VECTRA

EBOOK

Gare à vos gaps de sécurité

Comment les attaquants traversent votre SI

Par Lucie Cardiet · Cyberthreat Research Manager

Pourquoi j'ai écrit ce ebook

Mot de l'auteure

Je passe mes journées à observer ce que les attaquants font réellement, pas ce que les éditeurs prétendent qu'ils font, pas ce que disaient les rapports de menaces de l'année dernière, pas ce que la catégorie de produits que nous utilisons tous est censée détecter. Ce qu'ils font réellement, cette semaine, dans des environnements qui ressemblent au vôtre.

Ce que je constate systématiquement, c'est que les défenseurs ne perdent pas par manque d'investissement. Ils perdent parce que leurs investissements restent dans une zone d'efficacité partielle. Leur EDR fonctionne exactement comme prévu ; l'attaquant, lui, opère sur le plan de l'identité. Leur SIEM ingère tous les logs ; et l'attaque n'est visible que dans la corrélation entre ces logs. Leur IAM approuve chaque connexion conforme à la politique ; sauf que la personne en face n'est pas l'employé dont on utilise les identifiants.

Voici la deuxième édition de ce que j'ai d'abord écrit en 2025. Quoi de neuf : deux campagnes supplémentaires (Volt Typhoon et AWS compromis par des agents IA en huit minutes), les résultats mesurés par IDC en 2025 sur l'utilisation de Vectra AI, une section sur la pression réglementaire qui fait de la détection continue une question de conformité, et une auto-évaluation à la fin.

Lucie Cardiet

Le réseau a dépassé son architecture de sécurité.

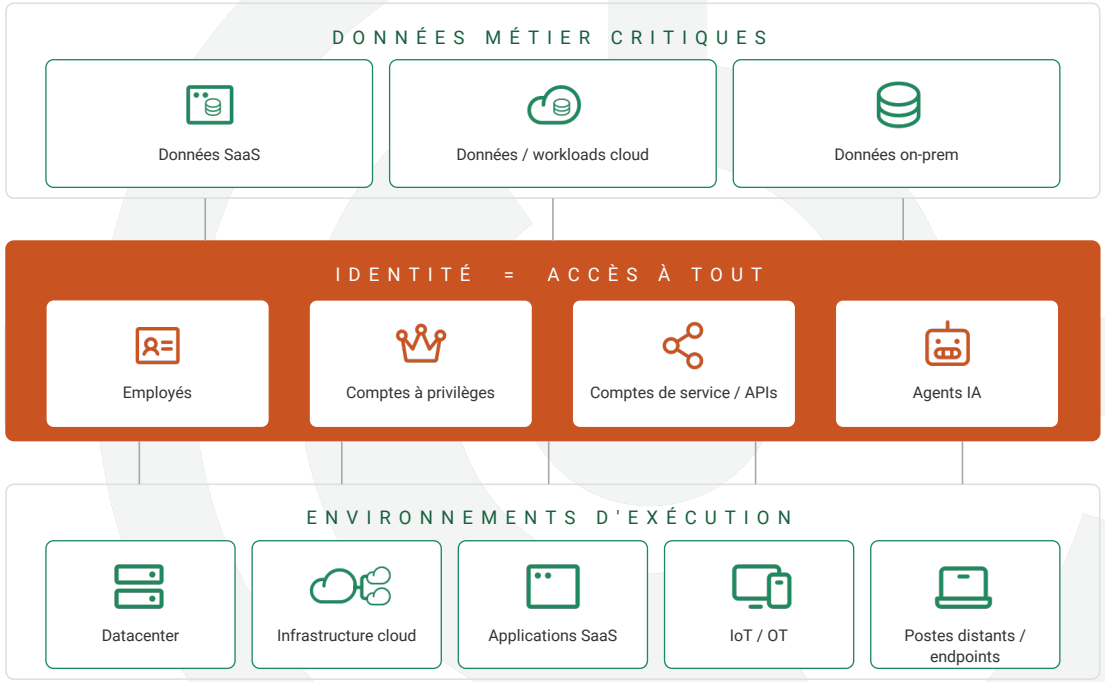
Aujourd'hui, l'entreprise ne vit plus derrière un seul périmètre

Les environnements d'entreprise s'étendent sur l'infrastructure on-prem, plusieurs clouds publics, des dizaines d'applications SaaS, des fournisseurs d'identité, des systèmes IoT et OT, des services d'IA et les agents autonomes qui opèrent par-dessus. Ces domaines ne sont pas indépendants, ils forment un seul système connecté.

