AYI NEDJIMI Consultants

ITDR : détecter les menaces identitaires en temps réel

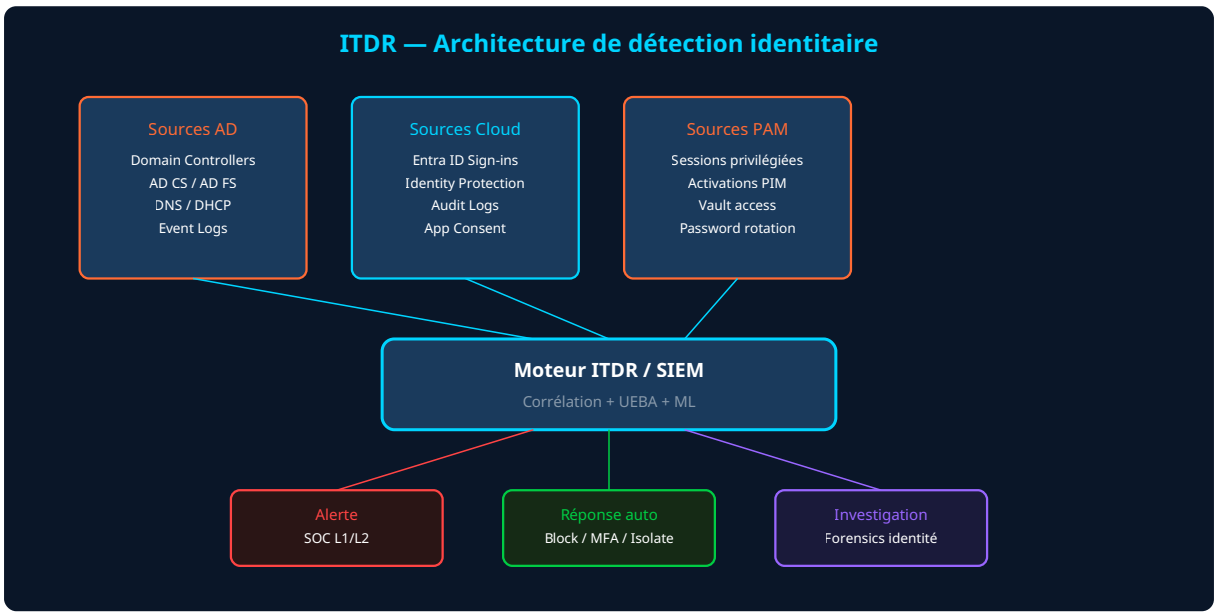
Catégorie : IAM et Gestion des Identités Lecture : 6 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

ITDR (Identity Threat Detection and Response) : détectez les menaces sur les identités en temps réel avec corrélation SOC, UEBA et réponse.

Les identités sont devenues le vecteur d'attaque principal. Compromission de comptes, élévation de privilèges illégitime, mouvement latéral via des credentials volés — ces scénarios représentent plus de 80% des brèches en 2025 selon le rapport Verizon DBIR. Face à ce constat, une nouvelle discipline émerge : l'Identity Threat Detection and Response, ou ITDR. Là où le SOC traditionnel surveille les événements réseau et les endpoints, l'ITDR se concentre spécifiquement sur les signaux liés aux identités. Connexions suspectes, modifications de privilèges non autorisées, usage anormal de comptes de service, tentatives de Kerberoasting — l'ITDR corrèle ces signaux pour détecter et répondre aux menaces identitaires avant qu'elles ne se transforment en incidents majeurs. Ce guide vous présente l'architecture ITDR de référence, les sources de données à intégrer, les cas d'usage de détection et les workflows de réponse automatisée. Nous nous appuyons sur des retours d'expérience terrain avec Microsoft Defender for Identity, CrowdStrike Falcon Identity Protection et Silverfort pour vous donner une vision pragmatique de l'ITDR en production.

Points clés à retenir

- **ITDR** est la convergence entre la gestion des identités et la détection des menaces
- Les signaux identitaires permettent de détecter les attaques 3 à 5 jours avant l'impact
- **Microsoft Defender for Identity** couvre l'AD on-premise, **Identity Protection** couvre Entra ID
- La corrélation identity + endpoint + network dans le **SOC** multiplie l'efficacité de détection
- La réponse automatisée (blocage de compte, MFA forcé) réduit le MTTR de 90%



Qu'est-ce que l'ITDR et pourquoi votre SOC en a besoin

L'*ITDR* (Identity Threat Detection and Response) est un concept formalisé par Gartner en 2022 qui désigne la capacité à détecter et répondre aux menaces ciblant les identités numériques. Le SOC traditionnel surveille trois domaines : le réseau (NDR), les endpoints (EDR) et le cloud (CSPM). L'ITDR ajoute un quatrième pilier : les identités. Cette vision est cohérente avec la réalité des attaques modernes où la compromission d'identité précède systématiquement l'accès aux données.

