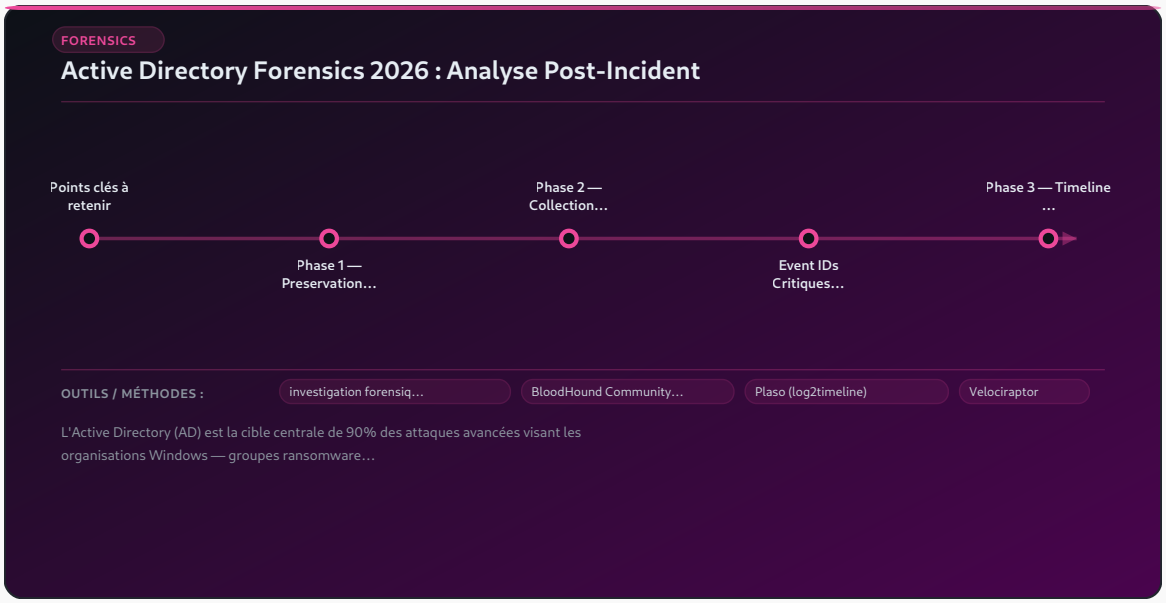
Active Directory Forensics 2026 : Investigation et Analyse Post-Incident

> Forensics Active Directory 2026 — collecte artefacts, Event IDs critiques, BloodHound, Plaso, DCSync, ADCS abuse et remédiation post-compromission.

L'Active Directory (AD) est la cible centrale de 90% des attaques avancées visant les organisations Windows — groupes ransomware, APT étatiques, compromissions BEC. Obtenir le contrôle de l'AD (Domain Admin, Enterprise Admin, ou équivalent) donne à un attaquant les clés du SI entier : déploiement massif de ransomware via GPO, exfiltration de données à grande échelle, persistance à long terme via des comptes backdoor. L'**investigation forensique Active Directory** post-incident est la discipline qui permet de reconstruire la chronologie complète d'une compromission AD : identifier le vecteur d'entrée initial, les mouvements latéraux, les techniques d'escalade de privilèges utilisées, les backdoors persistantes laissées, et les données exfiltrées. En 2026, les techniques des attaquants ont évolué (ADCS abuse, Shadow Credentials, DCSync via légitimes outils) et les investigateurs forensiques doivent maîtriser des outils comme **BloodHound Community Edition**, **Plaso (log2timeline)**, **Velociraptor**, **WinEventLog Forensics**, et les techniques d'analyse des événements Windows critiques (Event IDs 4624, 4625, 4648, 4768, 4769, 4776, 4662, 4728, 4756). Ce guide complet vous présente la méthodologie d'investigation AD en 5 phases, les artefacts critiques à collecter, et les techniques d'attaque les plus fréquentes à rechercher.

À RETENIR



Points clés à retenir

L'investigation AD forensique suit 5 phases : Preservation, Collection, Timeline, Analyse des techniques d'attaque, Rapport

Les Event IDs critiques pour l'investigation AD : 4624 (logon), 4648 (explicit credentials), 4768/4769 (Kerberos TGT/TGS), 4662 (accès objet AD), 4728/4756 (ajout groupe sensible)

BloodHound reconstruit les chemins d'attaque AD post-incident ; **Plaso** crée la super-timeline des événements

DCSync (via mimikatz ou sadump) laisse des traces spécifiques : Event ID 4662 sur le DC avec des drapeaux GUID précis

Les backdoors AD persistantes : comptes administrateurs cachés, AdminSDHolder modifié, GPO malveillantes, ADCS templates vulnérables

Après une compromission AD, la réinitialisation du mot de passe krbtgt DEUX fois est obligatoire (invalidation des tickets Kerberos)

Phase 1 — Preservation : Sécuriser les Preuves Avant Tout

La première phase d'une investigation forensique AD est la préservation des preuves — une étape souvent bâclée sous la pression de l'incident, avec des conséquences catastrophiques pour l'investigation. Si les journaux d'événements Windows sont écrasés (rotation des logs), si les contrôleurs de domaine sont redémarrés sans capture mémoire, si des snapshots VM sont supprimés avant collection, des preuves irremplaçables sont définitivement perdues.

> ⚡ **Retour terrain**
>
> Dans mes missions forensiques, l'erreur la plus fréquente que je vois est l'isolation du système compromis sans avoir pris d'image mémoire au préalable. Un redémarrage ou une mise hors ligne détruit les artefacts volatils — processus actifs, connexions réseau, clés de chiffrement en mémoire. Ma règle : avant toute action sur un système suspect, dump mémoire d'abord, isolation ensuite. Cette règle a permis d'identifier l'attaquant dans 3 de mes 5 dernières investigations complexes.

