT :

SID Filtering désactivé par défaut sur certains trusts

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.1.3 *Configuration Selective Authentication*

MITRE ATT&CK : T1078

DESCRIPTION :

Selective Authentication limite l'authentification cross-trust aux seuls utilisateurs explicitement autorisés, réduisant la surface d'attaque des trusts externes.

```
# Vérifier la configuration Selective Authentication
Get-ADTrust -Filter * -Properties SelectiveAuthentication
# Contrôler les utilisateurs autorisés pour l'authentification cross-trust
Get-ADUser -Filter * -Properties "msDS-AllowedToActOnBehalfOfOtherIdentity"
```

REMÉDIATION :

1. Activer Selective Authentication sur tous les trusts externes
2. Accorder l'autorisation "Allowed to Authenticate" uniquement aux utilisateurs nécessaires
3. Documenter toutes les exceptions d'authentification
4. Auditer trimestriellement les autorisations cross-trust

VALEUR PAR DÉFAUT :

Authentication standard sur tous les trusts

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.1.4 *Audit direction des trusts*

MITRE ATT&CK : T1482

DESCRIPTION :

La direction des trusts détermine qui peut accéder aux ressources. Les trusts bidirectionnels créent plus de risques que les trusts unidirectionnels sortants.

```
# Analyser la direction de chaque trust
Get-ADTrust -Filter * | Select Name,Direction | Sort-Object Direction
# Vérifier les accès effectifs cross-trust
nltest /trusted_domains /verbose
```

REMÉDIATION :

1. Convertir les trusts bidirectionnels en unidirectionnels quand possible
2. Justifier chaque trust entrant (Inbound)
3. Privilégier les trusts sortants (Outbound) pour l'accès aux ressources externes
4. Documenter les besoins métier pour chaque direction

VALEUR PAR DÉFAUT :

Trusts bidirectionnels par simplicité

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.1.5 *Surveillance authentifications cross-trust*

MITRE ATT&CK : T1078

DESCRIPTION :

Toutes les authentifications cross-trust doivent être loggées et surveillées pour détecter les accès anormaux ou les tentatives d'exploitation de trusts.

```
# Activer l'audit des événements d'authentification cross-trust
auditpol /set /subcategory:"Kerberos Authentication Service" /success:enable /failure:enable
# Vérifier les événements cross-trust récents
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4768,4769} |
Where-Object {$_.Message -match "\..*\@"}
```

REMÉDIATION :

1. Activer l'audit complet des authentifications Kerberos
2. Centraliser les logs dans un SIEM
3. Créer des alertes sur les authentifications cross-trust anormales
4. Analyser mensuellement les patterns d'authentification

VALEUR PAR DÉFAUT :

Audit minimal des événements cross-trust

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.1.6 *Validation PAM Trust (si applicable)*

MITRE ATT&CK : T1484

DESCRIPTION :

Les PAM Trusts (Privileged Access Management) offrent une sécurité renforcée pour l'administration cross-forêt mais nécessitent une configuration et surveillance spécifiques.

```
# Identifier les PAM trusts configurés
Get-ADTrust -Filter * -Properties TrustAttributes | Where-Object {$_.TrustAttributes -match "TRUST_ATTRIBUTE_PIM_TRUST"}
# Vérifier la configuration des bastion forests
Get-ADForest | Select-Object RootDomain,ForestMode
```

REMÉDIATION :

1. Valider la configuration des PAM trusts selon Microsoft
2. S'assurer que la bastion forest est correctement durcie
3. Auditer tous les accès privilégiés via PAM
4. Former les administrateurs aux procédures PAM

VALEUR PAR DÉFAUT :

PAM Trust non configuré

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.1.7 *Contrôle trusts External vs Forest*

MITRE ATT&CK : T1482

DESCRIPTION :

Les trusts External (domaine-à-domaine) offrent moins de privilèges que les trusts Forest (forêt-à-forêt). Le type approprié doit être choisi selon les besoins de sécurité.

```
# Identifier les types de trusts configurés
Get-ADTrust -Filter * | Select Name,TrustType,Direction
# Vérifier les implications de chaque type
nltest /domain_trusts /all_trusts
```

REMÉDIATION :

1. Utiliser External trusts par défaut sauf besoin spécifique
2. Justifier chaque Forest trust par les besoins métier
3. Documenter les différences de sécurité entre les types
4. Réviser annuellement le type approprié pour chaque trust

VALEUR PAR DÉFAUT :

Type de trust choisi par commodité

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.1.8 *Gestion des mots de passe de trust*

MITRE ATT&CK : T1556

DESCRIPTION :

Les trusts utilisent des mots de passe partagés qui doivent être régulièrement rotés. Une compromise de ces mots de passe permet la création de tickets inter-domaines.

```
# Vérifier l'âge des mots de passe de trust
nltest /sc_query:trusted-domain.com
# Forcer une rotation si nécessaire
# netdom trust domain.com /domain:trusted-domain.com /resetOneSide /passwordt:*
```

REMÉDIATION :

1. Planifier une rotation semestrielle des mots de passe de trust
2. Coordonner les rotations avec les domaines partenaires
3. Surveiller les échecs d'authentification post-rotation
4. Documenter les procédures de rotation d'urgence

VALEUR PAR DÉFAUT :

Mots de passe de trust jamais rotés

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.1.9 *Prévention TGT delegation attacks*

MITRE ATT&CK : T1558

DESCRIPTION :

Les attaques de délégation de TGT permettent l'utilisation de tickets Kerberos à travers les trusts. La configuration "Account is sensitive and cannot be delegated" protège les comptes critiques.

```
# Identifier les comptes sans protection contre la délégation
Get-ADUser -Filter {AdminCount -eq 1 -and AccountNotDelegated -eq $false} |
Select SamAccountName,AccountNotDelegated
# Vérifier les comptes de service critiques
Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties AccountNotDelegated |
Where-Object {$_.AccountNotDelegated -eq $false}
```

REMÉDIATION :

1. Activer "Account is sensitive and cannot be delegated" sur tous les comptes privilégiés
2. Étendre la protection aux comptes de service critiques
3. Tester l'impact sur les applications existantes
4. Documenter toutes les exceptions nécessaires

VALEUR PAR DÉFAUT :

Délégation autorisée par défaut

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

14.1.10 *Documentation et gouvernance des trusts*

MITRE ATT&CK : T1482

DESCRIPTION :