Le SOC, qu'il soit interne ou externalisé, doit intégrer les signaux identitaires dans sa stratégie de détection. Un mouvement latéral via Pass-the-Hash, une élévation de privilèges via Kerberoasting, un accès anormal à un compte de service — ces événements sont invisibles pour l'EDR mais parfaitement détectables par l'ITDR. La corrélation identity + endpoint multiplie les capacités de détection : quand un compte se connecte à un serveur inhabituel (signal identité) ET qu'un processus suspect s'exécute sur ce serveur (signal endpoint), la confiance dans l'alerte est très élevée.

Sources de données et intégration SIEM

L'ITDR repose sur quatre catégories de sources de données. Les **journaux Active Directory** : événements de connexion (4624/4625), modifications de groupes sensibles (4728/4732), changements de mot de passe (4723/4724), requêtes Kerberos (4769) et réplication DCSynC (4662). Les **journaux Entra ID** : sign-in logs, audit logs, Identity Protection risk detections et provisioning logs. Les **journaux PAM** : activations PIM, sessions privilégiées, accès vault. Les journaux Microsoft 365 : activité Exchange, SharePoint, Teams et compliance.

L'intégration dans le SIEM (Microsoft Sentinel, Splunk, Elastic) centralise ces sources et permet la corrélation croisée. Les règles de détection ITDR se divisent en deux catégories : les règles *signature-based* (patterns d'attaque connus comme le Kerberoasting ou le DCSync) et les règles

UEBA (User and Entity Behavior Analytics) qui détectent les anomalies comportementales par machine learning. La combinaison des deux approches couvre à la fois les attaques connues et les comportements anormaux qui pourraient signaler une attaque inédite.

Cas d'usage de détection ITDR

Voici les dix cas d'usage de détection ITDR à implémenter en priorité dans votre SOC. Le **Kerberoasting** : un utilisateur demande un nombre anormal de tickets TGS pour des SPNs différents en peu de temps. Le **DCSync** : un compte non-DC utilise les droits de réplication Active Directory. L'**AS-REP Roasting** : tentatives d'authentification pré-auth désactivée sur des comptes sensibles. Le **Password Spraying** : multiples échecs de connexion sur différents comptes depuis la même source. Le SID History injection : modification suspecte de l'attribut SIDHistory sur un compte.

Côté cloud : l'**Impossible Travel** (connexion depuis Paris puis Tokyo en 30 minutes), le **Token Replay** (utilisation d'un token de session depuis une IP différente de celle d'émission), le **Consent Phishing** (consentement applicatif pour des permissions élevées), la **création de backdoor** (ajout de credentials sur un Service Principal) et l'**élévation de rôle non autorisée** (attribution de Global Admin hors processus PIM). Les techniques d'attaque Active Directory fournissent le contexte technique pour calibrer ces détections.

Cas d'usage	Source de données	Priorité	Outil recommandé
Kerberoasting	Event 4769 (AD)	Critique	Defender for Identity
DCSync	Event 4662 (AD)	Critique	Defender for Identity
Password Spraying	Sign-in logs (Entra)	Élevée	Identity Protection
Impossible Travel	Sign-in logs (Entra)	Élevée	Identity Protection
Consent Phishing	Audit logs (Entra)	Élevée	Sentinel / Splunk
Privilege Escalation	PIM + Audit logs	Critique	Sentinel + SOAR

Microsoft Defender for Identity en pratique

Microsoft Defender for Identity (ex-Azure ATP) est la solution ITDR la plus déployée pour les environnements Active Directory. Un capteur installé sur chaque contrôleur de domaine analyse le trafic réseau (pas d'agent endpoint nécessaire) et détecte les attaques en temps réel. La couverture inclut : reconnaissance (LDAP enumeration, DNS recon), compromission de credentials (Kerberoasting, Brute Force, AS-REP Roast), mouvement latéral (Pass-the-Hash, Pass-the-Ticket, Overpass-the-Hash) et persistance (DCSync, Golden Ticket, SID History injection).

L'intégration avec **Microsoft 365 Defender** corrèle les alertes identité avec les alertes endpoint (Defender for Endpoint) et email (Defender for Office 365). Un scénario type : Defender for Identity détecte une tentative de Kerberoasting (signal identité), Defender for Endpoint identifie l'outil Rubeus sur le poste source (signal endpoint), et l'incident unifié dans le portail M365

Defender offre une vue complète de la chaîne d'attaque. La réponse peut être automatisée : désactivation du compte compromis, isolation du poste et notification au playbook de réponse à incident.

