AYI NEDJIMI Consultants

ADReplicationInspector : détection des attaque réplication Active Directory

10 mai 2026 • Mis à jour le 17 mai 2026 • 13 min de lecture • 2101 mots • 5 vu

> ADReplicationInspector surveille les événements de réplication Active Dire pour détecter DCSync, DCShadow, Golden Ticket et abus DRSUAPI.

ADReplicationInspector est un outil Python open source que je publie sur le portfo github de Ayi Nedjimi pour surveiller en continu les opérations de réplication Activ Directory. Le projet collecte les événements DSReplicaSync, DRSUAPI et les trace Sysmon générés par les contrôleurs de domaine, puis applique une couche d'anal comportementale pour distinguer une réplication légitime initiée par un DC parten d'une exfiltration de hachés via DCSync, d'un branchement frauduleux de DC fant via DCShadow ou d'un usage anormal d'un Golden Ticket Kerberos. L'objectif est fournir aux équipes SOC et aux Tier 0 administrators une détection précoce, lisible corrélée des techniques d'attaque AD les plus critiques, sans dépendre d'un EDR propriétaire ni d'une licence Microsoft Defender for ose ses dét

sous forme d'événements normalisés ECS, prêts à être ingérés dans Wazuh, Elast
Splunk ou un Sentinel hybride.

À RETENIR

Points clés

ADReplicationInspector détecte DCSync, DCShadow, Golden Ticket et abu
DRSUAPI via Event Log et Sysmon.

Collecte WinRM ou agent léger, normalisation ECS, alerting vers SIEM Waz
Elastic, Splunk ou Sentinel.

Aucun agent propriétaire requis, projet Python pur, déploiement sur n'impo
quel forêt Active Directory 2016 et au-delà.

Règles de corrélation alignées sur MITRE ATT&CK T1003.006, T1207, T155
T1484.001.

Pourquoi un outil dédié à la réplication Active Directory

La réplication est le cœur battant d'Active Directory. Sans elle, plus de propagation
mots de passe, plus de mise à jour des stratégies de groupe, plus de cohérence d
SYSVOL entre sites. Cette criticité explique pourquoi les attaquants ciblent la couc
réplication : en se faisant passer pour un contrôleur de domaine légitime via le pro
DRSUAPI, ils peuvent extraire la totalité des hachés NTLM stockés dans la base N
y compris le compte krbtgt qui sert à signer les tickets Kerberos.

Réponse sous 24h

Devis gratuit →