AYI NEDJIMI Consultants

NTFS Tampering et Anti-Forensics : Analyse Technique

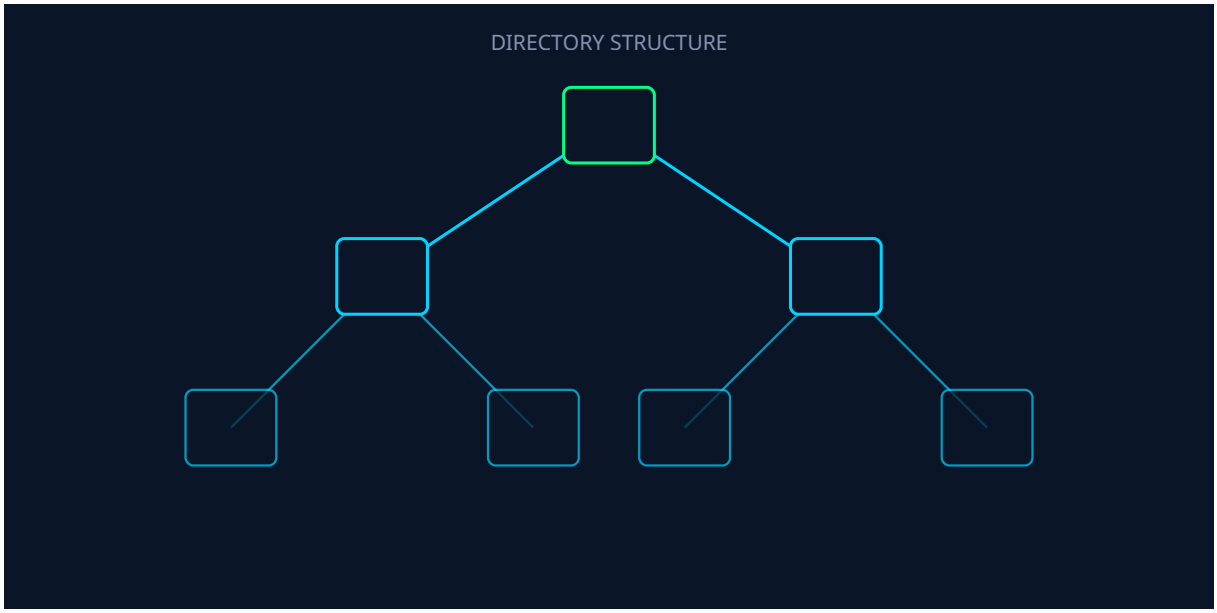
Catégorie : Attaques Active Directory Lecture : 10 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Techniques anti-forensics : manipulation MFT, timestomping, ADS. Méthodes de détection et investigation forensic. NTFS Tampering et Anti-Forensics.

Cette analyse detaillee de NTFS Tampering et Anti-Forensics s'appuie sur les retours d'experience d'equipes de securite confrontees quotidiennement aux menaces actuelles. Les methodologies presentees couvrent l'ensemble du cycle de vie de la securite, de la detection initiale a la remediation complete, en passant par l'investigation forensique et le durcissement des configurations. Les recommandations sont directement applicables dans les environnements de production et tiennent compte des contraintes operationnelles rencontrees par les equipes techniques sur le terrain. Les outils et techniques presentes ont ete valides dans des contextes reels d'incidents et de tests d'intrusion. La mise en oeuvre d'une strategie de defense en profondeur reste essentielle face a l'evolution constante du paysage des menaces, en combinant prevention, detection et capacite de reponse rapide aux incidents de securite.

Cette analyse technique de NTFS Tampering et Anti-Forensics s'appuie sur les retours d'experience d'equipes confrontees quotidiennement aux defis operationnels du domaine. Les methodologies presentees couvrent l'ensemble du cycle de vie, de la conception initiale au deploiement en production, en passant par les phases de test et de validation. Les recommandations sont directement applicables dans les environnements professionnels.