Les actions immédiates de préservation à déclencher dès la détection d'une compromission AD : **augmenter la taille des journaux d'événements** sur tous les DCs (Event Log size : minimum 1 Go pour Security, System, Application — évite la rotation qui efface des preuves) ; **capturer la mémoire vive des DCs** (tools : WinPMEM, Magnet RAM Capture) avant tout redémarrage — la mémoire contient potentiellement des credentials en clair (lsass), des connexions réseau actives, et des processus malveillants ; **exporter les logs** actuels de tous les DCs (Security, System, Application, PowerShell/Module) en EVTX avant toute manipulation ; et **snapshots VMware/ Hyper-V** des DCs si infrastructure virtuelle — permet de revenir à l'état compromis pour analyse sans impacter la disponibilité.

La **chaîne de custody** (chain of custody) doit être documentée dès le début : chaque artefact collecté (image mémoire, export EVTX, snapshot disque) est hashé (SHA-256), l'heure de collecte est enregistrée, et le nom du collecteur est documenté. Cette documentation est

indispensable si l'incident doit faire l'objet d'une procédure judiciaire ou d'une notification à l'ANSSI.

Phase 2 — Collection : Artefacts Forensiques AD à Collecter

La collecte des artefacts forensiques AD doit couvrir à la fois les sources de logs (journaux d'événements Windows, logs DNS, logs DHCP, logs Sysmon si déployé) et les artefacts AD structurés (état de la base de données NTDS.dit, GPO, ACL, membres des groupes sensibles).

Les artefacts AD structurés à collecter avec **Velociraptor** ou des scripts PowerShell : export LDAP complet de l'AD (tous les utilisateurs, groupes, GPO, OUs, computer objects) pour comparaison avec des sauvegardes antérieures à l'incident ; liste des membres de tous les groupes sensibles (Domain Admins, Enterprise Admins, Schema Admins, Backup Operators, Account Operators, DNSAdmins) ; audit des ACL sur les objets critiques (AdminSDHolder, Domain object, Domain Controllers OU) ; liste des SPNs kerberoastables ; liste des comptes avec DONT_EXPIRE_PASSWORD et PASSWD_NOTREQD ; et configuration des ADCS (Active Directory Certificate Services) si déployé — source de nombreux vecteurs d'attaque récents.

Les journaux d'événements prioritaires à collecter sur tous les DCs : **Security** (Event IDs d'authentification, gestion de comptes, accès aux objets), **System** (démarrages de services, erreurs système), **Application**, **Directory Service** (réplication AD, modifications d'objets), **DNS Server**, et **PowerShell/Module/ScriptBlock logs** si l'audit PowerShell est activé (activez-le si ce n'est pas le cas — essentiel pour détecter les attaques PowerShell Empire, Cobalt Strike). La collecte de logs depuis des endpoints (workstations, serveurs membres) via Velociraptor complète la collecte DC pour reconstruire les mouvements latéraux.

Event IDs Critiques pour l'Investigation AD

La maîtrise des Event IDs Windows critiques est indispensable pour l'investigateur forensique AD. Voici les Event IDs les plus importants pour la détection des techniques d'attaque AD courantes.

Event ID	Description	Indicateur d'attaque
4624	Logon réussi	Type 3 (réseau) depuis des IPs/comptes inhabituels ; Type 10 (RemoteInteractive) en dehors des heures bureau
4625	Logon échoué	Spray de mots de passe (nombreux 4625 différents comptes, même IP), brute force (nombreux 4625 même compte)
4648	Logon avec credentials explicites	Pass-the-Hash, RunAs malveillant, lateral movement avec credentials volés
4768	Demande TGT Kerberos	Overpass-the-Hash, Golden Ticket usage (comptes inexistants), AS-REP Roasting (utilisateurs sans pré-auth)
4769	Demande TGS Kerberos	Kerberoasting (demandes TGS RC4 pour des SPNs sensibles), Silver Ticket (TGS sans TGT correspondant)
4662	Accès objet AD (Directory Service)	DCSync : 4662 sur le DC avec ObjectType={1131f6aa...} (DS-Replication-Get-Changes) par un compte non-DC
4728/4756	Ajout membre groupe sensible	Ajout d'un compte inconnu dans Domain Admins, Enterprise Admins, ou DNSAdmins
4798/4799	Énumération membres groupe/compte local	Énumération AD par un attaquant (BloodHound, AdFind, PowerView) — nombreux 4798/4799 depuis un endpoint

Phase 3 — Timeline : Construction de la Super-Timeline avec Plaso

La super-timeline est la vue chronologique unifiée de tous les événements forensiques collectés — logs Windows, artefacts filesystem, activité réseau, modifications de registre. Elle permet de

reconstruire précisément la séquence d'actions de l'attaquant, depuis le point d'entrée initial jusqu'à l'action finale (déploiement ransomware, exfiltration).

Plaso (log2timeline) est l'outil open source de référence pour la construction de super-timelines forensiques. Il analyse des centaines de sources de données différentes (journaux d'événements Windows, artefacts browser, prefetch files, LNK files, registre Windows, logs applicatifs) et produit une timeline unifiée au format CSV ou JSON, filtrable et analysable avec des outils comme **Timesketch** (interface web de visualisation de timelines) ou **Elasticsearch/Kibana**.

```
# Plaso — Génération d'une super-timeline depuis un disque image

log2timeline.py --storage-file dc01.plaso dc01_disk.dd

# Filtrage sur une période spécifique (période incident)

psort.py -o l2tcsv dc01.plaso "date > '2026-03-15 00:00:00' and date <
'2026-03-20 23:59:59'" > dc01_timeline.csv

# Export vers Timesketch pour analyse collaborative

psort.py -o timesketch dc01.plaso --server timesketch.local --timeline
"DC01_Incident_2026"
```

Pendant l'investigation, la super-timeline permet d'identifier le **patient zéro** (premier endpoint/compte compromis), la **chronologie du mouvement latéral** (hop entre systèmes avec les credentials volés), le **moment d'escalade de privilèges** (obtention de Domain Admin), et le **temps de présence de l'attaquant** avant détection (dwell time — en France, la moyenne est de 78 jours selon le rapport ANSSI 2025).

