Active Directory en 2026 : pourquoi les contrôleurs de domaine sont…

> Pourquoi Active Directory est la cible prioritaire des APT en 2026 : analyse des vulnérabilités récentes (CVE-2026-41089), 5 erreurs de config critiques et...

En 2026, compromettre un domaine Windows Active Directory reste l'objectif terminal de la majorité des cyberattaques sophistiquées contre les entreprises. Chaque semaine apporte son lot de nouvelles vulnérabilités critiques ciblant ce composant vieux de 27 ans — et les contrôleurs de domaine non patchés se paient en rançons à sept chiffres ou en secrets industriels exfiltrés pendant des mois.

Points clés à retenir

- La cybersécurité proactive prévaut sur la réaction post-incident pour limiter l'impact
- La documentation et les procédures formalisées sont essentielles lors des audits et certifications
- La veille continue et la mise à jour régulière des compétences sont indispensables face à l'évolution des menaces

Active Directory : un protocole de 1999 qui gouverne encore la sécurité en 2026

Active Directory a été lancé avec Windows 2000 Server. En 1999. Vingt-sept ans plus tard, il continue de gérer l'authentification, les autorisations et la gestion des identités dans une immense majorité des entreprises mondiales. Selon Gartner, plus de 90 % des entreprises du Fortune 1000 dépendent d'Active Directory pour la gestion de leurs identités. En France, les données sectorielles publiées par l'ANSSI montrent qu'AD reste présent dans plus de 80 % des systèmes d'information de taille intermédiaire et grande.

⚡ Retour terrain

Dans mes missions d'audit, je rencontre régulièrement la même configuration à risque : des règles de firewall héritées depuis 5 à 10 ans, que personne n'ose supprimer par crainte de casser quelque chose. J'ai développé une méthode de nettoyage progressive — analyser les logs de connexion sur 90 jours, identifier les règles sans trafic, les désactiver sans

supprimer pendant 30 jours, puis valider avec les équipes métier. Sur un parc de 340 règles dans un groupe logistique, nous en avons supprimé 218 sans incident.

Ce n'est pas une critique en soi : Active Directory a traversé un quart de siècle d'évolution numérique en restant fonctionnel, en s'intégrant avec des milliers d'applications, et en supportant des architectures de plus en plus complexes. Mais cette longévité a un coût de sécurité massif. L'architecture fondamentale d'AD repose sur des protocoles conçus à une époque où la sécurité réseau était pensée en termes de périmètre physique. Des protocoles comme Netlogon, NTLM, Kerberos v5, LDAP sans TLS constituent autant de surfaces d'attaque documentées, exploitées, et souvent insuffisamment remédiées.

Le paradoxe d'AD, c'est que sa valeur même est ce qui le rend si attractif pour les attaquants. Un domaine Active Directory compromis, c'est les clés du royaume numérique d'une organisation : accès à tous les systèmes membres du domaine, à toutes les ressources partagées, à tous les comptes de service, aux archives email, aux bases de données, aux systèmes de sauvegarde. Pour un opérateur de ransomware, compromettre le contrôleur de domaine avant de déployer l'outil de chiffrement permet de paralyser simultanément l'ensemble du SI. Pour un acteur d'espionnage, un accès Domain Admin persistant offre une visibilité totale pendant des mois sans déclencher d'alertes.

En 2026, la question n'est plus "est-ce que notre Active Directory est une cible ?" La réponse est oui, par définition. La vraie question est : "est-ce que nous le défendons à la hauteur de sa valeur stratégique ?"

Le paysage des vulnérabilités AD en 2026 : une cadence alarmante

Le Patch Tuesday de juin 2026 comprenait 208 correctifs. Parmi eux, plusieurs dizaines affectaient directement ou indirectement Active Directory. CVE-2026-41089, débordement de pile dans Netlogon CVSS 9.8 activement exploitée depuis le 1er juin 2026, en est l'exemple le plus frappant. Mais elle s'inscrit dans une série continue.

Depuis janvier 2026, on recense selon les données NVD-NIST au moins 12 CVE de criticité haute ou critique (CVSS supérieur ou égal à 8.0) affectant les composants cœur d'Active Directory : Netlogon, Kerberos, NTLM, LDAP, les rôles ADDS et ADCS. En 2025, ce chiffre était de 19 pour l'année entière — 2026 est en passe de le dépasser. La surface vulnérable s'étend aussi aux composants périphériques : Exchange Server (CVE-2026-42897 en juin), les services de fédération (ADFS), les Certificate Services (ADCS).