- ✓ Votre EDR surveille les endpoints.
- ✓ Votre IAM approuve les connexions.
- ✓ Votre CSPM lit les configurations.
- ✓ Votre SIEM stocke les logs.

Chacun fait son travail.

Les attaquants, de plus en plus assistés par l'IA, ont passé trois ans à apprendre à naviguer entre eux, dans les zones qu'aucun outil n'observe.



Le réseau a évolué. Les attaquants aussi.

Votre stack est solide, mais est-il complet ?

À première vue, vous avez mis en place un stack de sécurité solide.

- Vous avez investi dans les meilleures technologies de sécurité disponibles aujourd'hui.
- Vous avez une protection des endpoints sur chaque appareil.
- Vous avez des outils qui surveillent votre réseau.
- Vos outils de cloud posture management scannent correctement vos configurations.
- Vous avez renforcé la gestion des identités avec un IAM ou un PAM.

Et pourtant, les attaquants peuvent passer à travers, et ils le font.

Pas parce que vos outils sont défectueux. Parce que chaque outil a été conçu pour couvrir son propre domaine, et que les attaquants opèrent désormais entre eux.

Les attaquants ne cassent pas vos outils. Ils les contournent.

La réalité : les attaquants modernes ne combattent pas votre stack. Ils l'évitent.

Abus d'identité
Les identifiants compromis sont le vecteur d'accès initial dans 22 % des breaches.[1] 88 % des attaques web élémentaires impliquent des identifiants volés.[1]

Mouvement latéral
Ils se déplacent latéralement sans déclencher d'alerte. Le breakout time eCrime moyen – l'écart entre l'accès initial et le premier pivot latéral – est tombé à 29 minutes.[2]

Abus de privilèges cloud
L'abus de comptes valides représente désormais 35 % des incidents cloud.[2]

Opération entre les outils
Ils se cachent dans les interstices entre les outils, dans des espaces qu'aucun système n'a été conçu pour observer.

Exploitation du bruit des alertes
Ils opèrent en dessous de vos seuils, sachant que votre SOC ne peut pas tout investiguer.

Vitesse cross-domain
Le MFA bloque plus de 99 % des attaques d'identité, mais les adversaires se connectent de plus en plus via des tokens volés, des applications OAuth consenties, des flux device-code et des proxies adversary-in-the-middle.[3]

Reconnaissance accélérée par l'IA
Les attaques menées par des adversaires utilisant l'IA ont augmenté de 89 % d'une année sur l'autre. En 2025, des attaquants ont exploité des outils GenAI légitimes dans plus de 90 organisations pour générer des commandes de vol d'identifiants.[2]

[1] Verizon DBIR 2025. [2] CrowdStrike 2026 Global Threat Report. [3] Microsoft Digital Defense Report 2025.

Les meilleurs outils ne valent pas une couverture complète.

Si chacun de vos investissements réduit le risque dans son domaine, ils laissent des angles morts en visibilité et en détection entre les outils. Les chiffres de 2026 le confirment :

- 82 % des détections d'intrusion en 2025 étaient sans malware. Les attaquants ont opéré avec des identifiants valides, des flux d'identité de confiance et des intégrations SaaS approuvées.[1]
- Les breaches impliquant plusieurs environnements coûtent 5,05 M$ en moyenne, soit 25 % de plus que les breaches purement on-prem.[2]
- Le breakout time moyen est tombé à 29 minutes. Record observé : 27 secondes.[1]

[1] CrowdStrike 2026 Global Threat Report. [2] IBM Cost of a Data Breach Report 2025.

Le schéma n'est pas nouveau. C'est la nouvelle norme.

Ce ebook est conçu pour vous aider à cartographier ces angles morts, à vous montrer où Vectra AI s'inscrit et comment Vectra AI les comble.

Sommaire

Vue d'ensemble de la couverture

Illustration des gaps de sécurité, et trois campagnes nommées qui l'exploitent.

L'illustration des gaps de sécurité

Votre stack actuel : aucune combinaison ne fournit une détection continue sur l'ensemble de l'infrastructure hybride. Chaque outil s'arrête à des étapes clés.