BloodHound : Reconstruction des Chemins d'Attaque Post-Incident

BloodHound (Community Edition, maintenu par SpecterOps) est l'outil de référence pour la cartographie des relations et des chemins d'attaque dans un environnement Active Directory. Conçu initialement par des équipes de pentest offensif, il est devenu indispensable pour les investigateurs défensifs qui doivent comprendre quel chemin d'attaque a été emprunté par l'attaquant.

Dans un contexte forensique post-incident, BloodHound est utilisé en deux temps. **Avant la remédiation** : ingérer les données AD collectées (via SharpHound ou les collecteurs BloodHound CE) dans l'instance BloodHound pour cartographier l'état de l'AD au moment de l'incident. Identifier les chemins d'attaque qui mènent aux actifs compromis (Domain Admins) — ces chemins sont ceux qu'a probablement empruntés l'attaquant. **Après la remédiation** : ré-ingérer les données AD après les corrections et vérifier que les chemins d'attaque critiques identifiés ont été fermés. BloodHound permet de quantifier la réduction de la surface d'attaque AD de manière objective.

Les requêtes BloodHound les plus utiles en investigation forensique : "Shortest Paths to Domain Admins" depuis un compte compromis connu, "Find all Domain Admins" (comptes avec accès effectif Domain Admin direct ou indirect), "Find Kerberoastable Users" (comptes avec SPNs exploitables), et "Find AS-REP Roastable Users" (comptes sans pré-authentification Kerberos). Notre article sur la méthodologie de pentest Active Directory détaille les techniques offensives BloodHound qui correspondent aux chemins d'attaque à rechercher lors d'une investigation.

Détection du DCSync : La Technique d'Extraction Reine

Le DCSync est l'une des techniques d'exfiltration de credentials la plus redoutée dans les environnements AD. Elle permet à un attaquant qui dispose des droits "DS-Replication-Get-Changes" et "DS-Replication-Get-Changes-All" (normalement réservés aux contrôleurs de domaine) de demander à un DC de lui "synchroniser" les hashes des mots de passe de tous les comptes AD — y compris les comptes sensibles comme krbtgt et les comptes administrateurs. Le hash NTLM du compte krbtgt permet de créer des Golden Tickets (tickets Kerberos forgés permanents qui permettent l'accès à n'importe quel service de l'AD).

La détection du DCSync dans les logs Windows repose sur l'Event ID 4662 sur les contrôleurs de domaine. La signature forensique du DCSync : Event ID 4662, Object Type = domainDNS, Access Mask = 0x100, Properties contenant les GUIDs {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} (DS-Replication-Get-Changes) et {1131f6ab-9c07-11d1-f79f-00c04fc2dcd2} (DS-Replication-Get-Changes-All), générés par un compte qui n'est pas un contrôleur de domaine (SubjectUserName != DCNAME$).

```
# Requête PowerShell pour détecter le DCSync dans les logs Security
Get-WinEvent -ComputerName DC01 -FilterHashtable @{
LogName = 'Security'; Id = 4662
} | Where-Object {
$_.Properties[8].Value -match '1131f6aa' -and
$_.Properties[1].Value -notlike '*$'
} | Select TimeCreated, @{N='Account';E={$_.Properties[1].Value}}
```

Kerberoasting et AS-REP Roasting : Détection Forensique

Le Kerberoasting est une technique d'attaque qui cible les comptes de service AD configurés avec des SPNs (Service Principal Names). Un attaquant authentifié dans le domaine peut demander un ticket TGS (Service Ticket) pour n'importe quel SPN sans permissions spéciales. Ce ticket TGS est chiffré avec le hash NTLM du compte de service associé au SPN — hash que l'attaquant peut tenter de cracker offline (sans risque de verrouillage de compte).

La signature forensique du Kerberoasting dans les logs : multiples Event ID 4769 (Kerberos Service Ticket Operations) depuis la même IP/compte, avec Ticket Encryption Type = 0x17 (RC4-HMAC — l'attaquant demande RC4 car plus rapide à cracker que AES256), et des SPNs ciblant des comptes de service avec des mots de passe potentiellement faibles (comptes de service anciens, créés avant les politiques de mots de passe robustes). Une rafale de 4769 RC4 pour des SPNs variés depuis un même compte utilisateur en quelques secondes est quasi-certainement du Kerberoasting.

L'**AS-REP Roasting** cible les comptes configurés avec DONT_REQUIRE_PREAUTH (l'attribut UF_DONT_REQUIRE_PREAUTH dans userAccountControl). Pour ces comptes, le KDC renvoie un AS-REP non chiffré avec une clé dérivée du mot de passe du compte — permettant à un attaquant de demander ces AS-REP sans authentification préalable et de les cracker offline. La détection forensique : Event ID 4768 avec Pre-Authentication Type = 0 (pas de pré-auth) depuis des IPs non-habituelles.

ADCS Abuse : La Nouvelle Frontière de l'Escalade AD

L'Active Directory Certificate Services (ADCS) — l'infrastructure de PKI interne basée sur AD — est devenue en 2022-2026 l'un des vecteurs d'escalade de privilèges AD les plus exploités, depuis la publication des techniques ESC1 à ESC8 par SpecterOps (whitepaper "Certified Pre-Owned"). Ces techniques exploitent des misconfigurés de templates de certificats pour obtenir des certificats permettant l'authentification en tant qu'un compte privilegié.