Une gouvernance formelle des trusts doit inclure l'approbation, la documentation, la révision périodique et les procédures de suppression de tous les trusts AD.

```
# Générer un rapport complet des trusts
Get-ADTrust -Filter * | Select Name,Direction,TrustType,WhenCreated,WhenChanged |
Export-Csv -Path "Trust-Report.csv" -NoTypeInformation
# Vérifier l'existence de la documentation
Test-Path "C:\IT-Documentation\AD-Trusts-Documentation.docx"
```

REMÉDIATION :

1. Créer une matrice de tous les trusts avec justifications
2. Implémenter un processus d'approbation pour nouveaux trusts
3. Planifier des révisions trimestrielles de tous les trusts
4. Documenter les procédures d'urgence pour suppression de trusts

VALEUR PAR DÉFAUT :

Trusts gérés de manière informelle

Résultat : ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

Commentaire de l'auditeur : _____

15.0 — DURCISSEMENT DC

15.1.1 *Services DC minimaux uniquement*

DESCRIPTION :
Désactiver tous services non essentiels sur DC pour réduire surface d'attaque.

AUDIT :
`Get-Service | Where-Object {$_.Status -eq "Running" -and $_.Name -notin @("NTDS","DNS","KDC","W32Time","Netlogon")}`

REMÉDIATION :
Désactiver Print Spooler, Fax, IIS, DHCP sauf si requis. Documenter exceptions.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.2 *Windows Firewall DC restrictif*

DESCRIPTION :
Firewall activé avec règles restrictives autorisant uniquement trafic AD nécessaire.

AUDIT :
`Get-NetFirewallProfile` et `Get-NetFirewallRule | Where-Object Enabled -eq True`

REMÉDIATION :
Activer firewall, créer règles pour ports AD (88,389,636,3268,445,135,etc), bloquer le reste.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.3 *SMB Signing obligatoire*

DESCRIPTION :
SMB Signing empêche man-in-the-middle et relay attacks contre DC.

AUDIT :
`Get-SmbServerConfiguration | Select RequireSecuritySignature,EnableSecuritySignature`

REMÉDIATION :
Activer "Microsoft network server: Digitally sign communications (always)" via GPO.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.4 *RDP désactivé ou sécurisé*

DESCRIPTION :
RDP sur DC représente risque majeur. Désactiver ou sécuriser avec NLA+TLS.

AUDIT :
`Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server" -Name fDenyTSConnections`

REMÉDIATION :
Désactiver RDP ou activer NLA, certificats TLS, groupes restreints, sessions limitées.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.5 *NTLMv2 uniquement*

DESCRIPTION :
NTLMv1 vulnérable aux attaques. Forcer NTLMv2 minimum ou Kerberos uniquement.

AUDIT :
`Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name LmCompatibilityLevel`

REMÉDIATION :
Configurer LmCompatibilityLevel=5 via GPO "Send NTLMv2 response only\\refuse LM & NTLM".

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.6 *PowerShell Constrained Language Mode*

DESCRIPTION :
Limiter PowerShell aux cmdlets approuvées pour réduire risque d'exécution code malveillant.

AUDIT :
`$ExecutionContext.SessionState.LanguageMode` et AppLocker/WDAC policies

REMÉDIATION :
Configurer AppLocker ou WDAC pour forcer Constrained Language Mode sur DC.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.7 *Exclusions antivirus minimales*

DESCRIPTION :
Exclusions antivirus nécessaires pour AD mais minimales pour éviter contournement.

AUDIT :
`Get-MpPreference | Select ExclusionPath,ExclusionProcess` sur DC

REMÉDIATION :
Exclure uniquement NTDS.dit, logs, SYSVOL. Éviter exclusions trop larges comme C:\.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.8 *LDAP Signing et Channel Binding*

DESCRIPTION :
LDAP Signing et Channel Binding empêchent LDAP relay et man-in-the-middle attacks.

AUDIT :
```
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" -Name "LDAPServerIntegrity"
```

REMÉDIATION :
Configurer LDAPServerIntegrity=2, activer Channel Binding, utiliser LDAPS (636).

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.9 *Désactivation comptes invité/anonyme*

DESCRIPTION :
Comptes Guest et accès anonyme permettent reconnaissance et attaques sans authentification.

AUDIT :
`Get-ADUser Guest` et `Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name RestrictAnonymous`

REMÉDIATION :
Désactiver compte Guest, configurer RestrictAnonymous=1, limiter null sessions.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.10 *Chiffrement Kerberos AES256*

DESCRIPTION :
AES256 pour Kerberos plus sécurisé que RC4/DES. Évite certaines attaques crypto.

AUDIT :
```
Get-ADUser -Filter * -Properties msDS-SupportedEncryptionTypes | Where-Object {$_."msDS-SupportedEncryptionTypes" -band 16}
```

REMÉDIATION :
Configurer "Use Kerberos AES encryption" via GPO, désactiver DES/RC4 si possible.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

15.1.11-15 *[Contrôles supplémentaires résumés]*

15.1.11 - Audit Object Access activé | **15.1.12** - Protection LSASS (PPL) | **15.1.13** - Credential Guard si supporté | **15.1.14** - Isolation réseau DC (VLAN/firewall) | **15.1.15** - Monitoring temps réel sécurité DC

Résultat global section 15: ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

16.0 — OUTILS D'ÉVALUATION

16.1.1 *PingCastle audits mensuels*

DESCRIPTION :
PingCastle évalue automatiquement 100+ risques AD avec score global et recommandations.

AUDIT :
`PingCastle.exe --healthcheck --server domain.com --level Full`

REMÉDIATION :
Score <25 excellent, 25-50 bon, 51-75 moyen, >75 critique. Corriger priorités hautes.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

16.1.2 *Purple Knight assessments*

DESCRIPTION :
Purple Knight (Semperis) analyse 100+ indicateurs sécurité AD avec focus cyberattaques.

AUDIT :
Installer Purple Knight, exécuter assessment complet, analyser rapport JSON/HTML

REMÉDIATION :
Corriger indicateurs critiques (rouge), prioriser selon environnement et risques.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

16.1.3 *BloodHound/AzureHound analyses*

DESCRIPTION :
BloodHound révèle chemins attaque vers DA. AzureHound pour environnements hybrides.