		Accès initial	Exécution	Persistance	Élévation de privilèges	Évasion des défenses	Accès aux identifiants	Découverte	Mouvement latéral	Collecte	Commande et contrôle	Exfiltration	Impact
ENDPOINT	EDR	●	●	●	●	●	●	●	●	●	●	●	●
ENDPOINT	EPP	●	●	○	○	○	○	○	○	○	○	○	○
CLOUD	CASB	●	○	○	●	○	●	○	○	●	○	●	○
CLOUD	CNAPP	●	●	●	●	●	●	●	●	●	●	●	●
CLOUD	CSPM	○	○	○	●	○	●	○	○	○	○	○	○
CLOUD	CWPP	●	●	●	●	○	○	●	○	●	●	○	●
CLOUD	SASE	●	○	○	○	○	○	○	●	○	●	●	○
RÉSEAU	Email	●	○	○	○	○	○	○	○	○	○	○	○
RÉSEAU	Firewalls	●	○	○	○	○	○	●	○	○	●	●	○
RÉSEAU	IDPS	●	○	○	○	○	○	●	●	○	●	●	○
RÉSEAU	NAC	●	○	○	○	○	○	○	○	○	○	○	○
RÉSEAU	SSE	●	○	○	○	○	○	○	●	○	●	●	○
IDENTITÉ	IAM	●	○	○	●	○	○	○	○	○	○	○	○
IDENTITÉ	PAM	○	○	○	●	○	●	○	○	○	○	○	○
IDENTITÉ	UEBA	●	○	●	●	●	●	●	●	○	○	●	○
Plateforme Vectra AI		●	●	●	●	●	●	●	●	●	●	●	●

● Visibilité partielle ● Visibilité totale ○ Aucune visibilité

Trois angles morts dans tous les stacks aujourd'hui.

Pas des angles morts de couverture. Des angles morts d'exécution. Des contrôles qui existent mais ne détectent pas.

1. Rien ne paraît anormal.

Les outils de l'attaquant sont vos outils. Bureau distant. PowerShell. Un binaire signé. Des binaires living-off-the-land que vos sysadmins utilisent à 2 h du matin. Chaque action prise individuellement ressemble à une opération normale.

2. L'authentification réussit.

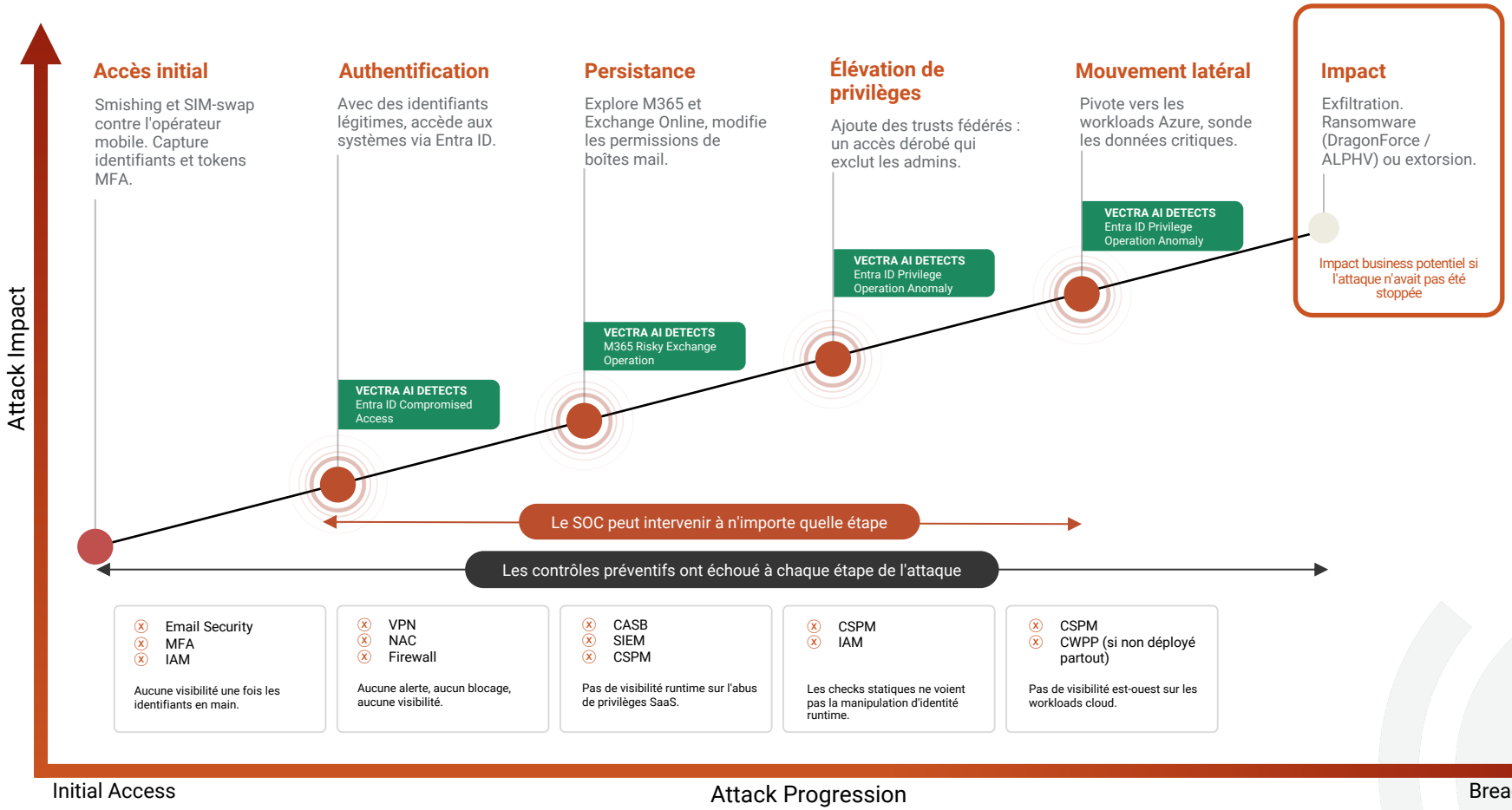
Identifiants valides, MFA approuvé, la connexion est réelle. Ce n'est juste pas la personne que vous croyez. Chaque vérification d'authentification dit oui. Mais l'utilisateur valide n'est pas réellement l'utilisateur.

