AYI NEDJIMI Consultants

Agent IA pour auditer Active Directo

16 mai 2026 • Mis à jour le 17 mai 2026 • 19 min de lecture • 3011 mots •

Créez un agent IA autonome pour auditer Active Directory : LangChain + B
Kerberoasting automatisé. Guide technique complet pour red teams.

À RETENIR

A retenir -- Agent IA audit Active Directory

Un **agent IA audit Active Directory** combine la puissance de graphe de Blood
des LLM pour identifier et expliquer les chemins d'escalade de privileges en
L'architecture LangChain/smolagents + Neo4j BloodHound permet un attack
requetes Cypher complexes en recommandations operationnelles compréhe
doit etre deploye que dans le cadre d'un mandat de pentest ou de red teamin

L'audit de securite d'un environnement **Active Directory** est l'une des missions les
cybersecurite offensive. La multitude de chemins d'e ges possibl
Roasting, DCSync, Pass-the-Hash, Pass-the-Ticket, os non cont

impossible une analyse manuelle exhaustive dans les delais d'un engagement per
Directory change la donne : en combinant la puissance d'analyse de graphe de Bl
d'un LLM, il est possible d'automatiser l'identification des chemins d'attaque critic
pour les clients non techniques, et de prioriser automatiquement les remédiations
architecture complete, du code deployable et les considerations legales et ethique
un cadre professionnel legitime.

Architecture agent LLM + BloodHound + Neo4j

L'architecture de l'**agent IA d'audit AD** repose sur trois composants principaux qu

BloodHound CE (Community Edition) : collecte les donnees AD via SharpHoun
Fournit une API REST pour requeter les chemins d'attaque.

Neo4j + Cypher : base de donnees de graphe qui stocke les objets AD (utilisate
relations. Les requetes Cypher permettent d'identifier les chemins de privilege

Agent LLM (LangChain ou smolagents) : orchestre les outils disponibles (reque
documentation) pour repondre a des objectifs d'audit en langage naturel.

L'agent dispose de plusieurs outils : un outil de requete Cypher sur Neo4j, un outil
MITRE ATT&CK, un outil de generation de commandes de collecte additionnelle, e
objectif ("Trouver tous les chemins d'escalade de privileges vers Domain Admin")
requetes.

Réponse sous 24h

Devis gratuit →