📑 Table des matières



• Introduction

- Qu'est-ce que Tampering NTFS / MFT ?
- Comment fonctionne l'attaque ?
- Méthodes de détection
- Contremesures et prévention
- Procédure de remédiation
- Conclusion

Votre Active Directory résisterait-il à une attaque Kerberoasting ?

🎯 Introduction

L'attaque **Tampering NTFS / MFT** représente une menace critique pour les environnements Active Directory modernes. Dans le secteur de la cybersécurité en 2025, cette technique d'attaque continue d'être largement exploitée par les acteurs malveillants, des cybercriminels opportunistes aux groupes APT (Advanced Persistent Threat) complexes. La securisation d'Active Directory represente un defi majeur pour les entreprises modernes. Les attaquants ciblent systematiquement ces infrastructures critiques, exploitant des configurations par defaut ou des privileges excessifs pour compromettre l'ensemble du systeme d'information. Cet article fournit une analyse technique approfondie des mecanismes d'attaque et des contre-mesures efficaces, basee sur des retours d'experience terrain et les recommandations des autorites de reference comme l'ANSSI et le MITRE.

Selon le Verizon Data Breach Investigations Report 2024, les attaques ciblant Active Directory représentent **plus de 80% des compromissions d'entreprise**. L'attaque Tampering NTFS / MFT fait partie du top 20 des techniques les plus observées en environnement réel.

⚠️ Impact critique
Altération de la MFT, timestamps, ou utilisation d'Alternate Data Streams (ADS) pour cacher malwares et entraver les enquêtes forensic

Une exploitation réussie peut permettre à un attaquant de :

- Maintenir une persistance long-terme dans le domaine
- Escalader ses privilèges jusqu'au niveau Domain Admin
- Se déplacer latéralement à travers le réseau
- Exfiltrer des données sensibles sans détection
- Déployer des ransomwares ou autres malwares

Ce guide expert, rédigé par **Ayi NEDJIMI**, consultant spécialisé en sécurité Active Directory, vous fournira une compréhension approfondie de cette attaque, des techniques de détection avancées et des stratégies de défense éprouvées.

Notre avis d'expert
Le modèle Zero Trust remet fondamentalement en question l'architecture traditionnelle d'Active Directory. Pourtant, la majorité des entreprises restent dépendantes d'AD pour leur gestion d'identités. La transition vers une architecture hybride sécurisée nécessite une planification minutieuse et un modèle de Tiering rigoureux.

📚 Qu'est-ce que Tampering NTFS / MFT ?

L'attaque **Tampering NTFS / MFT** est une technique d'exploitation d'Active Directory qui permet à un attaquant de : *Altération de la MFT, timestamps, ou utilisation d'Alternate Data Streams (ADS) pour cacher malwares et entraver les enquêtes forensic*

Contexte historique

Cette technique a été popularisée dans la communauté sécurité autour de 2015-2016, bien que les principes sous-jacents soient connus depuis plus longtemps. Elle a été documentée dans plusieurs frameworks d'attaque :

- **MITRE ATT&CK** : Technique référencée dans le framework de tactiques adversaires
- **Mimikatz** : Outil incluant des modules pour cette attaque (Benjamin Delpy)
- **BloodHound** : Capacité à identifier les chemins d'attaque potentiels
- **Impacket** : Suite Python incluant des outils d'exploitation

Prérequis de l'attaque

Pour qu'un attaquant puisse mener cette attaque avec succès, plusieurs conditions doivent généralement être réunies :

✅ Conditions d'exploitation

- **Accès initial** : Compromission d'au moins un compte utilisateur ou machine dans le domaine
- **Privilèges requis** : Selon l'attaque, des privilèges spécifiques peuvent être nécessaires
- **Outils d'attaque** : Mimikatz, Rubeus, Impacket, ou outils personnalisés
- **Connaissance du domaine** : Compréhension de la topologie et des comptes sensibles

Différences avec d'autres attaques similaires

Caractéristique	Tampering NTFS / MFT	Autres techniques
Furtivité	Élevée - difficile à détecter	Variable selon la technique
Persistance	Long-terme possible	Souvent temporaire
Complexité	Modérée à élevée	Variable
Impact	Critique - accès privilégié	Dépend de la technique

Voir aussi notre article sur le Top 10 des Attaques Active Directory pour une vue d'ensemble complète du paysage des menaces.