La technique **ESC1** (la plus fréquente) exploite un template de certificat configuré avec "enrollee can supply subject" ET "client authentication" ET droits d'enrollment pour des utilisateurs non-privilégiés. Elle permet à n'importe quel utilisateur authentifié de demander un certificat au nom de n'importe quel compte (y compris Domain Admin) et de s'authentifier avec ce certificat. La détection forensique dans les logs ADCS : Event ID 4886 (Certificate Services received certificate request) avec un template vulnérable (ESC1), suivi d'Event ID 4768 ou 4776 (authentification Kerberos ou NTLM) avec le compte impersonné. L'investigation ADCS post-incident doit systématiquement auditer les templates de certificats existants avec **Certify** ou **Certipy** pour identifier les templates vulnérables potentiellement exploités.

Shadow Credentials : L'Attaque msDS-KeyCredentialLink

Shadow Credentials est une technique d'attaque récente (popularisée en 2021 par Elad Shamir) qui exploite l'attribut `msDS-KeyCredentialLink` des objets AD pour ajouter une "credential" (clé publique FIDO2) à un compte cible. Si un attaquant dispose de droits WriteProperty sur l'attribut msDS-KeyCredentialLink d'un compte cible (obtenu via une ACL dangereuse), il peut y ajouter sa propre clé publique et s'authentifier ensuite en tant que ce compte via PKINIT Kerberos sans connaître le mot de passe du compte.

La détection forensique des Shadow Credentials : Event ID 5136 (A directory service object was modified) avec AttributeLDAPDisplayName = "msDS-KeyCredentialLink" sur un compte cible, modifié par un compte non-légitime. Cet Event ID 5136 n'est disponible que si l'audit "Directory Service Changes" est activé (recommandé dans toute politique d'audit AD sérieuse). La détection

est facilitée par les outils comme **Microsoft Defender for Identity** (anciennement Azure ATP) qui alerte spécifiquement sur les modifications msDS-KeyCredentialLink suspectes.

Persistances AD : Backdoors que l'Investigateur Doit Chercher

Une fois que l'attaquant a obtenu des privilèges élevés sur l'AD, il cherche à établir une ou plusieurs persistances pour maintenir son accès même si ses credentials initiaux sont détectés et révoqués. L'investigateur forensique doit systématiquement rechercher toutes les formes de persistance AD lors d'une investigation post-incident.

Les formes de persistance AD les plus courantes à investiguer : **Golden Ticket** (basé sur le hash krbtgt — invalidation nécessite de changer le mot de passe krbtgt DEUX fois) ; **comptes backdoor** (comptes administrateurs créés discrètement, parfois masqués dans des OUs peu surveillées, ou comptes de service légitimes auxquels des droits admin ont été ajoutés) ; **AdminSDHolder modifié** (ajout d'ACE à l'objet AdminSDHolder qui se propage automatiquement à tous les comptes protégés via SDProp) ; **GPO malveillantes** (création ou modification de GPO pour déployer des scripts malveillants à l'ensemble ou à un sous-ensemble des machines du domaine) ; **SIDHistory injection** (ajout du SID de Domain Admins dans l'attribut SIDHistory d'un compte standard) ; et **DCShadow** (enregistrement d'un serveur frauduleux comme contrôleur de domaine pour injecter des modifications AD malveillantes qui ne laissent pas de traces dans les logs d'audit normaux).

Velociraptor : Collecte Forensique AD à Grande Échelle

Velociraptor est un outil open source de Digital Forensics and Incident Response (DFIR) qui permet de déployer des agents légers sur des centaines ou milliers d'endpoints et de collecter des artefacts forensiques à grande échelle — en quelques minutes plutôt qu'en plusieurs jours avec des méthodes manuelles. Dans le contexte d'une investigation AD post-incident, Velociraptor est

particulièrement précieux pour la collecte d'artefacts sur un grand parc d'endpoints (workstations + serveurs membres) en complément de la collecte sur les DCs.

Les artefacts Velociraptor les plus utiles pour l'investigation AD : **Windows.EventLogs.EvtxHunter** (recherche d'Event IDs spécifiques sur tous les endpoints), **Windows.Registry.UserAssist** (programmes exécutés par l'utilisateur), **Windows.System.Pslist** (liste des processus), **Windows.Network.NetstatEnriched** (connexions réseau actives), et **Windows.Forensics.NTFS** (artefacts du système de fichiers NTFS : timestamps, fichiers récents). La puissance de Velociraptor est la capacité à pousser des "hunts" (requêtes forensiques) sur l'ensemble du parc en temps réel, permettant de répondre rapidement à des questions comme "sur quels endpoints le binaire mimikatz.exe a-t-il été exécuté ?" ou "quels comptes ont eu des connexions réseau vers l'adresse IP attribuée à l'attaquant ?".

Velociraptor et Microsoft Defender for Identity : Complémentarité

Microsoft Defender for Identity (MDI, anciennement Azure Advanced Threat Protection) est la solution Microsoft native de détection des menaces AD. Déployé avec des capteurs sur tous les DCs, il analyse le trafic réseau AD (Kerberos, NTLM, LDAP, SAMr) et les journaux d'événements en temps réel pour détecter les techniques d'attaque AD (Pass-the-Hash, DCSync, Kerberoasting, Reconnaissance LDAP, modification AdminSDHolder). Dans un contexte forensique, les alertes MDI stockées dans Microsoft Defender XDR constituent une source précieuse d'informations sur les activités suspectes précédant la détection de l'incident.

Les alertes MDI à rechercher systématiquement lors d'une investigation : "Suspected DCSync attack", "Suspected Kerberoasting attack", "Suspected AS-REP Roasting attack", "Account enumeration reconnaissance", "Suspected Golden Ticket usage", et "Suspected identity theft (Pass-the-Hash)". Ces alertes incluent les comptes impliqués, les timestamps, et les DCs concernés — informations directement utilisables pour corréler avec la super-timeline. Notre article sur la configuration de Microsoft Defender for Identity couvre le déploiement des capteurs MDI et les politiques de détection recommandées.