3. Le mouvement n'est pas visible.

Une fois à l'intérieur, le mouvement latéral passe par des intégrations de confiance : SaaS-vers-SaaS, identité fédérée, tokens OAuth, comptes de service. L'EDR ne le voit pas. Le CASB ne le voit pas. Le mouvement est invisible par architecture, pas par furtivité.

Scattered Spider : le playbook du helpdesk

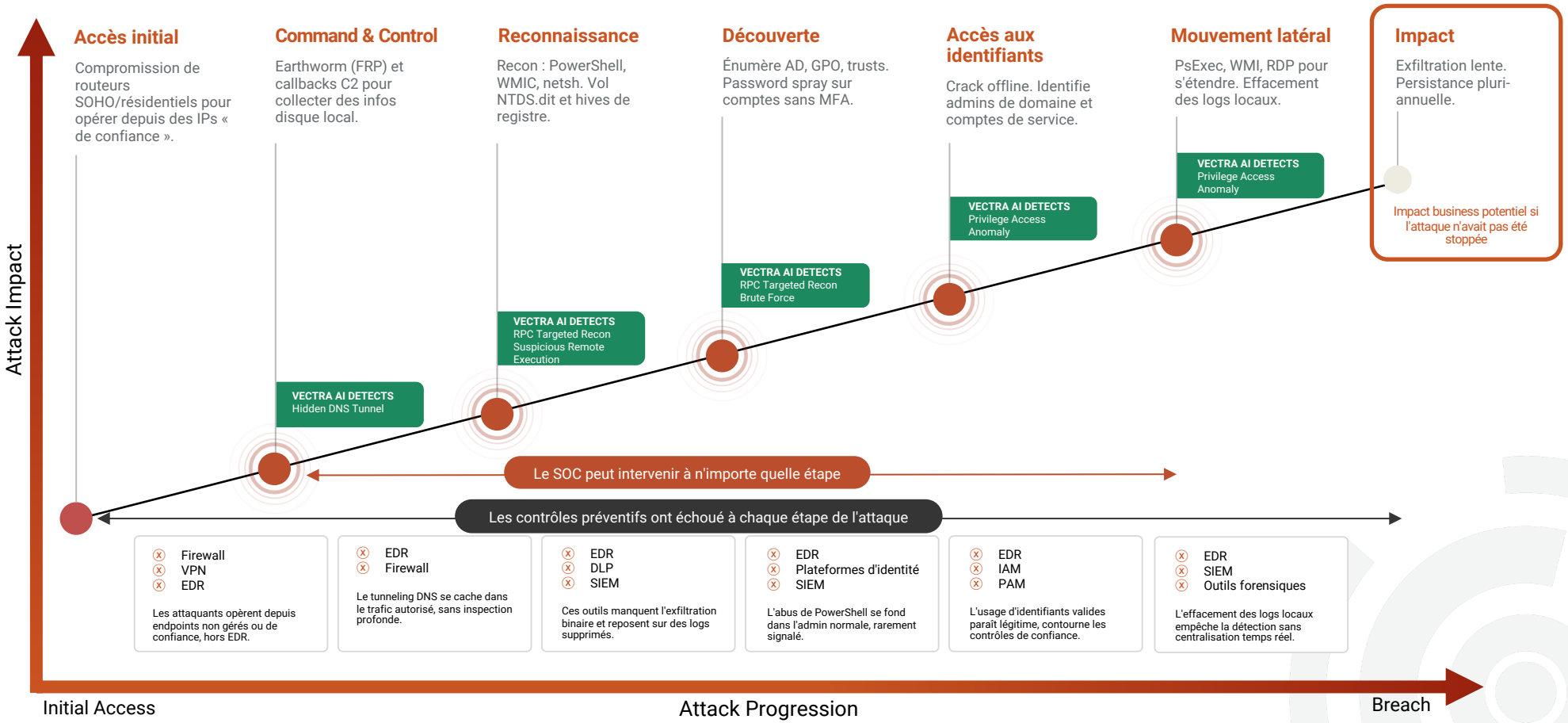
Scattered Spider (UNC3944) illustre parfaitement la raison pour laquelle les « identifiants valides » sont devenus un problème de détection. Le groupe n'a pas exploité de vulnérabilités. Ils ont appelé le helpdesk.