⚙️ Comment fonctionne l'attaque ?

Comprendre le fonctionnement technique de l'attaque **Tampering NTFS / MFT** est essentiel pour mettre en place des défenses efficaces. Décomposons l'attaque en phases distinctes :

Phase 1 : Reconnaissance et énumération

L'attaquant commence par énumérer l'environnement Active Directory pour identifier les cibles potentielles. Outils et techniques couramment utilisés :

```
# Énumération avec PowerView (PowerShell)
Import-Module PowerView.ps1
Get-DomainUser -Properties samaccountname,description
Get-DomainComputer
Get-DomainGroup

# Énumération LDAP avec Python (ldap3)
from ldap3 import Server, Connection, ALL
server = Server('dc.exemple.local', get_info=ALL)
conn = Connection(server, user='DOMAIN\user', password='pass')
conn.search('dc=exemple,dc=local', '(objectClass=*)')

# Énumération avec BloodHound
SharpHound.exe -c All -d exemple.local
```

Phase 2 : Exploitation

Une fois les cibles identifiées, l'attaquant procède à l'exploitation proprement dite. Les techniques varient selon les privilèges disponibles :

🔴 **Techniques d'exploitation courantes**

- Utilisation de **Mimikatz** pour interagir avec LSASS
- Exploitation via **Rubeus** pour les attaques Kerberos
- Utilisation d'**Impacket** pour les opérations à distance
- Scripts PowerShell personnalisés pour la furtivité

Phase 3 : Post-exploitation

Après une exploitation réussie, l'attaquant cherche à :

1. **Maintenir l'accès** : Création de backdoors, comptes cachés
2. **Escalader les privilèges** : Progression vers Domain Admin
3. **Mouvement latéral** : Compromission d'autres systèmes
4. **Exfiltration** : Vol de données sensibles

Chaîne d'attaque typique (Kill Chain)

Voici un scénario réaliste d'exploitation :

1. **Initial Access** : Phishing avec macro malveillante → Beacon Cobalt Strike
2. **Enumeration** : Découverte du domaine avec BloodHound
3. **Privilege Escalation** : Exploitation de Tampering NTFS / MFT
4. **Lateral Movement** : PsExec / WMI vers serveurs sensibles
5. **Persistence** : Golden Ticket / Silver Ticket / Skeleton Key
6. **Data Exfiltration** : Rapatriement via DNS tunneling ou HTTPS

Note forensique : Les artifacts de cette attaque peuvent persister dans les logs pendant 90 à 180 jours selon votre politique de rétention. Une investigation rétrospective est souvent possible.

Pour approfondir les techniques d'investigation, consultez notre guide sur le Forensics Windows et Active Directory.

Cas concret
L'attaque SolarWinds (2020) a utilisé la technique Golden SAML pour forger des tokens d'authentification, permettant un accès persistant aux environnements Microsoft 365 et Azure AD sans déclencher d'alertes. Cette technique a démontré que la compromission d'un serveur AD FS pouvait anéantir la confiance dans toute l'infrastructure d'identité.

Savez-vous combien de comptes à privilèges existent réellement dans votre domaine ?

🔍 Méthodes de détection

La détection de l'attaque **Tampering NTFS / MFT** repose sur une approche multicouche combinant :

- Surveillance des logs Windows et Active Directory
- Corrélation d'événements via SIEM
- Solutions EDR (Endpoint Detection and Response)
- Produits spécialisés de protection d'identité (Microsoft Defender for Identity, etc.)