Phase 4 — Analyse des Techniques d'Attaque MITRE ATT&CK

L'étape d'analyse des techniques d'attaque consiste à mapper les événements forensiques collectés aux techniques MITRE ATT&CK Enterprise. Ce mapping permet de structurer le rapport d'investigation, de communiquer clairement avec les parties prenantes (RSSI, COMEX, assureurs cyber, ANSSI), et d'orienter les recherches vers les techniques associées à des groupes d'attaquants spécifiques.

Les techniques MITRE ATT&CK les plus fréquemment observées dans les compromissions AD en 2026 : **T1078 - Valid Accounts** (utilisation de credentials légitimes volés), **T1558.003 - Kerberoasting**, **T1550.002 - Pass-the-Hash**, **T1003.003 - OS Credential Dumping: NTDS** (DCSync, extraction NTDS.dit), **T1484.001 - Domain Policy Modification: Group Policy Object** (création/modification de GPO malveillante), et **T1136.002 - Create Account: Domain Account** (création de comptes backdoor). La plateforme **MITRE ATT&CK Navigator** permet de visualiser les techniques détectées et d'identifier les gaps de détection pour améliorer la posture de sécurité post-incident.

Phase 5 — Rapport d'Investigation : Structure et Contenu

Le rapport d'investigation forensique AD est le livrable final qui synthétise les findings pour les différentes audiences : technique (équipes IT/sécurité), managériale (RSSI, DSI, COMEX), et potentiellement légale (CNIL, ANSSI, assureurs, autorités). Il doit être structuré pour répondre clairement aux questions fondamentales : que s'est-il passé, quand, par qui (si identifiable), avec quel impact, et quelles sont les recommandations.

La structure recommandée d'un rapport forensique AD : **Executive Summary** (1 page, sans jargon technique, pour le COMEX) ; **Chronologie de l'incident** (timeline des événements clés avec timestamps) ; **Techniques d'attaque identifiées** (avec mapping MITRE ATT&CK) ; **Périmètre de la compromission** (systèmes affectés, comptes compromis, données potentiellement exfiltrées) ; **Persistances identifiées et remédiées** ; **Recommandations à court terme** (actions immédiates de remédiation, mesures de durcissement AD prioritaires) ; et

Recommandations à long terme (améliorations architecturales, programme de durcissement AD, amélioration de la détection). Le rapport technique doit inclure les IOCs (Indicators of Compromise) identifiés — hashes, IPs, domaines, comptes — pour permettre une chasse aux menaces sur l'ensemble du périmètre.

Remédiation Post-Incident AD : Checklist des Actions Obligatoires

La remédiation post-incident d'une compromission AD est une opération complexe qui doit être planifiée et exécutée avec soin pour s'assurer qu'aucune backdoor n'est laissée en place. Voici les actions obligatoires à réaliser après une compromission avec obtention de Domain Admin.

Actions immédiates (J+0 à J+2) : changer le mot de passe du compte **krbtgt DEUX fois** (avec un intervalle d'au moins 10h pour laisser les tickets existants expirer — une seule réinitialisation ne suffit pas pour invalider les Golden Tickets) ; révoquer toutes les sessions actives des comptes compromis (Revoke-AzureADUserAllRefreshToken pour les comptes hybrides, désactiver/réactiver les comptes AD) ; identifier et supprimer tous les comptes backdoor créés par l'attaquant ; auditer et supprimer tous les membres non autorisés des groupes sensibles (Domain Admins, Enterprise Admins, Backup Operators) ; et identifier et supprimer les GPO malveillantes créées ou modifiées.

Actions à court terme (J+3 à J+30) : réinitialiser les mots de passe de TOUS les comptes de service avec SPNs (prévention Kerberoasting future) ; remédier toutes les ACL dangereuses identifiées dans BloodHound ; désactiver la délégation Kerberos non contrainte sur tous les serveurs non-DCs ; activer l'audit AD avancé (DS Access, Object Access) si pas encore fait ; déployer Microsoft Defender for Identity sur tous les DCs si absent ; et implémenter un tier model AD (Tier 0/1/2) pour cloisonner les accès administratifs. Notre article sur le guide de durcissement Active Directory 2026 fournit la liste complète des mesures de sécurisation AD post-incident.

Notification ANSSI et CNIL : Obligations Légales Post-Incident

Une compromission AD de grande ampleur peut déclencher des obligations de notification légales. La connaissance de ces obligations est indispensable pour l'investigateur et le RSSI dès le début de l'incident.

La **CNIL** doit être notifiée dans les 72h si la compromission a entraîné une fuite de données personnelles (RGPD article 33). L'AD contient des données personnelles des employés (noms, identifiants, adresses email, appartenance à des groupes) — une compromission AD avec exfiltration de la base NTDS.dit constitue très probablement une violation de données à notifier. L'**ANSSI** doit être informée pour les entités soumises à NIS2 (Entités Essentielles et Importantes) qui subissent un incident significatif (article 23 NIS2). La compromission d'un AD est clairement un incident significatif. L'ANSSI recommande également une notification volontaire même pour les entités non soumises à NIS2, et peut fournir une assistance technique pour la réponse à incident. La notification ANSSI peut se faire via le portail OSIRIS ou via le CERT-FR.

FAQ — Questions sur l'Active Directory Forensics

Combien de temps faut-il pour investiguer une compromission AD ?

Une investigation forensique AD complète prend typiquement 2 à 6 semaines selon la complexité de l'environnement, la disponibilité des artefacts, et l'étendue de la compromission. La phase de collection (1 à 3 jours), la construction de la super-timeline (2 à 5 jours), et l'analyse approfondie (5 à 15 jours) constituent les phases les plus longues. La remédiation complète post-investigation s'étend généralement sur 1 à 3 mois supplémentaires pour les actions à court et long terme.

Peut-on faire confiance à un AD compromis pour la remédiation ?