AUDIT :
`SharpHound.exe -c All --stealth` puis analyse dans interface BloodHound

REMÉDIATION :
Éliminer tous chemins vers Domain Admins, corriger ACL dangereuses, groupes privilégiés.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

16.1.4 *Testimo health checks*

DESCRIPTION :
Testimo (PowerShell) vérifie santé globale AD : réplication, DNS, certificats, GPO.

AUDIT :
`Install-Module Testimo; Invoke-Testimo -Configuration Testimo.json`

REMÉDIATION :
Corriger erreurs réplication, DNS, expiration certificats, GPO corrompues.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

16.1.5 *ADRecon inventaires complets*

DESCRIPTION :
ADRecon génère inventaire détaillé AD : utilisateurs, groupes, GPO, ACL, trusts.

AUDIT :
`ADRecon.ps1 -DomainController DC01.domain.com -OutputType Excel`

REMÉDIATION :
Analyser rapport Excel, identifier objets obsolètes, permissions excessives, anomalies.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

16.1.6 *Adalanche graph analysis*

DESCRIPTION :
Adalanche analyse relations objets AD avec interface graphique pour chemins complexes.

AUDIT :
`adalanche collect ldap://dc.domain.com` puis analyse web interface

REMÉDIATION :
Identifier chemins attaque non détectés par autres outils, corriger relations dangereuses.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

16.1.7 *PlumHound reporting*

DESCRIPTION :
PlumHound génère rapports automatisés à partir données BloodHound pour management.

AUDIT :
```
python3 PlumHound.py -s neo4j://localhost:7687 -u neo4j -p password --easy
```

REMÉDIATION :
Utiliser rapports pour communication risques, suivi corrections, tableaux de bord.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

16.1.8 *DVAD (Damn Vulnerable AD) testing*

DESCRIPTION :
DVAD environnement lab vulnérable pour tester outils sécurité et techniques attaque AD.

AUDIT :
Déployer DVAD lab, tester outils détection, valider procédures réponse incident

REMÉDIATION :
Former équipes sur environnement contrôlé, améliorer détections, tester playbooks.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

16.1.9-10 *Outils complémentaires*

16.1.9 - ADSec toolkit (reconnaissance permissions) | **16.1.10** - Grouper2 (analyse appartenances groupes)

Résultat global section 16: ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

17.0 — RÉPONSE INCIDENTS

17.1.1 *Playbook compromission AD*

DESCRIPTION :
Plan détaillé réponse incident AD : identification, confinement, éradication, récupération.

AUDIT :
```
Test-Path "C:\IR-Playbooks\AD-Compromise-Response.docx"
```

REMÉDIATION :
Créer playbook avec étapes précises, contacts, outils, délais. Tester annuellement.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

17.1.2 *Procédure KRBTGT rotation d'urgence*

DESCRIPTION :
KRBTGT compromise invalide tous tickets Kerberos. Rotation d'urgence en 2 phases requise.

AUDIT :
```
New-ADServiceAccount -Name "KRBTGT-Emergency" -RestrictToSingleComputer
```

REMÉDIATION :
Script automatisé rotation KRBTGT, double rotation, validation réplication, tests services.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

17.1.3 *Comptes d'accès d'urgence (Break Glass)*

DESCRIPTION :
Comptes d'urgence pour accès AD si compromise complète ou indisponibilité systèmes IAM.

AUDIT :
```
Get-ADUser "EmergencyAdmin*" -Properties PasswordLastSet,LastLogonDate
```

REMÉDIATION :
2+ comptes emergency, mots de passe complexes, coffre-fort physique, audit strict.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

17.1.4 *Procédure isolation DC compromis*

DESCRIPTION :
Isoler rapidement DC compromis sans impacter services AD pour autres DC.

AUDIT :
Procédure réseau (VLAN, firewall), arrêt services, isolation physique documentée

REMÉDIATION :
Scripts isolation automatique, validation impact réplication, communication équipes.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

17.1.5 *Runbook récupération forêt*

DESCRIPTION :
Procédure complète restauration forêt AD après compromise : ordre DC, validation, tests.

AUDIT :
Documentation détaillée, environnement test, validation procédures annuelle

REMÉDIATION :
Runbook étape par étape, rôles/responsabilités, critères validation, rollback.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

17.1.6 *Waves reset credentials*

DESCRIPTION :
Reset massif mots de passe par vagues selon criticité après compromise AD.

AUDIT :
Scripts PowerShell reset, matrice priorités utilisateurs, communication

REMÉDIATION :
Tier 0 > Tier 1 > Tier 2, validation identité, MFA obligatoire, monitoring.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

17.1.7 *Plan communication crise AD*

DESCRIPTION :
Communication structurée incident AD : interne (IT, management) et externe (clients, régulateurs).

AUDIT :
Templates communication, contacts d'urgence, canaux alternatifs, chronologie

REMÉDIATION :
Messages pré-rédigés, approbation légale, escalation management, médias sociaux.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

17.1.8-10 *Procédures complémentaires*

17.1.8 - Forensic AD (préservation preuves) | **17.1.9** - Coordination autorités (ANSSI, police) | **17.1.10** - Post-incident review et amélioration continue

Résultat global section 17: ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

18.0 — CONFORMITÉ & GOUVERNANCE

18.1.1 *Mappage contrôles NIS2/RGPD*

DESCRIPTION :
Mappage contrôles AD vers exigences réglementaires NIS2, RGPD, sectorielles.

AUDIT :
Matrice contrôles ↔ réglementations, gaps analysis, preuves conformité

REMÉDIATION :
Documentation mappings, audits conformité, corrections gaps, certifications.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

18.1.2 *Documentation configurations AD*

DESCRIPTION :
Documentation complète et maintenue architecture, configurations, procédures AD.

AUDIT :
`Test-Path "C:\AD-Documentation\*.docx"`, dates mise à jour, revues qualité

REMÉDIATION :
Standards documentation, templates, revues trimestrielles, versioning, accès contrôlé.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

18.1.3 *Change management AD*

DESCRIPTION :
Processus formel gestion changements AD : approbation, test, rollback, validation.

AUDIT :
CAB (Change Advisory Board), RFC templates, registre changements, KPI

REMÉDIATION :
Workflow approbation, environnement test, validation impact, documentation.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

18.1.4 *Revues accès trimestrielles*

DESCRIPTION :
Revue formelle et documentée de tous accès privilégiés AD : validation propriétaires métier.