Event IDs Windows critiques

Incohérences entre MFT/timestamps et journaux d'événements, fichiers avec ADS inhabituels, alertes d'intégrité bas-niveau

Event ID	Log Source	Description	Priorité
4768	Security	Ticket TGT Kerberos demandé	Haute
4769	Security	Ticket service Kerberos demandé	Haute
4662	Security	Opération effectuée sur un objet AD	Critique
4624	Security	Ouverture de session réussie	Moyenne
4672	Security	Privilèges spéciaux attribués	Haute

Requêtes SIEM (Splunk / Microsoft Sentinel)

Splunk Query

```
index=windows EventCode=4768 OR EventCode=4769
| stats count by src_ip, user, dest
| where count > 50
| table _time, src_ip, user, dest, count
| sort -count
```

Microsoft Sentinel (KQL)

```
SecurityEvent
| where EventID in (4768, 4769, 4662)
| where TimeGenerated > ago(24h)
| summarize Count=count() by Account, Computer, IpAddress
| where Count > 50
| order by Count desc
```

Solutions EDR et Identity Protection

🛡️ **Outils de détection recommandés**

- **Microsoft Defender for Identity** : Détection native des attaques AD, alertes en temps réel
- **CrowdStrike Falcon** : EDR avec détection comportementale avancée
- **Vectra AI** : IA pour détection d'anomalies réseau et AD
- **Silverfort** : Protection d'identité unifiée pour AD hybride
- **Sysmon** : Logging avancé des événements système (gratuit)

Indicateurs de compromission (IOC)

Soyez attentif aux signes suivants :

- Accès à LSASS par des processus non autorisés
- Requêtes LDAP massives depuis workstations
- Tickets Kerberos avec durées inhabituelles (> 10 heures)
- Authentifications depuis adresses IP inconnues
- Modifications d'attributs sensibles AD (ACL, groupes, SPN)

Consultez également notre article sur les Top 5 Outils d'Audit Active Directory pour découvrir les meilleurs outils de détection.

🛡️ Contremesures et prévention

La prévention de l'attaque **Tampering NTFS / MFT** nécessite une approche de défense en profondeur (Defense in Depth). Voici les mesures recommandées :

1. Architecture de sécurité (Tiered Administration)

Implémentez un modèle d'administration par niveaux (Tier 0/1/2) pour limiter l'exposition :

🏗️ **Modèle Tiered Administration**

- **Tier 0** : Domain Controllers, comptes Domain Admin, serveurs d'identité
  - Stations d'administration dédiées (PAW - Privileged Access Workstations)
  - MFA obligatoire
  - Pas de navigation Internet
  - Pas d'email

- **Tier 1** : Serveurs applicatifs, serveurs de fichiers
  - Comptes d'administration séparés de Tier 0
  - Jump servers pour l'accès
  - MFA recommandé
- **Tier 2** : Workstations utilisateurs
  - Comptes utilisateurs standard
  - Pas de privilèges admin locaux
  - UAC activé

2. Durcissement Active Directory

Monitoring d'intégrité fichier/MFT (solutions type tripwire), réduction des accès bas-niveau, snapshots immuables réguliers

Hardening Kerberos

```
# Forcer AES pour Kerberos (GPO)
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies
> Security Options
Network security: Configure encryption types allowed for Kerberos
→ Cocher uniquement AES128_HMAC_SHA1, AES256_HMAC_SHA1

# Réduire la durée de vie des tickets (GPO)
Computer Configuration > Policies > Windows Settings > Security Settings > Account
Policies > Kerberos Policy
Maximum lifetime for user ticket: 10 hours (default)
Maximum lifetime for service ticket: 600 minutes
Maximum lifetime for user ticket renewal: 7 days
```

Protected Users Group
Ajoutez les comptes privilégiés au groupe `Protected Users` (introduit dans Windows Server 2012 R2) :

- Pas de chiffrement DES ou RC4 Kerberos
- Pas de délégation Kerberos
- Pas de cache des credentials NTLM
- TGT max 4 heures (non renouvelable au-delà)

```
# PowerShell : Ajouter utilisateurs au groupe Protected Users
Add-ADGroupMember -Identity "Protected Users" -Members "AdminDA01","AdminDA02"
```