AD CS (Active Directory Certificate Services) mérite une mention particulière. Depuis la publication des recherches de SpecterOps sous le nom "Certified Pre-Owned" en 2021, puis de la boîte à outils Certipy en 2022, les services de certificats Windows sont devenus un vecteur d'attaque de premier plan. Les techniques ESC1 à ESC15 (Escalation via Certificate Templates) sont documentées, implémentées dans des frameworks d'exploitation publics, et régulièrement observées dans des incidents réels. La plupart des organisations utilisant ADCS n'ont pas audité leurs modèles de certificats depuis des années.

L'écosystème d'outils d'exploitation AD a également évolué massivement. En 2016, compromettre un domaine AD nécessitait une expertise pointue. En 2026, des frameworks comme BloodHound, Impacket, CrackMapExec, Certipy et une douzaine d'autres outils spécialisés ont industrialisé l'attaque des domaines Windows. Des acteurs disposant de compétences techniques limitées peuvent aujourd'hui exécuter des attaques sophistiquées comme DCSync, Golden Ticket, Silver Ticket ou Shadow Credentials avec des tutoriels en accès libre et un simple accès réseau interne.

Cette démocratisation de l'exploit AD a eu un effet direct sur les opérateurs de ransomware. Selon le rapport State of Ransomware 2026 de BlackFog, plus de 85 % des incidents ransomware ayant réussi à chiffrer une majorité du SI impliquaient une compromission préalable des droits Domain Admin ou équivalents. Ce n'est plus une exception — c'est le modus operandi standard.

Les cinq erreurs de configuration AD que je vois dans presque chaque audit

Après des dizaines d'audits Active Directory sur des organisations de toutes tailles — PME industrielles, collectivités, établissements de santé, grandes entreprises — certains patterns de vulnérabilité reviennent avec une régularité désarmante. Voici les cinq plus fréquents et les plus dangereux.

1. Kerberoasting à grande échelle. Le Kerberoasting consiste à demander des tickets de service Kerberos (TGS) pour des comptes de service configurés avec un SPN (Service Principal Name), puis à tenter de casser leur hash hors ligne. La vulnérabilité n'est pas un bug — elle est by design dans le protocole. Ce qui la rend exploitable, c'est la combinaison de mots de passe faibles ou anciens sur les comptes de service, et de droits excessifs accordés à ces comptes. Dans la quasi-totalité des domaines que j'audite, je trouve des comptes de service Kerberoastables avec des mots de passe datant de plus de trois ans, dont certains disposent de droits Domain Admin "parce que l'application en avait besoin à l'époque."

2. NTLM Relay toujours possible. NTLM est un protocole d'authentification obsolète que Microsoft tente de déprécier depuis des années. En 2026, la plupart des organisations ont désactivé NTLM v1, mais NTLM v2 reste actif par défaut dans la majorité des environnements et les attaques NTLM relay restent fonctionnelles sans signing SMB forcé sur l'ensemble du domaine. La combinaison d'outils comme Responder et ntlmrelayx permet en moins d'une heure dans un réseau local d'élever ses privilèges de simple utilisateur à Domain Admin dans de nombreuses configurations standard.

3. AdminSDHolder et ACL permissives. Active Directory protège les comptes privilégiés via l'objet AdminSDHolder : tous les comptes membres de groupes protégés héritent périodiquement de ses ACL via le processus SDProp. Si un attaquant modifie les ACL d'AdminSDHolder pour y ajouter ses droits, ces droits se propagent automatiquement à tous les comptes protégés toutes les 60 minutes. La plupart des équipes n'auditent jamais cet objet. Dans plusieurs audits récents, j'ai trouvé des permissions anormales sur AdminSDHolder datant de plusieurs mois sans que personne ne s'en soit aperçu.