Sources : reporting Mandiant UNC3944 (2023–2024) ; CISA Advisory AA23-320A sur les TTPs de Scattered Spider.

Volt Typhoon : le playbook living-off-the-land

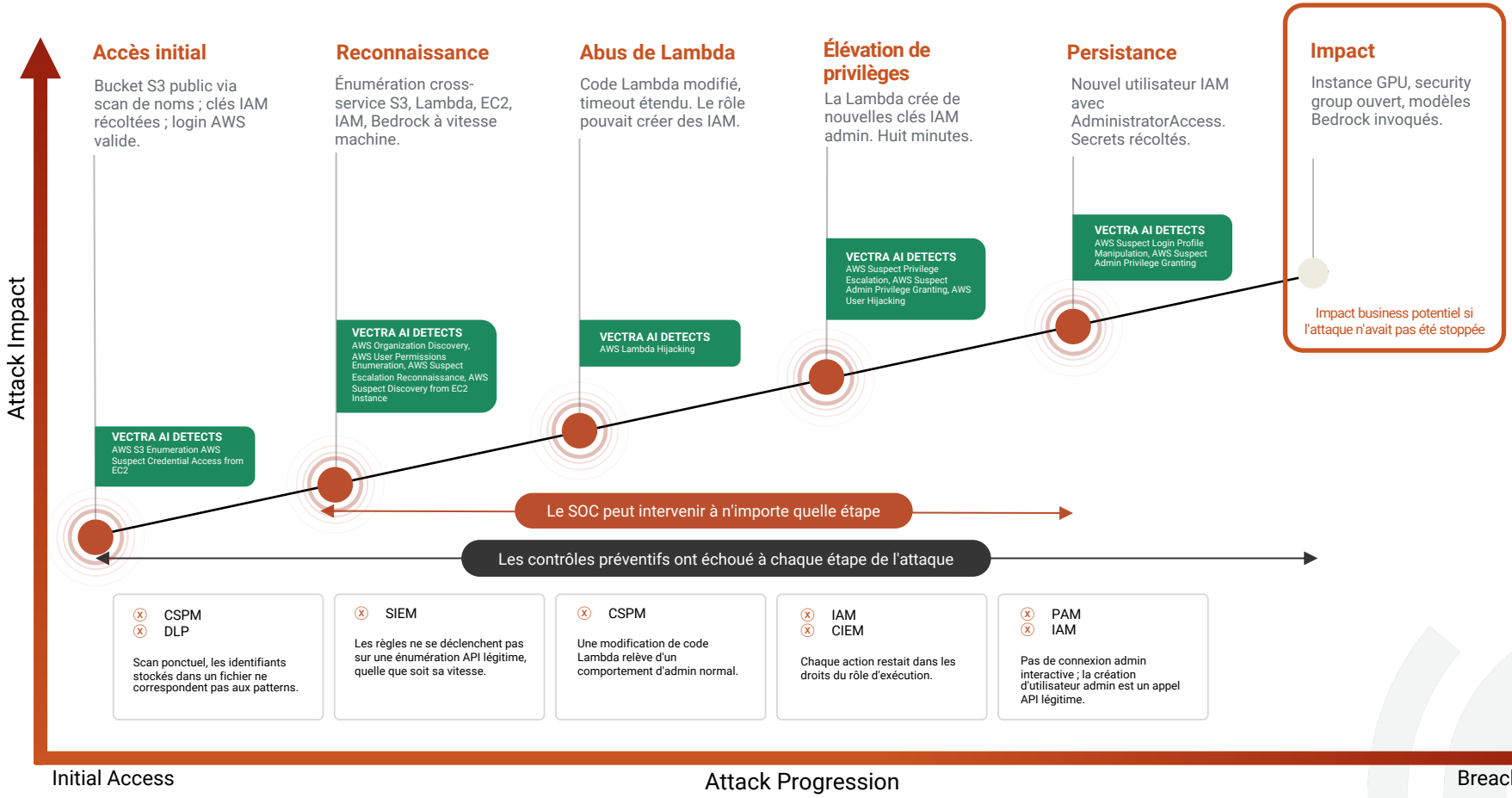
Volt Typhoon est la campagne attribuée à la RPC qui a montré aux défenseurs américains à quoi ressemble réellement le « living off the land ». L'advisory CISA/NSA/FBI de février 2024 a documenté des opérateurs présents dans des réseaux d'infrastructures critiques jusqu'à cinq ans, en utilisant uniquement des outils Windows natifs, sans aucun malware à signaler.