3. Solutions techniques de protection

Microsoft LAPS (Local Administrator Password Solution)
Rotation automatique des mots de passe administrateur locaux :

```
# Installation LAPS
msiexec /i LAPS.x64.msi /quiet

# Configuration GPO LAPS
Computer Configuration > Policies > Administrative Templates > LAPS
Enable local admin password management: Enabled
Password Settings:
  - Complexity: Large letters + small letters + numbers + specials
  - Length: 20 characters
  - Age: 30 days
```

Credential Guard (Windows 10/11 Enterprise, Server 2016+)
Protection par virtualisation des secrets d'identité :

```
# Activer Credential Guard (GPO ou script)
Computer Configuration > Administrative Templates > System > Device Guard
Turn On Virtualization Based Security: Enabled
  - Credential Guard Configuration: Enabled with UEFI lock

# Vérifier activation Credential Guard
Get-ComputerInfo | select DeviceGuardSecurityServicesConfigured
```

4. Surveillance et audit

✅ Checklist de prévention

- ☑️ Audit SACL activé sur objets sensibles AD
- ☑️ Rétention des logs Security minimum 180 jours
- ☑️ SIEM avec corrélation d'événements AD
- ☑️ EDR déployé sur tous les endpoints
- ☑️ Microsoft Defender for Identity configuré
- ☑️ Honeypots / Deception technologies déployés
- ☑️ Segmentation réseau (VLANs, micro-segmentation)
- ☑️ MFA pour tous les comptes privilégiés
- ☑️ Revue trimestrielle des ACL AD
- ☑️ Pentest annuel ciblé Active Directory

Pour un guide complet de sécurisation, consultez notre Guide de Sécurisation Active Directory 2025.

🚨 Procédure de remédiation

Si vous suspectez ou confirmez une compromission via **Tampering NTFS / MFT**, suivez cette procédure de réponse à incident :

⚠️ Avertissement critique
Ne prenez jamais de mesures précipitées qui pourraient alerter l'attaquant ou détruire des preuves forensiques. Documentez chaque action et coordonnez-vous avec votre équipe IR (Incident Response).

Phase 1 : Containment (Confinement) ⏱️ 0-4 heures

1. **Isoler les systèmes compromis**
   - Déconnecter du réseau (physiquement si critique)
   - Désactiver les comptes compromis (ne pas supprimer)
   - Bloquer les adresses IP sources suspectes (firewall)
2. **Préserver les preuves**
   - Capturer images mémoire (RAM) avec FTK Imager ou WinPmem
   - Exporter les logs pertinents avant rotation
   - Prendre snapshots des VMs affectées
3. **Activer le mode "Incident Response"**
   - Augmenter le niveau de logging (verbose)
   - Activer monitoring continu (24/7)
   - Notifier le management et l'équipe juridique

Phase 2 : Évaluation de l'impact ⏱️ 4-12 heures

1. **Analyse forensique**

```
# Analyse mémoire avec Volatility
volatility -f memory.dmp --profile=Win10x64 psscan
volatility -f memory.dmp --profile=Win10x64 dlllist -p
volatility -f memory.dmp --profile=Win10x64 malfind

# Analyse disque avec PowerForensics
Get-ForensicTimeline -VolumeName C:\ | Export-Csv timeline.csv
Get-ForensicEventLog -Path C:\Windows\System32\winevt\Logs\Security.evtx
```

2. **Identifier la portée**
   - Quels comptes ont été compromis ?
   - Quels systèmes ont été accédés ?
   - Quelles données ont été exfiltrées ?
   - Depuis combien de temps l'attaquant est-il présent ? (Dwell Time)

Phase 3 : Eradication ⏱️ 12-48 heures

Isoler endpoint, image forensic, restaurer depuis snapshot sain, corriger privilèges

1. **Supprimer la présence de l'attaquant**
   - Réinitialiser mots de passe de tous les comptes compromis
   - Révoquer certificats et tokens compromis
   - Supprimer backdoors et malwares identifiés
   - Corriger les vulnérabilités exploitées
2. **Réimager les systèmes critiques**
   - Domain Controllers si compromission confirmée
   - Serveurs critiques (SQL, Exchange, etc.)