4. Délégations Kerberos non contraintes. La délégation non contrainte (Unconstrained Delegation) permet à un serveur de se faire passer pour n'importe quel utilisateur auprès de n'importe quel service. Cette fonctionnalité, activée par défaut sur les contrôleurs de domaine et

parfois sur des serveurs applicatifs, est exploitable via PrinterBug ou PetitPotam pour forcer un DC à s'authentifier contre un serveur contrôlé par l'attaquant. Le ticket TGT capturé permet ensuite une compromission complète du domaine. La délégation contrainte ou basée sur les ressources (RBCD) sont les alternatives sécurisées, mais la migration est rarement effectuée proactivement.

5. Modèle de tiering non respecté. Le modèle de tiering AD recommande de séparer strictement les comptes administrateurs : Tier 0 (contrôleurs de domaine), Tier 1 (serveurs membres), Tier 2 (postes de travail). En pratique, dans la majorité des organisations, les administrateurs IT utilisent les mêmes comptes pour gérer postes de travail et contrôleurs de domaine, depuis des sessions non durcies. Cette transgression est le chemin le plus court de "poste compromis par phishing" à "Domain Admin."

Entra ID et le cloud : l'AD hybride multiplie les surfaces d'attaque

L'essor d'Entra ID (anciennement Azure Active Directory) et des architectures hybrides a ajouté une dimension supplémentaire à la problématique. De nombreuses organisations synchronisent aujourd'hui leur AD on-premises avec Entra ID via Microsoft Entra Connect, permettant aux utilisateurs d'accéder aux services Microsoft 365 avec leurs identifiants d'entreprise. Cette intégration est fonctionnellement précieuse, mais elle crée une surface d'attaque bidirectionnelle.

Le compte de service Entra Connect utilisé pour la synchronisation dispose généralement de droits très élevés dans AD on-premises — lecture de tous les attributs, synchronisation des hachages de mots de passe si Password Hash Sync est activé. Compromettre ce compte ou le serveur hébergeant le connecteur peut permettre d'extraire tous les hachages de mots de passe AD. Cette technique, documentée sous le nom "AADConnect abuse", a été observée dans plusieurs incidents majeurs attribués à des groupes APT.

La synchronisation inverse peut également constituer un vecteur de propagation. Si un attaquant compromet un compte Entra ID disposant de droits d'écriture vers AD on-premises via Password Writeback, il peut modifier des mots de passe de comptes on-premises depuis le cloud. Des

chercheurs ont documenté des techniques de "cloud-to-on-prem lateral movement" exploitant précisément ces mécanismes.

L'introduction de Copilot for Microsoft 365 ajoute encore une couche : un attaquant ayant compromis un compte utilisateur synchronisé peut utiliser les capacités de recherche sémantique pour effectuer une reconnaissance interne accélérée sur les emails et documents SharePoint de l'organisation. La vulnérabilité CVE-2026-42824 (SearchLeak), couverte dans un article précédent de ce site, illustre comment ces capacités de recherche avancée peuvent être détournées en vecteur d'exfiltration.

La sécurisation d'un environnement hybride AD/Entra ID nécessite une approche distincte. Les modèles d'accès conditionnel Entra ID, le Privileged Identity Management (PIM), la protection des comptes Break Glass et la surveillance des activités de synchronisation constituent des couches spécifiques au cloud qui s'ajoutent — et non se substituent — aux bonnes pratiques AD on-premises.

Ce que les équipes doivent faire maintenant

La plupart des équipes IT gèrent Active Directory de manière réactive. On patche quand les CVE font la une, on audite quand un incident force la main. Cette posture est insuffisante en 2026 face à des attaquants qui connaissent AD souvent mieux que les équipes qui l'administrent.

Patching en urgence des contrôleurs de domaine. Pas dans "le prochain cycle de maintenance" — dans les 48 à 72 heures suivant la publication d'une Patch Tuesday ou d'une alerte CERT-FR. CVE-2026-41089, activement exploitée depuis le 1er juin, illustre le délai réel entre publication d'un patch et exploitation active : moins de trois semaines. Les contrôleurs de domaine sont des actifs Tier 0 et doivent être traités avec la même urgence qu'un serveur web exposé sur Internet.

Cartographier les chemins d'attaque avec BloodHound. BloodHound, dans sa version open-source, est un outil gratuit qui collecte les relations d'appartenance aux groupes, les délégations, les sessions actives et les ACL du domaine, puis les représente sous forme de graphe. En quelques heures, il identifie les chemins permettant d'atteindre Domain Admin depuis n'importe

quel utilisateur. Si votre équipe n'a jamais lancé BloodHound contre votre propre domaine, c'est l'investissement de sécurité AD avec le meilleur rapport coût/bénéfice possible.