Sources : advisory conjoint CISA/NSA/FBI AA24-038A (févr. 2024) ; Microsoft Threat Intelligence « Volt Typhoon targets US critical infrastructure with living-off-the-land techniques » (mai 2023).

AWS compromis par des agents IA en huit minutes.

Intrusion documentée par Sysdig (2025). Identifiants valides. Services AWS natifs. Reconnaissance à vitesse machine.



Sources : blog de threat research Sysdig (2025) ; techniques MITRE ATLAS d'abus de comptes valides et de découverte de services cloud.

Pourquoi votre stack actuel vous laisse à découvert.

Trois attaquants. Trois années. Trois points d'entrée. Chaque attaque paraissait légitime de bout en bout dans n'importe quel outil. Ce n'est qu'en croisant réseau, identité et plan de contrôle cloud que l'intention apparaît.

Il est tentant de penser qu'avec vos investissements en firewalls, EDR, CASB, CSPM, IAM et SIEM, les angles morts sont comblés. La réalité : ces outils n'ont pas été conçus pour détecter les comportements d'attaquants dans des environnements hybrides, et les chiffres le montrent.

82 %

des détections d'intrusion en 2025 étaient sans malware.

CrowdStrike 2026 Global Threat Report

32 %

de hausse des attaques basées sur l'identité au premier semestre 2025.

Microsoft Digital Defense Report 2025

241 jours

pour identifier et contenir une breach. 292 jours quand des identifiants volés sont impliqués.

IBM Cost of a Data Breach Report 2025

Dans les sections suivantes, nous décortiquons précisément où chaque partie de votre stack fait défaut, et nous vous montrons comment Vectra AI comble ces angles morts dans le réseau, le cloud, le SaaS et l'identité.

VECTRA

GARE À VOS GAPS

Sécurité des endpoints

Pourquoi l'EDR et l'EPP ne suffisent pas seuls.

EDR : profond sur l'hôte, mais nulle part ailleurs.

L'Endpoint Detection and Response offre une télémétrie détaillée là où il est déployé.

Accès initial	Partielle
Exécution	Totale
Persistance	Partielle
Élévation de privilèges	Partielle
Évasion des défenses	Partielle
Accès aux identifiants	Partielle
Découverte	Partielle
Mouvement latéral	Partielle
Collecte	Partielle
Commande et contrôle	Partielle
Exfiltration	Partielle
Impact	Totale

VISIBILITÉ : Partielle Totale Aucune

L'EDR va plus loin que la prévention, en offrant télémétrie et analytics détaillés sur les processus, les changements de registre et l'activité locale. Il est puissant là où il est installé. La réalité 2025 : 82 % des détections d'intrusion étaient sans malware.[1] Les attaquants opèrent avec des identifiants valides, dans des sessions de confiance, là où l'EDR n'a rien à signaler.

COMMENT LES ATTAQUANTS CONTOURNENT

- Évitent l'endpoint en opérant directement dans des consoles cloud ou des apps SaaS.
- Exploitent les angles morts de couverture. L'EDR ne voit que les hôtes où il est installé.
- Se déplacent via des appareils non gérés ou BYOD qui ne font tourner aucun agent.
- Utilisent des identifiants valides pour mener une activité qui paraît « normale » à l'EDR.

L'EDR n'a aucune visibilité sur les attaques cloud-natives, les abus d'identité ou l'activité SaaS.