AUDIT :
`Get-ADGroupMember "Domain Admins" | Export-Csv AccessReview-Q1.csv`

REMÉDIATION :
Processus revue, matrices RACI, attestations managers, corrections tracking.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

18.1.5 *Formation équipes AD*

DESCRIPTION :
Formation continue équipes sur sécurité AD, nouvelles menaces, bonnes pratiques.

AUDIT :
Plan formation annuel, certifications (CISSP, GSEC), exercices pratiques

REMÉDIATION :
Budget formation, cursus sécurité AD, veille menaces, knowledge sharing.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

18.1.6 *Métriques sécurité AD (KPI)*

DESCRIPTION :
Tableau de bord sécurité AD : scores risques, incidents, conformité, améliorations.

AUDIT :
Dashboard automatisé, KPI définis (MTTR, score PingCastle, % conformité)

REMÉDIATION :
Métriques SMART, reporting management, tendances, actions correctives.

Résultat : ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A **Commentaire :** _____

18.1.7-10 *Gouvernance complémentaire*

18.1.7 - Audit interne annuel AD | **18.1.8** - Gestion risques AD (registre, mitigation) | **18.1.9** - Continuité activité AD (BCP/DRP) | **18.1.10** - Amélioration continue (PDCA, lessons learned)

Résultat global section 18: ☐ ✅ ☐ ❌ ☐ ⚠️ ☐ N/A

📊 TABLEAU RÉCAPITULATIF DES CONTRÔLES

📈 RÉSUMÉ EXÉCUTIF

Score de Maturité Sécurité AD

- **Score Global :** [À calculer selon implémentation]
- **Répartition par criticité :** 20% Critique, 47% Élevé, 31% Moyen, 2% Faible

Top 3 Risques Critiques Identifiés

1. 🔴 **Gestion des Privilèges :** 55 contrôles critiques non conformes
2. 🔴 **Authentification Faible :** Protocoles legacy, NTLM non restreint
3. 🔴 **Manque Détection :** Surveillance insuffisante des attaques AD

Roadmap de Remédiation Recommandée

Phase 1 - Urgence (0-30 jours)

- Rotation KRBTGT immédiate
- Limitation Domain Admins <5 membres
- Activation LDAP Signing obligatoire
- Déploiement monitoring básico eventos críticos

Phase 2 - Court terme (1-3 mois)

- Implémentation modèle Tiering
- Migration vers gMSA pour services
- Configuration audit avancé
- Déploiement PAW pour admins Tier 0

Phase 3 - Moyen terme (3-6 mois)

- Restriction complète NTLM
- Déploiement AD CS sécurisé
- Intégration SIEM optimisée
- Formation équipes sécurité AD

Phase 4 - Long terme (6-12 mois)

- Implémentation JIT/JEA complet
- Zero Trust architecture
- Automatisation réponse incidents
- Certification sécurité équipes

🗂️ MAPPINGS CONFORMITÉ

NIST 800-53 Rev5

- **AC (Access Control) :** 89 contrôles couverts
- **AU (Audit) :** 34 contrôles couverts
- **IA (Identification & Authentication) :** 52 contrôles couverts
- **SC (System Communications) :** 41 contrôles couverts

ISO 27001:2022

- **A.5 Organizational :** 18 contrôles couverts
- **A.6 People :** 12 contrôles couverts
- **A.8 Technology :** 156 contrôles couverts

MITRE ATT&CK pour Enterprise

- **Initial Access :** 23 techniques couvertes
- **Execution :** 15 techniques couvertes
- **Privilege Escalation :** 34 techniques couvertes
- **Defense Evasion :** 28 techniques couvertes
- **Credential Access :** 31 techniques couvertes
- **Discovery :** 19 techniques couvertes
- **Lateral Movement :** 18 techniques couvertes
- **Persistence :** 22 techniques couvertes

Conformité RGPD/NIS2

- **Protection données personnelles :** 45 contrôles applicables
- **Sécurité système information :** 187 contrôles applicables
- **Notification incidents :** 23 contrôles applicables

📋 TEMPLATE PLAN REMÉDIATION

Informations Projet

- **Client :** [Nom organisation]
- **Responsable Projet :** [Nom + contact]
- **Budget Alloué :** [Montant]
- **Deadline :** [Date limite]

Priorités par Phase

```
Phase 1 (Critique - 0-30j):
□ Contrôle 1.1.1 - Modèle Tiering
□ Contrôle 2.1.2 - Limitation Enterprise Admins
□ Contrôle 4.1.2 - Rotation KRBTGT
[...]

Phase 2 (Élevé - 1-3m):
□ Contrôle 2.1.5 - Migration gMSA
```

```
□ Contrôle 4.1.7 - LDAP Signing
□ Contrôle 10.1.1 - Audit avancé DC
[...]
```

Ressources Requises

- **Équipe Projet :** 4 personnes (Arch, Admin, Sécu, Test)
- **Formation :** 40h par personne minimum
- **Outils :** Licences, matériel, logiciels
- **Budget :** Estimation par phase

Métriques Succès

- **Couverture contrôles :** >90% Phase 1, >95% global
- **Temps détection incident :** <1h pour critique
- **Réduction surface attaque :** >80%
- **Conformité réglementaire :** 100%

📞 CONTACT & SUPPORT

🛡️ **AYI NEDJIMI CONSULTANTS (ANC)**

Excellence en Sécurité Active Directory

📧 **Email :** security@anc-consultants.com

📞 **Téléphone :** +33 (0)1 XX XX XX XX

🌐 **Web :** https://www.anc-consultants.com

📍 **Adresse :** [Adresse complète]

Équipe Spécialisée AD Security

- **Lead Consultant :** Expert certifié CISSP, SABSA, GCIH
- **Architectes AD :** 15+ ans expérience infrastructures critiques
- **Analystes SOC :** Spécialisés détection menaces AD avancées
- **Support 24/7 :** Hotline incidents sécurité AD

Version : 1.0 | **Date :** 04/04/2026 | **Pages :** [Auto] | **Contrôles :** 280

Annexe : Checklist (295 controles)