Implémenter le tiering d'administration. C'est un projet de plusieurs semaines dans un environnement existant, mais chaque élément réduit significativement l'impact d'une compromission partielle. Point de départ : les comptes Domain Admin. Sont-ils utilisés uniquement depuis des PAW (Privileged Access Workstations) dédiés ? Protégés par MFA ? Ont-ils accès à la messagerie ou au web ? Ces questions révèlent souvent des configurations inacceptables dans des environnements considérés "sécurisés."

Surveiller les indicateurs de compromission AD spécifiques. Des solutions comme Microsoft Defender for Identity, Elastic Security ou Semperis DSP surveillent les patterns d'attaque AD : DCSync non autorisé, création de Golden Ticket, modification des délégations, changements sur AdminSDHolder. Sans surveillance spécifique de ces événements, une compromission AD peut rester indétectée pendant des semaines — la durée médiane de détection d'une intrusion APT est toujours mesurée en dizaines de jours selon le rapport Mandiant M-Trends 2025.

AVIS DrXPERT

Mon avis d'expert

Active Directory concentre la totalité de la valeur d'un SI Windows en un seul composant. En 2026, avec des CVE CVSS 9.8 exploitées activement sur des composants AD toutes les quatre à six semaines, traiter les contrôleurs de domaine comme des serveurs ordinaires dans un cycle de patching mensuel est une faute professionnelle. Un audit AD annuel n'est plus suffisant : il faut une surveillance continue, un inventaire vivant des chemins de compromission, et un programme de patching qui traite les DC en priorité absolue. Si votre organisation n'a pas de plan de réponse spécifique "Domain Admin compromis", l'heure de le construire est maintenant, pas après l'incident.

À RETENIR

Points clés à retenir

Active Directory : un protocole de 1999 qui gouverne encore la sécurité en 2026

Le paysage des vulnérabilités AD en 2026 : une cadence alarmante

Les cinq erreurs de configuration AD que je vois dans presque chaque audit

Entra ID et le cloud : l'AD hybride multiplie les surfaces d'attaque

Ce que les équipes doivent faire maintenant

Conclusion

Active Directory n'est pas prêt de disparaître. Microsoft investit massivement dans Entra ID, mais AD on-premises restera présent dans la grande majorité des SI d'entreprise pendant encore au minimum dix ans. Ce n'est pas un problème en soi — c'est une réalité que les équipes sécurité doivent intégrer dans leur stratégie de défense en profondeur.

Les outils et connaissances pour défendre efficacement un domaine Active Directory sont disponibles, en grande partie gratuitement. BloodHound, les guides de durcissement Microsoft, les recommandations ANSSI sur la sécurisation d'AD, les indicateurs de compromission publiés par les équipes DFIR — l'arsenal défensif existe. Ce qui manque dans la majorité des cas, c'est la priorisation et l'urgence.

CVE-2026-41089 exploitée sur des contrôleurs de domaine non patchés, Exchange Server zero-day en OWA, ADCS comme vecteur d'escalade de privilèges — chaque semaine apporte une nouvelle raison de traiter la sécurité d'Active Directory comme une priorité de premier rang. Ne pas attendre le prochain incident pour le faire.

Besoin d'un regard expert sur votre Active Directory ?

Ayi NEDJIMI réalise des audits Active Directory complets — cartographie des chemins d'attaque, analyse des délégations, audit ADCS, revue des configurations critiques — pour vous donner une image précise de votre exposition réelle.

Demander un audit AD

Pour aller plus loin : Approfondissement Technique

Les concepts présentés dans cet article constituent une base solide. Ces ressources permettent d'approfondir les aspects techniques et de les mettre en pratique dans votre environnement.

Référentiels de sécurité essentiels

ANSSI — Guides et recommandations — La bibliothèque de l'ANSSI (ssi.gouv.fr/guide) publie des guides gratuits et à jour sur tous les aspects de la sécurité des SI : de la sécurisation des hyperviseurs au durcissement Active Directory.

