AYI NEDJIMI Consultants

BloodHound : Cartographier les Attaques Active Directory

10 mai 2026 • Mis à jour le 17 mai 2026 • 16 min de lecture • 3506 mots • 71 vues •

BloodHound est l'outil de reference open source pour la cartographie des chemins d'attaque dans les environnements Active Directory et Azure AD/Entra ID. Developpe initialement par SpecterOps en 2016, BloodHound exploite la theorie des graphes via une base de donnees Neo4j pour modeliser les utilisateurs, groupes, machines, GPO, OU et leurs relations de privileges. La force de BloodHound reside dans sa capacite a transformer une enumeration brute d'objets AD en un graphe interroge par requetes Cypher, revelant en quelques secondes les chemins d'escalade vers Domain Admin, les relations AdminTo, CanRDP, HasSession ou GenericAll impossibles a detecter manuellement.

BloodHound est l'outil de reference open source pour la cartographie des chemins d'attaque dans les environnements **Active Directory** et **Azure AD/ Entra ID**. Developpe initialement par SpecterOps en 2016, BloodHound exploite la **theorie des graphes** via une base de donnees **Neo4j** pour modeliser les utilisateurs, groupes, machines, GPO, OU et leurs relations de privileges. La force de BloodHound reside dans sa capacite a transformer une enumeration brute d'objets AD en un graphe interroge par requetes **Cypher**, revelant en quelques secondes les chemins d'escalade vers *Domain Admin*, les relations *AdminTo*, *CanRDP*, *HasSession* ou *GenericAll* impossibles a detecter manuellement. Utilise par les equipes **red team** pour planifier les phases de mouvement lateral et d'escalade de privileges, BloodHound est aujourd'hui un pilier de la **blue team** moderne pour reduire la surface d'attaque AD, prioriser le hardening et identifier les principals *Tier 0* mal configures. Cette page entity couvre l'architecture, les collectors (SharpHound, AzureHound, BloodHound.py), la methodologie d'analyse, les requetes Cypher critiques, la detection cote blue team et le mapping **MITRE ATT&CK** — un guide complet pour comprendre et maitriser BloodHound CE 5.x ainsi que sa version commerciale **BloodHound Enterprise**.

À RETENIR

L'essentiel a retenir

BloodHound est l'outil open source incontournable de cartographie d'attack paths Active Directory et Azure AD, base sur Neo4j et des requetes Cypher.

Réponse sous 24h

Devis gratuit →