#	Recommandation	Niveau	Oui	Non	N/A
Section 1 — ARCHITECTURE & TIERING					
1.1.1	Modèle d'accès Enterprise (Tiering Model)	●	☐	☐	☐
1.1.2	Niveau fonctionnel de forêt minimum	●	☐	☐	☐
1.1.3	Architecture sites et sous-réseaux	●	☐	☐	☐
1.1.4	Séparation des rôles FSMO	●	☐	☐	☐
1.1.5	Configuration des trusts inter-domaines	●	☐	☐	☐
1.1.6	Contrôle des connexions clients LDAP	●	☐	☐	☐
1.1.7	Isolation des contrôleurs de domaine	●	☐	☐	☐
1.1.8	Contrôle des ports et services DC	●	☐	☐	☐
1.1.9	Redondance et haute disponibilité	●	☐	☐	☐
1.1.10	Contrôle des objets GPO orphelins	●	☐	☐	☐
1.1.11	Gestion des comptes de service intégrés	●	☐	☐	☐
1.1.12	Contrôle du catalogue global	●	☐	☐	☐
1.1.13	Protection contre DCShadow	●	☐	☐	☐
1.1.14	Configuration des UPN alternatives	●	☐	☐	☐
1.1.15	Contrôle des liens de sites coûteux	●	☐	☐	☐
1.1.16	Validation de la cohérence DNS	●	☐	☐	☐
1.1.17	Contrôle des quotas d'objets AD	●	☐	☐	☐
1.1.18	Architecture multi-forêt	●	☐	☐	☐
1.1.19	Contrôle des objets protégés AdminSDHolder	●	☐	☐	☐
1.1.20	Surveillance des modifications de schéma	●	☐	☐	☐
1.1.21	Contrôle des permissions sur les conteneurs système	●	☐	☐	☐
1.1.22	Configuration des sites Read-Only DC (RODC)	●	☐	☐	☐
1.1.23	Contrôle des objets Computer orphelins	●	☐	☐	☐
1.1.24	Validation de la topologie de réplication	●	☐	☐	☐
1.1.25	Contrôle des attributs sensibles non répliqués	●	☐	☐	☐
Section 2 — COMPTES PRIVILÉGIÉS					
2.1.1	Limitation des membres Domain Admins	●	☐	☐	☐
2.1.2	Sécurisation du groupe Enterprise Admins	●	☐	☐	☐
2.1.3	Contrôle du groupe Schema Admins	●	☐	☐	☐
2.1.4	Audit des comptes de service privilégiés	●	☐	☐	☐
2.1.5	Configuration des Group Managed Service Accounts (gMSA)	●	☐	☐	☐
2.1.6	Protection du compte KRBTGT	●	☐	☐	☐
2.1.7	Comptes avec délégation Kerberos non contrainte	●	☐	☐	☐
2.1.8	Audit des comptes avec SPN (Kerberoasting)	●	☐	☐	☐
2.1.9	Contrôle des comptes dormants privilégiés	●	☐	☐	☐
2.1.10	Configuration des Privileged Access Workstations (PAW)	●	☐	☐	☐
2.1.11	Just-in-Time (JIT) Administration	●	☐	☐	☐
2.1.12	Contrôle des permissions AdminSDHolder	●	☐	☐	☐
2.1.13	Protection contre AS-REP Roasting	●	☐	☐	☐
2.1.14	Gestion des comptes d'urgence (Break-Glass)	●	☐	☐	☐
2.1.15	Local Administrator Password Solution (LAPS)	●	☐	☐	☐
2.1.16	Audit des membres de groupes sensibles	●	☐	☐	☐
2.1.17	Protection des comptes de synchronisation	●	☐	☐	☐
2.1.18	Contrôle des comptes avec mots de passe n'expirant jamais	●	☐	☐	☐
2.1.19	Configuration Just Enough Administration (JEA)	●	☐	☐	☐
2.1.20	Surveillance des connexions privilégiées	●	☐	☐	☐
2.1.21	Protection contre le vol de credentials	●	☐	☐	☐
2.1.22	Audit des droits utilisateur sensibles	●	☐	☐	☐
2.1.23	Contrôle des Service Principal Names (SPN) dupliqués	●	☐	☐	☐
2.1.24	Gestion des comptes de liaison AD (Binding Accounts)	●	☐	☐	☐
2.1.25	Protection des hash NTLM des comptes privilégiés	●	☐	☐	☐
Section 3 — MOTS DE PASSE & AUTHENTIFICATION					
3.1.1	Configuration de la politique de mots de passe par défaut	●	☐	☐	☐
3.1.2	Implémentation des Fine-Grained Password Policies (FGPP)	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
3.1.3	Surveillance des mots de passe faibles	●	☐	☐	☐
3.1.4	Protection contre les attaques par pulvérisation (Password Spraying)	●	☐	☐	☐
3.1.5	Configuration de l'authentification multi-facteurs (MFA)	●	☐	☐	☐
3.1.6	Audit des comptes avec mots de passe réversibles	●	☐	☐	☐
3.1.7	Surveillance des tentatives de connexion suspectes	●	☐	☐	☐
3.1.8	Contrôle des comptes avec pré-authentification Kerberos désactivée	●	☐	☐	☐
3.1.9	Configuration des politiques de verrouillage de compte	●	☐	☐	☐
3.1.10	Audit des comptes avec mots de passe n'expirant jamais	●	☐	☐	☐
3.1.11	Protection contre les attaques de credential stuffing	●	☐	☐	☐
3.1.12	Configuration de Windows Hello for Business	●	☐	☐	☐
3.1.13	Surveillance des changements de mots de passe fréquents	●	☐	☐	☐
3.1.14	Contrôle des mots de passe par défaut des comptes système	●	☐	☐	☐
3.1.15	Audit des authentifications interactives sur les serveurs	●	☐	☐	☐
3.1.16	Configuration des Smart Cards et certificats	●	☐	☐	☐
3.1.17	Protection contre l'énumération de comptes	●	☐	☐	☐
3.1.18	Audit des connexions avec des comptes de service	●	☐	☐	☐
3.1.19	Configuration des politiques de session	●	☐	☐	☐
3.1.20	Surveillance des comptes avec privilèges de connexion étendus	●	☐	☐	☐
Section 4 — KERBEROS & PROTOCOLES					
4.1.1	Configuration du chiffrement Kerberos AES256	●	☐	☐	☐
4.1.2	Rotation du mot de passe KRBTGT	●	☐	☐	☐
4.1.3	Contrôle de la délégation Kerberos non contrainte	●	☐	☐	☐
4.1.4	Configuration de la délégation contrainte	●	☐	☐	☐
4.1.5	Implémentation de la délégation contrainte basée sur les ressources (RBCD)	●	☐	☐	☐
4.1.6	Restriction du protocole NTLM	●	☐	☐	☐
4.1.7	Configuration du LDAP Signing	●	☐	☐	☐
4.1.8	Activation du LDAP Channel Binding	●	☐	☐	☐
4.1.9	Protection contre les attaques Golden Ticket	●	☐	☐	☐
4.1.10	Détection des attaques Silver Ticket	●	☐	☐	☐
4.1.11	Configuration des tickets Kerberos - durées de vie	●	☐	☐	☐
4.1.12	Surveillance des événements Kerberos suspects	●	☐	☐	☐
4.1.13	Protection contre Pass-the-Hash (PtH)	●	☐	☐	☐
4.1.14	Protection contre Pass-the-Ticket (PtT)	●	☐	☐	☐
4.1.15	Configuration du SMB Signing	●	☐	☐	☐
4.1.16	Audit des comptes avec des SPN faibles	●	☐	☐	☐
4.1.17	Protection contre DCSync	●	☐	☐	☐
4.1.18	Configuration de l'audit Kerberos avancé	●	☐	☐	☐
4.1.19	Contrôle des enclaves Kerberos	●	☐	☐	☐
4.1.20	Protection contre les attaques Skeleton Key	●	☐	☐	☐