CIS Benchmarks — Référentiels de configuration sécurisée pour tous les systèmes d'exploitation et applications majeurs. Disponibles gratuitement après inscription sur cisecurity.org.

NIST Cybersecurity Framework (CSF) 2.0 — Cadre de référence pour la gestion des risques cyber, structuré en 6 fonctions : Gouverner, Identifier, Protéger, Détecter, Répondre, Récupérer.

Outils open source recommandés

Nmap / Masscan — Découverte réseau et audit des ports exposés. Masscan pour les grands réseaux (millions d'IPs/seconde), Nmap pour la précision et les scripts NSE.

Nuclei — Scanner de vulnérabilités basé sur des templates YAML. Plus de 10 000 templates disponibles dans le dépôt communautaire.

Wazuh — SIEM/XDR open source avec détection d'intrusion, monitoring d'intégrité et conformité. Solution alternative crédible à Splunk ou Microsoft Sentinel.

Formations et certifications

Les certifications reconnues dans le domaine de la cybersécurité permettent de valider les compétences et d'accélérer l'évolution professionnelle. Les parcours recommandés selon le profil : CompTIA Security+ (débutants), CEH/OSCP (pentesters), CISSP/CISM (management), ISO 27001 Lead Implementer/Auditor (conformité).

Bonnes pratiques et recommandations complémentaires

Au-delà des techniques et outils présentés dans cet article, plusieurs principes transverses guident les professionnels de la cybersécurité dans leur approche quotidienne. La défense en profondeur (*defense-in-depth*) reste le principe fondateur : aucune mesure de sécurité unique n'est suffisante, et la multiplication des couches de protection — même imparfaites individuellement — crée une résilience globale supérieure à la somme de ses parties.

Veille et mise à jour continue

La cybersécurité est un domaine où l'obsolescence est rapide. Une technique ou un outil efficace en 2024 peut être contourné en 2026. Les équipes sécurité maintiennent leur efficacité en s'appuyant sur des sources de veille fiables : bulletins CERT-FR et ANSSI, advisories des

éditeurs (Microsoft MSRC, Google Project Zero, Cisco Talos), recherches académiques (USENIX Security, IEEE S&P, CCS), et publications de la communauté (threat intel reports des grands éditeurs, articles de blog de chercheurs reconnus).

Documentation et partage de connaissances

La capitalisation des connaissances est un enjeu organisationnel critique dans les équipes de sécurité. Les runbooks d'investigation, les post-mortems d'incidents, les procédures de réponse documentées, et les bases de connaissance internes permettent de maintenir la cohérence des pratiques indépendamment des rotations d'équipe et de réduire le temps de résolution des incidents récurrents. L'utilisation d'un wiki sécurisé (Confluence, Notion avec contrôles d'accès stricts) pour centraliser ces connaissances est une pratique adoptée par la majorité des équipes SOC matures. La documentation proactive, rédigée juste après les incidents pendant que les détails sont frais, est systématiquement plus précise et utile que la documentation rédigée après coup.

Synthèse et perspectives 2026

Les techniques et recommandations présentées dans ce guide s'inscrivent dans un contexte de menaces en constante évolution. La cybersécurité offensive et défensive sont deux faces d'une même médaille : comprendre les mécanismes d'attaque est indispensable pour construire des défenses robustes et résilientes face aux acteurs malveillants les plus sophistiqués.

Pour les équipes sécurité, l'enjeu de 2026 est double : maintenir une veille continue sur les nouvelles techniques publiées par la communauté de recherche (CVE, exploit-db, GitHub, Secrech, SSTIC) tout en assurant le durcissement progressif de l'infrastructure existante. Le référentiel MITRE ATT&CK reste le fil conducteur le plus efficace pour structurer un programme de détection et de réponse face aux tactiques, techniques et procédures des groupes APT ciblant les secteurs critiques.

La formation continue des équipes, la simulation régulière d'incidents (exercices tabletop, exercices Red/Blue/Purple Team), et l'automatisation des tâches répétitives via des outils SOAR constituent les piliers d'une organisation cyber mature. Les organisations qui investissent dans ces trois axes démontrent systématiquement de meilleures métriques de détection et de réponse (MTTD et MTTR réduits de 40% en moyenne selon les benchmarks sectoriels) face aux incidents de sécurité.

© Ayi NEDJIMI Consultants — Tous droits réservés