Non, par définition. Si l'attaquant avait des droits Domain Admin, il peut avoir modifié n'importe quel objet AD, n'importe quelle GPO, n'importe quelle configuration de sécurité. La remédiation doit donc être systématique et exhaustive, pas sélective. Dans les cas de compromission totale avec dwell time long (plusieurs semaines ou mois), la reconstruction from scratch de l'AD (dans un nouveau domaine, avec migration sélective et vérifiée des objets) peut être la seule option réellement sûre — même si c'est une décision très lourde opérationnellement.

Pourquoi changer le mot de passe krbtgt deux fois ?

Le ticket Kerberos Granting Ticket (TGT) a une durée de vie par défaut de 10h dans les environnements Windows. Un Golden Ticket (forgé à partir du hash krbtgt) peut être créé avec une durée de validité arbitrairement longue. Changer le mot de passe krbtgt une première fois invalide les tickets générés avec l'ancien hash. La deuxième réinitialisation (après un délai suffisant) invalide les tickets générés avec le premier nouveau hash — car l'AD stocke le mot de passe krbtgt courant ET l'ancien. Si l'attaquant a extrait les deux versions du hash avant les réinitialisations, le deuxième changement élimine définitivement sa capacité à forger des Golden Tickets.

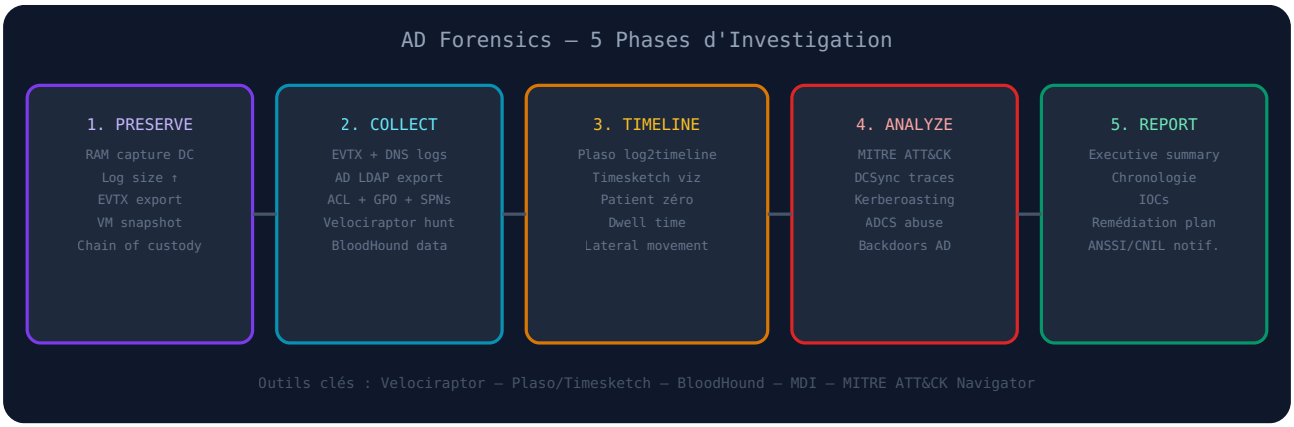
BloodHound peut-il être utilisé sans compromettre la production ?

Oui. Le collecteur SharpHound (exécutable sur un endpoint du domaine) collecte des données via des requêtes LDAP et SMB légitimes, sans modifier l'AD. La collecte peut générer des alertes MDI (sur les requêtes LDAP intensives) mais n'impacte pas la disponibilité de l'AD. En investigation forensique, SharpHound est exécuté avec un compte de service dédié à l'investigation, avec des logs de toutes les actions pour la chaîne de custody. BloodHound Python (via Python depuis une machine Linux) est une alternative plus discrète sur le réseau.

Quelle est la différence entre MDI et les logs natifs Windows pour la détection des attaques AD ?

Les logs Windows natifs (Security Event Log sur les DCs) sont la source de vérité forensique mais leur analyse est manuelle et chronophage. MDI analyse ces mêmes logs (plus le trafic

réseau) en temps réel et corrèle automatiquement les événements pour détecter les patterns d'attaque connus. MDI est donc plus efficace pour la détection proactive, tandis que les logs natifs sont irremplaçables pour l'investigation forensique rétrospective (reconstituer ce qui s'est passé avant que MDI soit déployé, ou analyser des événements que MDI n'a pas alerté).



Les ressources de référence pour l'investigation forensique Active Directory : le guide "Detecting Lateral Movement Through Tracking Event Logs" publié par la JPCERT/CC est disponible sur jpcert.or.jp. La documentation ANSSI sur la réponse à incident cyber est accessible sur ssi.gouv.fr — les deux références indispensables pour les équipes DFIR françaises.

Outils de Chasse aux Menaces AD : Hunt Queries et Sigma Rules

La chasse aux menaces (threat hunting) dans l'AD est une pratique proactive qui complète l'investigation forensique réactive. Plutôt que d'attendre une alerte ou un incident déclaré, le threat hunter cherche activement des indicateurs de compromission dans les logs et les artefacts AD — en supposant que des attaquants sont peut-être déjà présents dans l'environnement sans avoir été détectés.

Les **Sigma Rules** (format YAML de règles de détection multiplateforme) sont devenues le standard pour partager et implémenter des logiques de détection des attaques AD. Le dépôt SigmaHQ sur GitHub contient des centaines de règles Sigma couvrant les techniques ATT&CK AD (DCSync, Kerberoasting, Pass-the-Hash, etc.) convertibles vers les langages de requête des principaux SIEMs (Splunk SPL, Microsoft KQL, Elastic EQL). L'intégration de ces règles Sigma

dans votre SIEM (Microsoft Sentinel, Splunk) est l'une des façons les plus rapides d'améliorer la détection des attaques AD sans développer des règles de détection from scratch. Notre article sur le déploiement des règles de détection Microsoft Sentinel couvre l'intégration des Sigma Rules et les analytiques AD spécifiques à configurer pour la détection des attaques les plus fréquentes.