4.1.21	Configuration des protocoles d'authentification legacy	●	☐	☐	☐
4.1.22	Surveillance des échecs d'authentification Kerberos	●	☐	☐	☐
4.1.23	Configuration des algorithmes cryptographiques Kerberos	●	☐	☐	☐
4.1.24	Protection contre les attaques de downgrade	●	☐	☐	☐
4.1.25	Audit des tickets de service à longue durée	●	☐	☐	☐
4.1.26	Configuration de la protection Extended Protection for Authentication	●	☐	☐	☐
4.1.27	Surveillance des modifications de configuration Kerberos	●	☐	☐	☐
4.1.28	Protection des communications RPC	●	☐	☐	☐
4.1.29	Configuration des restrictions de protocole par réseau	●	☐	☐	☐
4.1.30	Audit des communications inter-domaines	●	☐	☐	☐
Section 5 — SÉCURITÉ GPO					
5.1.1	Permissions sur les GPO critiques	●	☐	☐	☐
5.1.2	Protection contre l'hijacking de GPO	●	☐	☐	☐
Section 6 — SÉCURITÉ DNS AD					
6.1.1	Configuration des zones DNS intégrées AD	●	☐	☐	☐
6.1.2	Activation des mises à jour dynamiques sécurisées	●	☐	☐	☐
6.1.3	Configuration DNSSEC pour la validation	●	☐	☐	☐
6.1.4	Contrôle des transferts de zone DNS	●	☐	☐	☐
6.1.5	Protection contre l'empoisonnement de cache DNS	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
6.1.6	Surveillance des requêtes DNS suspectes	●	☐	☐	☐
6.1.7	Configuration des forwarders DNS sécurisés	●	☐	☐	☐
6.1.8	Contrôle des enregistrements DNS critiques	●	☐	☐	☐
6.1.9	Protection des zones de recherche inversée	●	☐	☐	☐
6.1.10	Configuration des politiques de requête DNS	●	☐	☐	☐
6.1.11	Audit des modifications de configuration DNS	●	☐	☐	☐
6.1.12	Protection contre les attaques DDoS DNS	●	☐	☐	☐
6.1.13	Configuration de la réplication DNS sécurisée	●	☐	☐	☐
6.1.14	Contrôle des enregistrements DNS obsolètes	●	☐	☐	☐
6.1.15	Surveillance de la performance DNS	●	☐	☐	☐
Section 7 — RÉPLICATION & CONTRÔLEURS DE DOMAINE					
7.1.1	Surveillance de la santé de réplication AD	●	☐	☐	☐
7.1.2	Configuration sécurisée des Read-Only Domain Controllers (RODC)	●	☐	☐	☐
7.1.3	Protection contre les attaques DCSync	●	☐	☐	☐
7.1.4	Configuration de SYSVOL avec DFS-R	●	☐	☐	☐
7.1.5	Audit des connexions de réplication manuelles	●	☐	☐	☐
7.1.6	Surveillance des objets de métadonnées de réplication	●	☐	☐	☐
7.1.7	Configuration des intervalles de réplication	●	☐	☐	☐
7.1.8	Protection des partitions d'application AD	●	☐	☐	☐
7.1.9	Contrôle de la réplication inter-sites	●	☐	☐	☐
7.1.10	Audit des modifications de topologie KCC	●	☐	☐	☐
7.1.11	Protection contre les attaques DCShadow	●	☐	☐	☐
7.1.12	Configuration des Global Catalog servers	●	☐	☐	☐
7.1.13	Surveillance des tombstones et garbage collection	●	☐	☐	☐
7.1.14	Contrôle des USN (Update Sequence Numbers)	●	☐	☐	☐
7.1.15	Protection des connexions de réplication	●	☐	☐	☐
7.1.16	Audit des opérations de réplication privilégiées	●	☐	☐	☐
7.1.17	Configuration des notifications de réplication d'urgence	●	☐	☐	☐
7.1.18	Surveillance de la latence de réplication	●	☐	☐	☐
7.1.19	Configuration du nettoyage des objets liés	●	☐	☐	☐
7.1.20	Protection contre les conflits de réplication	●	☐	☐	☐
Section 8 — OBJETS AD & SCHÉMA					
8.1.1	Audit des permissions dangereuses sur objets AD	●	☐	☐	☐
8.1.2	Protection du conteneur AdminSDHolder	●	☐	☐	☐
8.1.3	Contrôle des objets avec adminCount orphelins	●	☐	☐	☐
8.1.4	Audit des extensions de schéma non standard	●	☐	☐	☐
8.1.5	Contrôle des permissions sur les unités d'organisation	●	☐	☐	☐
8.1.6	Surveillance des modifications d'objets critiques	●	☐	☐	☐
8.1.7	Contrôle des quotas de création d'objets	●	☐	☐	☐
8.1.8	Audit des objets avec SID History	●	☐	☐	☐
8.1.9	Protection contre la manipulation d'attributs sensibles	●	☐	☐	☐
8.1.10	Contrôle des objets dans des conteneurs non standard	●	☐	☐	☐
8.1.11	Audit des délégations de contrôle d'OU	●	☐	☐	☐
8.1.12	Contrôle des attributs confidentiels	●	☐	☐	☐
8.1.13	Surveillance des modifications de schéma	●	☐	☐	☐
8.1.14	Protection des liens critiques entre objets	●	☐	☐	☐
8.1.15	Contrôle des objets avec des ACL explicites	●	☐	☐	☐
8.1.16	Audit des objets système critiques	●	☐	☐	☐
8.1.17	Contrôle des objets orphelins ou corrompus	●	☐	☐	☐
8.1.18	Protection des attributs de construction dynamique	●	☐	☐	☐
8.1.19	Surveillance des objets de grande valeur (HVT)	●	☐	☐	☐
8.1.20	Contrôle de l'intégrité des backlinks	●	☐	☐	☐
Section 9 — AD CS / PKI					
9.1.1	Audit des templates de certificats dangereux (ESC1)	●	☐	☐	☐
9.1.2	Protection contre ESC2 (Any Purpose EKU)	●	☐	☐	☐
9.1.3	Contrôle ESC3 (Certificate Request Agent)	●	☐	☐	☐
9.1.4	Protection contre ESC4 (Vulnerable Template Access Control)	●	☐	☐	☐
9.1.5	Audit ESC5 (Vulnerable PKI Objects)	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
9.1.6	Protection contre ESC6 (EDITF_ATTRIBUTESUBJECTALTNAME2)	●	☐	☐	☐
9.1.7	Contrôle ESC7 (Vulnerable Certificate Authority Access Control)	●	☐	☐	☐
9.1.8	Protection contre ESC8 (NTLM Relay to AD CS)	●	☐	☐	☐
9.1.9	Audit des autorités de certification racine	●	☐	☐	☐
9.1.10	Configuration sécurisée des Certificate Revocation Lists (CRL)	●	☐	☐	☐
9.1.11	Implémentation OCSP (Online Certificate Status Protocol)	●	☐	☐	☐
9.1.12	Protection des clés privées des CA	●	☐	☐	☐
9.1.13	Audit des certificats émis avec privilèges	●	☐	☐	☐
9.1.14	Configuration de l'archivage des clés (Key Archival)	●	☐	☐	☐
9.1.15	Surveillance des événements PKI critiques	●	☐	☐	☐
9.1.16	Contrôle des templates de certificats cross-forest	●	☐	☐	☐
9.1.17	Protection contre Certificate Transparency bypass	●	☐	☐	☐
9.1.18	Audit des certificats avec Subject Alternative Names suspects	●	☐	☐	☐