Trois des quatre vulnérabilités les plus exploitées en 2024 étaient des zero-days dans des produits de sécurité eux-mêmes : Palo Alto, Ivanti, Fortinet.[2]

[1] CrowdStrike 2026 Global Threat Report. [2] Mandiant M-Trends 2025

EPP : bloque les malwares connus, aveugle au reste.

Les Endpoint Protection Platforms empêchent l'exécution des menaces connues.

Accès initial	●
Exécution	●
Persistance	
Élévation de privilèges	
Évasion des défenses	
Accès aux identifiants	
Découverte	
Mouvement latéral	
Collecte	
Commande et contrôle	
Exfiltration	
Impact	

VISIBILITÉ : ● Partielle ● Totale ○ Aucune

Les EPP utilisent signatures, heuristiques et sandboxing basique. Les EPP modernes (NGAV) ajoutent détection comportementale et analyse fileless ML, mais restent cantonnés à l'endpoint et aveugles aux mouvements d'attaquants entre domaines.

COMMENT LES ATTAQUANTS CONTOURNENT

- Malware fileless ou staging soigné, sous le radar comportemental.
- Zero-days ou binaires inédits sans signature.
- PowerShell, WMI, RDP : indissociables de l'admin.

L'EPP ne détecte pas living-off-the-land ni attaques par identifiants.

Même un EPP moderne reste cantonné à l'endpoint. Cloud, identité, SaaS-vers-SaaS sont invisibles par conception.

Le gap de la sécurité des endpoints, comment Vectra AI le comble.

LE GAP DE LA SÉCURITÉ ENDPOINT

L'EDR et l'EPP sont des fondations, mais ils ne couvrent qu'une partie de la kill chain.

Ils manquent :

- Identité avec identifiants valides dans Microsoft 365 ou Entra ID.
- Abus de privilèges SaaS hors endpoint.
- Mouvement latéral cloud, BYOD, identité fédérée.
- Recon et exfiltration sur canaux chiffrés ou non-HTTP.

Même sur les endpoints, l'EPP manque souvent les comportements sophistiqués, et l'EDR ne détecte pas toujours l'usage abusif de comptes si aucun malware n'est impliqué.

CE QUE VECTRA APPORTE

- Identity Threat Detection pour comptes compromis abusant SaaS et cloud.
- SaaS Misuse Detection sur Microsoft 365, Exchange Online, Entra ID.
- Couverture hybride : endpoint, cloud, réseau, identité.
- S'intègre avec CrowdStrike, Microsoft Defender, SentinelOne et d'autres plateformes EDR.

VECTRA

GARE À VOS GAPS

Sécurité du cloud

Le gap du cloud hybride.

CASB : bloque les apps non sanctionnées, ignore les abus actifs.

Applique des politiques sur le SaaS. Ne voit pas les attaquants dans des sessions valides.

Les CASB appliquent des politiques via API ou en mode proxy inline. En mode API (le déploiement courant), ils voient l'activité quasi temps réel avec quelques minutes de latence. Dans tous les cas, les CASB opèrent au-dessus des plans réseau et identité, aveugles à ce que font les attaquants une fois qu'une session valide existe.

COMMENT LES ATTAQUANTS CONTOURNENT

- Utilisent des identifiants valides pour accéder au SaaS sanctionné (Microsoft 365, Box, Salesforce).
- Exploitent les permissions depuis l'intérieur (délégation de boîte mail).
- Abusent de la confiance entre identités fédérées pour se connecter via des chemins SSO de confiance.

Le CASB ne fournit aucune visibilité au niveau réseau.

Il ne détecte pas toujours les abus de privilèges en direct, la manipulation d'identité ou les comportements de type insider.

CSPM : trouve les misconfigurations, pas les comportements.

Identifie les paramètres à risque. Bon pour la prévention, pas la détection.

Le CSPM signale les buckets S3 ouverts, les ports SSH exposés, les logs désactivés. Il est orienté prévention, il scanne les conditions susceptibles d'autoriser une attaque, pas les attaques elles-mêmes.

COMMENT LES ATTAQUANTS CONTOURNENT

- Exploitent une misconfiguration avant qu'elle soit corrigée.
- Utilisent tokens API ou OAuth pour escalader dans le cloud.
- Abusent de rôles IAM sur-privilégiés que le CSPM signale sans surveiller en temps réel.

Le CSPM ne fournit aucune visibilité au niveau réseau.

Il ne voit ni l'activité runtime, ni le mauvais usage d'identifiants, ni le mouvement latéral. Il signale des conditions, pas des attaques.

CWPP : protège les workloads, à condition de tout couvrir.