- Workstations administratives

Phase 4 : Recovery (Récupération) ⏱️ 48-72 heures

1. **Restauration des services**
   - Validation de l'intégrité AD (dcdiag, repadmin)
   - Tests de fonctionnement
   - Retour progressif à la normale
2. **Monitoring renforcé**
   - Surveillance 24/7 pendant 30 jours minimum
   - Recherche de réinfection
   - Validation que l'attaquant n'a plus accès

Phase 5 : Lessons Learned ⏱️ Post-incident

📊 **Post-Mortem**

- Rédaction d'un rapport d'incident détaillé
- Identification des failles de sécurité exploitées
- Mise à jour du plan de réponse à incident
- Formation des équipes sur les leçons apprises
- Implémentation de contrôles compensatoires

Quand faire appel à un expert externe ?

Faites appel à un consultant spécialisé en réponse à incident Active Directory si :

- Vous manquez d'expertise interne en forensics AD
- L'attaque est aboutie (APT potentiel)
- Vous avez besoin d'un regard externe impartial
- Des obligations réglementaires l'exigent (RGPD, NIS2, etc.)

Consultez notre page Investigation Forensics pour plus d'informations sur nos services de réponse à incident.

Approche defensive structuree

Quels outils forensiques permettent de detecter la falsification de la MFT ?

Les outils cles incluent Autopsy et Sleuth Kit pour l'analyse comparative des timestamps MFT avec les timestamps du journal USN ($UsnJrnl), MFTECmd d'Eric Zimmerman pour le parsing rapide de la MFT avec detection d'anomalies, NTFS Log Tracker pour l'analyse du journal $LogFile, et Velociraptor pour la collecte et l'analyse a distance de la MFT sur un parc de machines. La technique fondamentale consiste a croiser les timestamps $STANDARD_INFORMATION avec $FILE_NAME dans chaque enregistrement MFT, car seul $SI est modifiable via les API standard.

Pourquoi les techniques de timestomping sont-elles encore efficaces malgre les solutions EDR modernes ?

Le timestomping reste efficace car de nombreuses solutions EDR surveillent les API Windows de haut niveau (SetFileTime, NtSetInformationFile) mais ne detectent pas les modifications directes des structures NTFS au niveau du disque physique. Les attaquants avances utilisent des drivers noyau ou accedent directement au volume physique pour modifier les attributs $STANDARD_INFORMATION sans declencher les hooks des EDR. Seule une analyse forensique approfondie comparant les quatre timestamps SI avec les timestamps FN et les entrees du journal USN peut reveler ces manipulations.

Pour approfondir, consultez les ressources officielles : OWASP Testing Guide, CVE Details et ANSSI.

Sources et références : MITRE ATT&CK Privilege Escalation · ADSecurity.org

🎓 Conclusion

L'attaque **Tampering NTFS / MFT** représente une menace réelle et actuelle pour les environnements Active Directory. Comme nous l'avons vu dans ce guide, cette technique peut avoir des conséquences critiques si elle n'est pas détectée et mitigée rapidement.

Points clés à retenir

✅ **Synthèse des bonnes pratiques**

- **Prévention** : Monitoring d'intégrité fichier/MFT (solutions type tripwire), réduction des accès bas-niveau, snapshots immuables réguliers
- **Détection** : Incohérences entre MFT/timestamps et journaux d'événements, fichiers avec ADS inhabituels, alertes d'intégrité bas-niveau
- **Remédiation** : Isoler endpoint, image forensic, restaurer depuis snapshot sain, corriger privilèges
- **Architecture** : Modèle Tier 0/1/2, PAW, MFA, LAPS
- **Surveillance** : SIEM, EDR, Microsoft Defender for Identity

Prochaines étapes recommandées

1. **Évaluation de la posture actuelle**
   - Audit de sécurité Active Directory complet
   - Analyse de vulnérabilités avec BloodHound
   - Pentest ciblé AD
2. **Implémentation des contremesures prioritaires**
   - LAPS sur toutes les workstations
   - Protected Users pour comptes privilégiés
   - Microsoft Defender for Identity
   - Credential Guard sur endpoints Windows 10/11

