VEILLE TECHNOLOGIQUE • SÉCURISATION D'ACTIVE DIRECTORY — FICHE 6

Surveillance et détection : repérer les attaques Active Directory avant l'impact

Date de la veille : 12 novembre 2026 • Mise à jour : 27 novembre 2026

Dans la continuité des veilles précédentes, j'ai étudié comment détecter rapidement une compromission sur Active Directory à travers les guides du CERT-FR et la documentation de *Microsoft Defender for Identity*. Comme un attaquant met en moyenne quelques heures à atteindre l'annuaire en utilisant des outils légitimes, la prévention seule ne suffit plus : il faut une supervision capable d'alerter dès les premiers signes suspects.

L'enjeu principal consiste à collecter les bons journaux d'événements Windows (création de comptes privilégiés, modification de GPO avec les ID 5136 à 5141, demandes de tickets Kerberos anormales) et à les corréler via un SIEM ou une sonde dédiée comme **Defender for Identity**. Ces outils analysent les comportements directement sur les contrôleurs de domaine pour repérer en temps réel un *Kerberoasting*, une tentative de *DCSync* ou un mouvement latéral inhabituel.

Côté administration, mettre en place cette supervision permet de réduire drastiquement le temps de détection et d'isoler un compte compromis avant que l'attaquant ne déploie un ransomware sur tout le parc.

ACTUALITÉS 2026

- **Guide ACSC / CISA (sept. 2026) :** mise à jour sur 18 techniques de compromission AD, avec une nouvelle méthode de détection du **DCSync** et une section sur les **shadow credentials**.
- **Defender for Identity :** migration vers le capteur v3.x sans interruption (mars), réponse automatisée aux menaces d'identité annoncée à RSA 2026 (20 mars), page « Coverage and maturity » (juin, préversion).
- **Attaque réelle (mars 2026) :** sur un incident de ransomware Interlock, l'attaquant a interrogé les groupes puis les SPN de l'AD, signe d'un **Kerberoasting**. Sophos indique aussi une première tentative contre l'AD en moyenne 11 h après l'intrusion.
- **Vulnérabilité Certighost (juil. 2026) :** faille d'AD CS (CVE-2026-54121) permettant à un simple utilisateur du domaine de prendre le contrôle d'un contrôleur de domaine ; corrigée au Patch Tuesday de juillet.
- **Avis CERT-FR (2 nov. 2026) :** trois vulnérabilités dans Tenable Identity Exposure, un outil de surveillance AD : un outil de protection peut lui-même devenir une porte d'entrée.

SOURCES

- CERT-FR — *Détection des compromissions sur Active Directory : journaux et indicateurs clés*
- Microsoft — *Microsoft Defender for Identity : détection des menaces sur les contrôleurs de domaine*
- ACSC / CISA — *Detecting and mitigating Active Directory compromises* (septembre 2026)
- Microsoft — *What's new in Defender for Identity* (mars à juin 2026) ; *RSA 2026: What's new in Microsoft Defender?* (20 mars 2026)
- Sophos — *CISA's Active Directory compromise techniques: a Sophos MDR perspective* (2026)
- Kudelski Security — *Certighost, CVE-2026-54121* (juillet 2026)
- CERT-FR — *Avis CERTFR-2026-AVI-1436* (2 novembre 2026)