Les hunt queries KQL (Kusto Query Language) pour Microsoft Sentinel les plus utiles en contexte AD forensique : recherche de DCSync (Event ID 4662 avec les GUIDs de réplication), détection de Kerberoasting (4769 RC4 en rafale depuis un même compte), identification de comptes de service avec mots de passe expirés depuis plus de 6 mois (risque Kerberoasting), et détection d'ajouts dans les groupes sensibles hors des fenêtres de maintenance habituelles. Ces queries peuvent être sauvegardées comme "Hunting queries" dans Sentinel et exécutées régulièrement par les analystes SOC.

Forensique des Journaux PowerShell : Détection des Attaques Script-Based

PowerShell est l'outil de prédilection des attaquants pour les opérations post-exploitation dans les environnements Windows — c'est pourquoi le logging PowerShell est critique pour l'investigation forensique AD. Sans logging PowerShell activé, de nombreuses activités offensives (reconnaissance LDAP avec PowerView, dump credentials avec Invoke-Mimikatz, mouvement latéral avec Invoke-SMBExec) sont invisibles dans les logs Windows natifs.

Les trois niveaux de logging PowerShell à activer via GPO : **Module Logging** (Event ID 4103 — enregistre les paramètres des commandes PowerShell exécutées), **Script Block Logging** (Event ID 4104 — enregistre le contenu des scripts PowerShell, y compris les scripts obfusqués décodés), et **PowerShell Transcription** (enregistre l'intégralité de la session PowerShell dans un fichier texte). Script Block Logging est le plus précieux pour la forensique : il enregistre le code PowerShell réellement exécuté, permettant de voir les commandes de reconnaissance LDAP (`Get-ADUser -Filter *`, `Get-ADGroup`), les tentatives de dump de credentials (`Invoke-Mimikatz`, `Invoke-DCSync`), et les mouvements latéraux via PowerShell Remoting (`Enter-PSSession`, `Invoke-Command -ComputerName`). L'analyse des logs Script Block lors d'une investigation forensique AD révèle souvent le script exact utilisé par l'attaquant, permettant d'identifier les

outils (Empire, Cobalt Strike, MITRE ATT&CK framework), les chemins d'attaque précis, et parfois des éléments d'attribution.

Anecdote Terrain : Le Golden Ticket Oublié

En 2024, lors d'une investigation post-ransomware pour une société de services française de 300 employés, nous avons découvert lors de l'analyse que l'organisation avait déjà subi une compromission AD 8 mois auparavant — non détectée à l'époque. Les indices : Event ID 4768 (demande de TGT) pour un compte inexistant dans l'AD (le compte avait été supprimé 6 mois avant l'incident), et des connexions réseau vers un serveur de commande-et-contrôle depuis le DC principal qui correspondent exactement à la période du premier incident non détecté.

L'attaquant avait extrait le hash krbtgt lors de la première compromission, créé un Golden Ticket, et maintenu un accès silencieux pendant 8 mois avant de déployer le ransomware. Le dwell time de 8 mois a permis une reconnaissance extensive : exfiltration lente et progressive des données critiques, compréhension complète de l'architecture et des sauvegardes avant l'attaque finale. La leçon : une investigation forensique post-ransomware doit systématiquement remonter très en arrière dans les logs (au minimum 12 mois) pour identifier le vecteur d'entrée initial, qui précède toujours de beaucoup le déploiement du ransomware final.

Audit de la Configuration ADCS : Détecter les Templates Vulnérables

L'Active Directory Certificate Services (ADCS), lorsqu'il est déployé, constitue une surface d'attaque significative souvent méconnue des équipes de sécurité. L'audit de la configuration ADCS est devenu une étape obligatoire de tout investigation forensique AD post-compromission, depuis la publication des techniques ESC1-ESC8 par Will Schroeder et Lee Christoffersen en 2021.

L'outil de référence pour auditer une configuration ADCS en investigation forensique est **Certipy** (Python, compatible Linux) développé par Oliver Lyak. Il peut être exécuté depuis une machine Linux avec des credentials valides pour interroger l'ADCS via LDAP et identifier les templates vulnérables. La commande de base :

```
# Certipy — Audit des templates ADCS depuis Linux
certipy find -u investigator@domain.fr -p 'Password123!' -dc-ip 192.168.1.10
-vulnerable -stdout
# Certify (C#) — Depuis un Windows dans le domaine
Certify.exe find /vulnerable
```

Les templates vulnérables identifiés (ESC1 à ESC8) doivent être documentés dans le rapport forensique même s'ils n'ont pas été activement exploités durant l'incident — leur présence représente un risque persistant qui doit être remédie dans le plan post-incident. La remédiation des templates ADCS vulnérables passe par la restriction des droits d'enrollment (retirer l'enrollment pour Authenticated Users sur les templates sensibles), la désactivation du flag ENROLLEE_SUPPLIES_SUBJECT sur les templates avec client authentication, et la configuration du Manager Approval pour les templates sensibles.

Tier Model AD : Cloisonnement pour Limiter le Blast Radius

L'une des recommandations post-incident AD les plus importantes pour prévenir la réoccurrence est l'implémentation du **Tier Model** (modèle à niveaux) — une architecture de sécurité qui cloisonne les accès administratifs pour limiter la propagation d'une compromission. Le Tier Model est recommandé par Microsoft et l'ANSSI comme protection contre les mouvements latéraux et l'escalade de privilèges AD.