3. **Formation et sensibilisation**
    - Formation des équipes IT aux attaques AD
    - Sensibilisation des utilisateurs (phishing, social engineering)
    - Exercices de simulation d'incidents (tabletop exercises)
4. **Amélioration continue**
    - Veille technologique sur les nouvelles menaces AD
    - Participation aux communautés sécurité (forums, conférences)
    - Tests réguliers (pentest annuel, purple teaming)

Ressources complémentaires

Pour approfondir vos connaissances sur la sécurité Active Directory, consultez nos autres ressources :

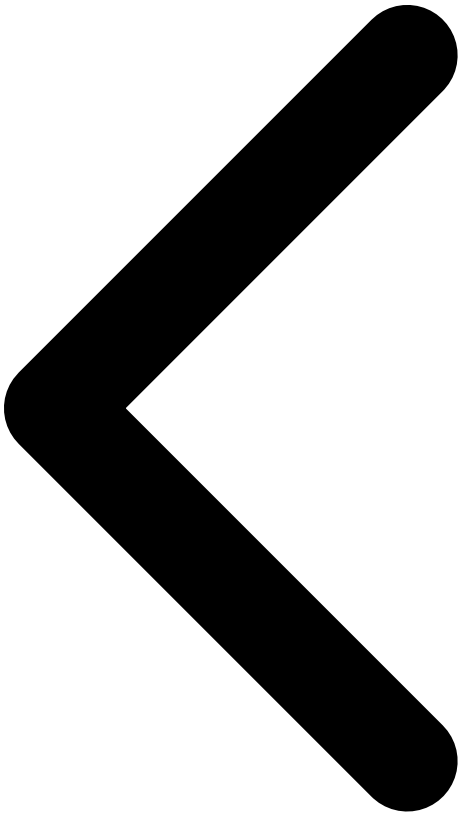
- Top 10 des Attaques Active Directory 2025
- Guide de Sécurisation Active Directory 2025
- Top 5 Outils d'Audit Active Directory
- Investigation Forensics Windows & Active Directory
- Nos Formations Cybersécurité
- Livres Blancs Gratuits

Citation : "La sécurité n'est pas un produit, mais un processus." — Bruce Schneier

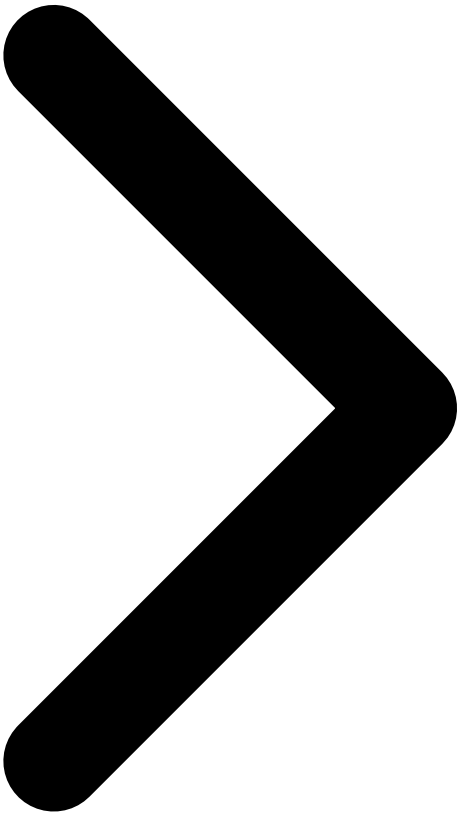
La protection contre Tampering NTFS / MFT et autres attaques Active Directory nécessite une approche holistique combinant technologie, processus et formation. N'attendez pas une compromission pour agir — la prévention est toujours plus efficace et moins coûteuse que la remédiation.

Besoin d'aide pour sécuriser votre Active Directory ?
Nos experts sont là pour vous accompagner.

Voir nos services



Article précédent Article suivant



Ressources open source associées :

- awesome-cybersecurity-tools — Liste de 100+ outils de cybersécurité

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr

© 2025 — Reproduction interdite sans autorisation.