VEILLE TECHNOLOGIQUE • SÉCURISATION D'ACTIVE DIRECTORY — FICHE 1

Les six menaces majeures qui ciblent Active Directory

Date de la veille : 27 février 2026

Pour cette veille, je me suis intéressé au guide publié par Microsoft en décembre 2025 recensant les six attaques principales contre Active Directory, croisé avec le *Sophos Active Adversary Report 2026*. Le constat est sans appel : en médiane, un attaquant met seulement **3,4 heures** après son intrusion pour atteindre l'AD, et **67 %** des incidents démarrent par une compromission d'identité (identifiants volés ou phishing).

Ce que je retiens de ces analyses, c'est que ces menaces (relais NTLM, Kerberoasting, délégation sans contrainte, Golden Ticket) détournent des mécanismes légitimes, ce qui les rend invisibles pendant près de 3 jours en moyenne. Heureusement, les contre-mesures se recoupent : migrer les comptes de service vers des **gMSA**, activer la signature SMB et le LDAP channel binding, et renouveler régulièrement le mot de passe du compte `krbtgt` permettent de bloquer plusieurs maillons de la chaîne en même temps.

D'un point de vue administration, cela confirme que la sécurité d'un domaine ne repose plus uniquement sur un antivirus, mais sur le durcissement natif de l'annuaire et le principe du moindre privilège.

SOURCES

- Microsoft — *Guidance to help mitigate critical threats to Active Directory Domain Services* (9 déc. 2025)
- Help Net Security — *Sophos Active Adversary Report 2026* (27 fév. 2026)