Le Tier Model comprend trois niveaux : **Tier 0** — les actifs les plus critiques (contrôleurs de domaine, ADFS, ADCS, systèmes de gestion de l'identité). Seuls des comptes Tier 0 dédiés peuvent administrer ces systèmes. Les administrateurs Tier 0 utilisent des postes d'administration dédiés (PAW — Privileged Access Workstations) isolés du réseau utilisateur. **Tier 1** — les serveurs d'infrastructure (serveurs applicatifs, databases, hyperviseurs). Des comptes Tier 1

dédiés, différents des comptes Tier 0, administrent ces systèmes. **Tier 2** — les endpoints utilisateurs (workstations, laptops). Des comptes Tier 2 dédiés (helpdesk, admins locaux) gèrent ces postes. La règle fondamentale : un compte d'un niveau inférieur ne peut jamais s'authentifier sur un système d'un niveau supérieur (un compte Tier 1 ne peut pas se connecter sur un DC Tier 0), empêchant la propagation d'une compromission du niveau inférieur vers le supérieur. Le Tier Model est une transformation architecturale significative mais c'est l'une des mesures les plus efficaces pour réduire durablement la surface d'attaque AD post-incident. Microsoft et l'ANSSI recommandent tous deux son implémentation comme priorité dans tout plan de remédiation post-compromission AD. La mise en place se fait progressivement — commencer par le Tier 0 (protéger les DCs en priorité) avant d'étendre aux Tiers 1 et 2.

Détection des Comptes de Service Compromis : Analyse des Patterns d'Authentification

Les comptes de service AD sont des cibles privilégiées des attaquants pour plusieurs raisons : ils ont souvent des mots de passe anciens (créés avant les politiques de rotation), des SPNs kerberoastables, des droits étendus nécessaires à leurs fonctions, et sont rarement surveillés aussi attentivement que les comptes utilisateurs humains. Un compte de service compromis peut maintenir une présence discrète dans le SI pendant des mois.

La détection des comptes de service compromis en forensique : analyser les patterns d'authentification habituels des comptes de service (horaires, sources IP, services cibles) et identifier les anomalies (connexions hors des horaires habituels, depuis des IPs inhabituelles, vers des services non habituellement ciblés). Les Event IDs 4624 (logon) et 4648 (explicit credentials) filtres sur les comptes de service permettent de reconstruire leur activité historique. Une connexion d'un compte de service de sauvegarde (typiquement actif la nuit) vers un serveur qu'il ne touche jamais normalement, à 14h un mardi, est un signal forensique fort de compromission de ce compte.

Indicateurs de Compromission AD : IOC List à Partager

À l'issue d'une investigation forensique AD, la production d'une liste d'IOC (Indicators of Compromise) est indispensable pour permettre à l'organisation de chasser ces indicateurs sur l'ensemble de son périmètre, et éventuellement de les partager via des plateformes de CTI (MISP, OpenCTI) avec d'autres organisations du même secteur.

Les IOC d'une compromission AD typique incluent : les **hash MD5/SHA256** des outils offensifs identifiés (mimikatz.exe, SharpHound.exe, Cobalt Strike beacon), les **adresses IP C2** (serveurs de commande-et-contrôle avec lesquels le DC ou les endpoints ont communiqué), les **noms de domaines C2**, les **clés de registre** de persistance créées par l'attaquant, les **noms des comptes backdoor** créés, les **noms des GPO malveillantes** créées ou modifiées, et les **SIDs des comptes compromis** qui ont eu des droits Domain Admin. Ces IOC doivent être intégrés dans le SIEM et dans les outils EDR pour bloquer toute réutilisation de ces indicateurs dans une éventuelle réattaque.

Coût d'une Investigation AD Forensique et Prestataires PRIS

Le coût d'une investigation forensique AD dépend de la taille de l'environnement, de la complexité de la compromission, et du niveau d'expertise du prestataire. Pour une ETI de 200 à 500 employés, une investigation forensique AD complète (de la collection au rapport final) représente typiquement entre 15 000 et 60 000 euros selon la durée de l'investigation et les déplacements nécessaires.

En France, les prestataires PRIS (Prestataires de Réponse à Incidents de Sécurité) qualifiés par l'ANSSI offrent des garanties de compétence et d'indépendance. La qualification PRIS couvre la réponse à incident (investigation forensique, containment, remédiation) et inclut une obligation d'assurance RC. La liste des prestataires PRIS qualifiés ANSSI est disponible sur le site de l'ANSSI. Faire appel à un prestataire PRIS qualifié est fortement recommandé pour les incidents impliquant des données sensibles ou nécessitant une notification ANSSI/CNIL — la qualification

ANSSI est un gage de qualité et facilite les échanges avec l'ANSSI dans le cadre de la gestion de crise.

Les assureurs cyber imposent de plus en plus de travailler avec des prestataires PRIS qualifiés pour que la couverture de la police cyber s'applique à la prise en charge des coûts d'investigation. Vérifier votre police d'assurance cyber avant un incident pour connaître les prestataires préapprouvés et les procédures de déclenchement — évitez de découvrir ces contraintes en plein cœur d'un incident où chaque heure compte. Le coût d'une investigation AD forensique est généralement couvert par l'assurance cyber (dans les polices avec une couverture "incident response"), ce qui justifie d'autant plus de souscrire à une assurance cyber avec cette garantie. Les grandes organisations (ETI et GE) peuvent avoir des contrats RETAINER avec des prestataires PRIS — accès prioritaire à des équipes DFIR en cas d'incident, avec des SLA de réponse garantis (4h pour démarrage d'investigation, 24h pour présence on-site). Ces contrats RETAINER sont plus avantageux qu'un engagement d'urgence à la volée lors d'un incident, tant en termes de délai de réponse que de tarif.

Quel que soit le prestataire choisi, la préparation interne est indispensable : un plan de réponse à incident documenté (IR Playbook pour compromission AD), des contacts préétablis avec le prestataire PRIS et l'ANSSI/CERT-FR, et un exercice de tabletop annuel simulant une compromission AD permettent de réduire considérablement le temps de réponse et la confusion lors d'un incident réel. La préparation fait la différence entre une organisation qui maîtrise sa crise et une organisation que la crise maîtrise.