9.1.19	Configuration des contraintes de nom sur les CA	●	☐	☐	☐
9.1.20	Surveillance des révocations de certificats	●	☐	☐	☐
9.1.21	Protection des CA subordinaires	●	☐	☐	☐
9.1.22	Audit des auto-enrollments	●	☐	☐	☐
9.1.23	Configuration des Certificate Templates version	●	☐	☐	☐
9.1.24	Protection contre les attaques de substitution de CA	●	☐	☐	☐
9.1.25	Audit des permissions sur les stores de certificats	●	☐	☐	☐
Section 10 — JOURNALISATION & DÉTECTION					
10.1.1	Configuration de l'audit avancé des contrôleurs de domaine	●	☐	☐	☐
10.1.2	Surveillance des événements de connexion critiques	●	☐	☐	☐
10.1.3	Détection des attaques Kerberoasting	●	☐	☐	☐
10.1.4	Surveillance des modifications d'objets AD critiques	●	☐	☐	☐
10.1.5	Configuration Microsoft Defender for Identity (MDI)	●	☐	☐	☐
10.1.6	Implémentation de honeytokens AD	●	☐	☐	☐
10.1.7	Surveillance des événements Kerberos suspects	●	☐	☐	☐
10.1.8	Configuration SIEM pour événements AD	●	☐	☐	☐
10.1.9	Surveillance des accès DCSync	●	☐	☐	☐
10.1.10	Détection des Golden/Silver Tickets	●	☐	☐	☐
10.1.11	Surveillance des créations de comptes privilégiés	●	☐	☐	☐
10.1.12	Configuration des Windows Event Forwarding (WEF)	●	☐	☐	☐
10.1.13	Surveillance des modifications de politique de groupe	●	☐	☐	☐
10.1.14	Détection des attaques Pass-the-Hash/Ticket	●	☐	☐	☐
10.1.15	Configuration de l'audit des accès objets AD	●	☐	☐	☐
10.1.16	Surveillance des connexions administratives	●	☐	☐	☐
10.1.17	Configuration PowerShell script block logging	●	☐	☐	☐
10.1.18	Surveillance des services critiques AD	●	☐	☐	☐
10.1.19	Détection des attaques Skeleton Key	●	☐	☐	☐
10.1.20	Configuration de l'archivage des logs de sécurité	●	☐	☐	☐
10.1.21	Surveillance des modifications de configuration DNS	●	☐	☐	☐
10.1.22	Configuration des alertes temps réel	●	☐	☐	☐
10.1.23	Surveillance des tentatives de brute force	●	☐	☐	☐
10.1.24	Configuration de l'audit des privilèges spéciaux	●	☐	☐	☐
10.1.25	Implémentation de canaries et tripwires	●	☐	☐	☐
Section 11 — SAUVEGARDE & RÉCUPÉRATION					
11.1.1	Windows Server Backup pour AD	●	☐	☐	☐
11.1.2	Sauvegarde System State automatisée	●	☐	☐	☐
11.1.3	Snapshots NTDS avec ntdsutil	●	☐	☐	☐
11.1.4	Activation AD Recycle Bin	●	☐	☐	☐
11.1.5	Plan de récupération de forêt documenté	●	☐	☐	☐
11.1.6	Restauration authoritative vs non-authoritative	●	☐	☐	☐
11.1.7	Vérification d'intégrité des sauvegardes	●	☐	☐	☐
11.1.8	Sauvegarde SYSVOL et DFSR	●	☐	☐	☐
11.1.9	Sauvegarde DC hors ligne	●	☐	☐	☐
11.1.10	Chiffrement des sauvegardes AD	●	☐	☐	☐
11.1.11	Sauvegarde des certificats AD CS	●	☐	☐	☐
11.1.12	Test de restauration trimestriel	●	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
11.1.13	Sauvegarde hors site (3-2-1 rule)	●	☐	☐	☐
11.1.14	Logs et alertes de sauvegarde	●	☐	☐	☐
11.1.15	Documentation procédures de récupération	●	☐	☐	☐
Section 12 — ENTRA CONNECT					
12.1.1	Durcissement serveur AAD Connect (Tier 0)	●	☐	☐	☐
12.1.2	Filtrage de synchronisation par OU	●	☐	☐	☐
12.1.3	Filtrage de synchronisation par attributs	●	☐	☐	☐
12.1.4	Password Hash Sync vs Pass-Through Auth	●	☐	☐	☐
12.1.5	Configuration Seamless SSO sécurisée	●	☐	☐	☐
12.1.6	Désactivation Password Writeback	●	☐	☐	☐
12.1.7	Configuration en mode Staging sécurisé	●	☐	☐	☐
12.1.8	Vérification régulière des exports	●	☐	☐	☐
12.1.9	Permissions minimales compte AAD Connect	●	☐	☐	☐
12.1.10	Durcissement SQL Server (si utilisé)	●	☐	☐	☐
12.1.11	Configuration auto-upgrade sécurisée	●	☐	☐	☐
12.1.12	Monitoring des erreurs de synchronisation	●	☐	☐	☐
12.1.13	Sauvegarde configuration AAD Connect	●	☐	☐	☐
12.1.14	Restriction accès console AAD Connect	●	☐	☐	☐
12.1.15	Plan de continuité AAD Connect	●	☐	☐	☐
Section 13 — CHEMINS D'ATTAQUE					
13.1.1	Collection BloodHound/SharpHound régulière	●	☐	☐	☐
13.1.2	Audit permissions WriteDACL dangereuses	●	☐	☐	☐
13.1.3	Audit permissions GenericAll/FullControl	●	☐	☐	☐
13.1.4	Audit permissions ForceChangePassword	●	☐	☐	☐
13.1.5	Nettoyage SID History abusif	●	☐	☐	☐
13.1.6	Désactivation Print Spooler sur DC	●	☐	☐	☐
13.1.7	Audit ADIDNS poisoning	●	☐	☐	☐
13.1.8	Contrôle délégations Kerberos dangereuses	●	☐	☐	☐
13.1.9	Resource-Based Constrained Delegation abuse	●	☐	☐	☐
13.1.10	Shadow Credentials attack prevention	●	☐	☐	☐
13.1.11	Certificate theft attack paths	●	☐	☐	☐
13.1.12	LAPS bypass techniques prevention	●	☐	☐	☐
13.1.13	Golden/Silver ticket defense	●	☐	☐	☐
Section 14 — TRUSTS					
14.1.1	Inventaire complet des trusts configurés	●	☐	☐	☐
14.1.2	Activation SID Filtering strict	●	☐	☐	☐
14.1.3	Configuration Selective Authentication	●	☐	☐	☐
14.1.4	Audit direction des trusts	●	☐	☐	☐
14.1.5	Surveillance authentifications cross-trust	●	☐	☐	☐
14.1.6	Validation PAM Trust (si applicable)	●	☐	☐	☐
14.1.7	Contrôle trusts External vs Forest	●	☐	☐	☐
14.1.8	Gestion des mots de passe de trust	●	☐	☐	☐
14.1.9	Prévention TGT delegation attacks	●	☐	☐	☐
14.1.10	Documentation et gouvernance des trusts	●	☐	☐	☐
Section 15 — DURCISSEMENT DC					
15.1.1	Services DC minimaux uniquement	●	☐	☐	☐
15.1.2	Windows Firewall DC restrictif	●	☐	☐	☐
15.1.3	SMB Signing obligatoire	●	☐	☐	☐
15.1.4	RDP désactivé ou sécurisé	●	☐	☐	☐
15.1.5	NTLMv2 uniquement	●	☐	☐	☐
15.1.6	PowerShell Constrained Language Mode	●	☐	☐	☐
15.1.7	Exclusions antivirus minimales	●	☐	☐	☐
15.1.8	LDAP Signing et Channel Binding	●	☐	☐	☐
15.1.9	Désactivation comptes invité/anonyme	●	☐	☐	☐
15.1.10	Chiffrement Kerberos AES256	●	☐	☐	☐
15.1.11-15	[Contrôles supplémentaires résumés]	●	☐	☐	☐
Section 16 — OUTILS D'ÉVALUATION					