Réponse automatisée aux menaces identitaires

La détection sans réponse ne sert à rien si le temps de réaction dépasse la vitesse de l'attaquant. L'**automatisation de la réponse** (SOAR — Security Orchestration, Automation and Response) réduit le temps moyen de réponse (MTTR) de plusieurs heures à quelques secondes. Les actions de réponse automatisée pour l'ITDR : blocage immédiat du compte compromis, forçage du MFA à la prochaine connexion, révocation de tous les tokens de session actifs, isolation du terminal source via l'EDR et création automatique du ticket d'incident.

La configuration des playbooks de réponse automatisée nécessite une calibration fine pour éviter les faux positifs qui bloquent des utilisateurs légitimes. La stratégie recommandée : automatisation complète pour les alertes à haute confiance (DCSync depuis un non-DC = blocage immédiat), semi-automatisation pour les alertes à confiance moyenne (impossible travel = MFA forcé + alerte SOC), alerte manuelle pour les alertes à faible confiance (connexion inhabituelle = notification pour investigation). Les playbooks Microsoft fournissent des modèles de réponse pour les scénarios courants.

Construire votre programme ITDR progressivement

Le déploiement de l'ITDR suit trois phases. La phase 1 (quick wins, 4-6 semaines) : déployez Defender for Identity sur les DC, activez Identity Protection dans Entra ID et configurez les 5 alertes critiques (DCSync, Kerberoasting, Password Spraying, Impossible Travel, privilege escalation). La phase 2 (consolidation, 2-3 mois) : intégrez les sources PAM, créez les règles UEBA personnalisées, configurez la réponse automatisée pour les scénarios à haute confiance. La phase 3 (maturité, 3-6 mois) : implémentez les cas d'usage avancés, le threat hunting identitaire proactif et les métriques de performance ITDR.

Le guide ANSSI sur la journalisation fournit un cadre de référence pour le dimensionnement des sources de données. Les métriques ITDR à suivre : temps moyen de détection (MTTD) d'une compromission d'identité, taux de faux positifs des alertes identitaires, couverture des comptes à privilèges par le monitoring et nombre de réponses automatisées déclenchées par mois.

Questions fréquentes sur l'ITDR

Quelle différence entre ITDR et IAM Security ?

L'IAM Security est un terme générique qui couvre la sécurisation des systèmes de gestion des identités. L'ITDR est spécifiquement la capacité de détection et de réponse aux menaces ciblant les identités, en temps réel, intégrée au SOC. Pensez à l'ITDR comme l'équivalent de l'EDR mais pour les identités : un outil de détection et de réponse opérationnel, pas un outil de gouvernance ou de configuration.

Faut-il un outil ITDR dédié ou le SIEM suffit-il ?

Le SIEM peut implémenter des règles de détection identitaire, mais les outils ITDR dédiés (Defender for Identity, CrowdStrike Falcon Identity, Silverfort) offrent des avantages significatifs : détection par analyse du trafic réseau (pas uniquement les logs), modèles ML pré-entraînés sur des millions de tenants, couverture des attaques spécifiques AD (Golden Ticket, DCSync) sans configuration manuelle des règles. L'approche optimale : outil ITDR dédié pour la détection, SIEM pour la corrélation et l'orchestration de la réponse.

Comment mesurer le ROI d'un programme ITDR ?

Trois axes de mesure : la réduction du temps moyen de détection des compromissions d'identité (benchmark : passer de 200+ jours à moins de 24 heures), le nombre d'incidents évités grâce à la détection précoce (quantifiez en coût moyen d'incident : 150 à 500 k€) et la réduction du temps d'investigation par incident (de 40 heures à 4 heures grâce à la corrélation automatique). Un programme ITDR mature se rentabilise dès le premier incident majeur détecté et contenu avant propagation.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et actions prioritaires

L'ITDR comble un gap critique dans la posture de sécurité de la plupart des organisations. Les identités sont attaquées quotidiennement, mais la majorité des SOC ne surveillent pas spécifiquement ce vecteur. Commencez par Defender for Identity sur vos contrôleurs de domaine et Identity Protection sur Entra ID — ces deux briques couvrent 80% des cas d'usage ITDR. Puis intégrez progressivement les sources PAM et les règles personnalisées. Chaque semaine sans ITDR est une semaine où une compromission d'identité pourrait passer inaperçue dans votre environnement.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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