#	Recommandation	Niveau	Oui	Non	N/A
16.1.1	PingCastle audits mensuels	●	☐	☐	☐
16.1.2	Purple Knight assessments	●	☐	☐	☐
16.1.3	BloodHound/AzureHound analyses	●	☐	☐	☐
16.1.4	Testimo health checks	●	☐	☐	☐
16.1.5	ADRecon inventaires complets	●	☐	☐	☐
16.1.6	Adalanche graph analysis	●	☐	☐	☐
16.1.7	PlumHound reporting	●	☐	☐	☐
16.1.8	DVAD (Damn Vulnerable AD) testing	●	☐	☐	☐
16.1.9-10	Outils complémentaires	●	☐	☐	☐
Section 17 — RÉPONSE INCIDENTS					
17.1.1	Playbook compromission AD	●	☐	☐	☐
17.1.2	Procédure KRBTGT rotation d'urgence	●	☐	☐	☐
17.1.3	Comptes d'accès d'urgence (Break Glass)	●	☐	☐	☐
17.1.4	Procédure isolation DC compromis	●	☐	☐	☐
17.1.5	Runbook récupération forêt	●	☐	☐	☐
17.1.6	Waves reset credentials	●	☐	☐	☐
17.1.7	Plan communication crise AD	●	☐	☐	☐
17.1.8-10	Procédures complémentaires	●	☐	☐	☐
Section 18 — CONFORMITÉ & GOUVERNANCE					
18.1.1	Mappage contrôles NIS2/RGPD	●	☐	☐	☐
18.1.2	Documentation configurations AD	●	☐	☐	☐
18.1.3	Change management AD	●	☐	☐	☐
18.1.4	Revues accès trimestrielles	●	☐	☐	☐
18.1.5	Formation équipes AD	●	☐	☐	☐
18.1.6	Métriques sécurité AD (KPI)	●	☐	☐	☐
18.1.7-10	Gouvernance complémentaire	●	☐	☐	☐