VMs, conteneurs, serverless, si les agents sont déployés.

Accès initial	●
Exécution	●
Persistance	●
Élévation de privilèges	●
Évasion des défenses	○
Accès aux identifiants	○
Découverte	●
Mouvement latéral	○
Collecte	●
Commande et contrôle	●
Exfiltration	○
Impact	●

VISIBILITÉ : ● Partielle ● Totale ○ Aucune

Les CWPP sécurisent les instances de calcul avec une visibilité runtime sur le comportement des workloads cloud. La couverture dépend de la cohérence du déploiement.

COMMENT LES ATTAQUANTS CONTOURNENT

- Se déplacent vers des workloads non gérés ou des régions où aucun agent n'est installé.
- Utilisent des outils légitimes au sein d'un workload (PowerShell, bash) pour échapper à la détection.
- Opèrent entièrement dans les couches SaaS ou identité, hors de portée du CWPP.

Les CWPP ne fournissent aucune visibilité au niveau réseau.

Aveugles aux abus SaaS et au mauvais usage de l'IAM cloud.

CNAPP : consolide, n'observe pas le comportement.

Combine CSPM, CWPP, parfois CIEM et détection runtime.

Les CNAPP modernes ajoutent la détection runtime (CDR) en plus du scanning de posture. Mais la détection runtime reste cantonnée au workload. Elle observe ce qui se passe sur un workload donné, pas les pivots sur le plan d'identité ou réseau que les attaquants utilisent pour passer d'un workload à un autre.

COMMENT LES ATTAQUANTS CONTOURNENT

- Utilisent l'identité fédérée ou la manipulation SaaS, que le CNAPP ne suit pas en profondeur.
- Opèrent entre les workloads, échappant à la détection si le trafic est-ouest n'est pas inspecté.
- Bougent vite, avant que le scan de configuration ne tourne à nouveau.

Le CNAPP améliore la visibilité, mais pas suffisamment.

Il manque toujours la détection des comportements d'attaquants dans les couches réseau, identité cloud et SaaS.

CIEM : consolide, mais ignore le comportement.

Combine CSPM, CWPP, de plus en plus CIEM et détection runtime..

Accès initial	○
Exécution	○
Persistance	○
Élévation de privilèges	●
Évasion des défenses	○
Accès aux identifiants	●
Découverte	○
Mouvement latéral	○
Collecte	○
Commande et contrôle	○
Exfiltration	○
Impact	○

VISIBILITÉ : ● Partielle ● Totale ○ Aucune

Le CIEM analyse les droits d'identité cloud : qui peut faire quoi dans AWS, Azure, GCP. Il signale les rôles sur-privilégiés, les accès dormants, les permissions excessives.

COMMENT LES ATTAQUANTS CONTOURNENT

- Utilisent des droits classés à faible risque mais exploitables pour une élévation de privilèges quand on les enchaîne.
- Agissent dans les limites approuvées d'une manière que la baseline n'a jamais modélisée.
- Abusent des rôles fédérés et de la confiance cross-account. Le CIEM les cartographie, mais ne les surveille pas en temps réel.

Le CIEM signale les accès sur-privilégiés. Il ne détecte pas l'abus de privilèges légitimes.

Comme le CSPM et le CNAPP, le CIEM opère au niveau de la posture. Les droits sont statiques ; les attaques sont des comportements dynamiques à l'intérieur de ces droits.

SASE : contrôle l'accès, pas ce qui se passe ensuite.

SWG + ZTNA + CASB + DLP, unifiés.

Le SASE contrôle la manière dont les utilisateurs accèdent aux applications, mais ne détecte pas ce que ces utilisateurs font une fois l'accès accordé dans le cloud.

COMMENT LES ATTAQUANTS CONTOURNENT

- Utilisent des droits faible-risque exploitables une fois enchaînés.
- Agissent dans les limites approuvées, jamais modélisées par la baseline.
- Se déplacent latéralement via des connexions cloud-natives (chaînage de rôles IAM, confiance fédérée).

Le SASE voit les chemins d'accès, pas les comportements d'attaquants qui s'y cachent.

Le gap de la sécurité du cloud et comment Vectra AI le comble.

LE GAP DE LA SÉCURITÉ DU CLOUD

Vos outils cloud sont solides en prévention, faibles en détection.

Ils manquent :

- Abus de privilèges SaaS (délégation mail dans M365).
- Backdoors d'identité fédérée (manipulation Entra ID).
- Trafic est-ouest cloud (entre VPCs, conteneurs, comptes).
- Patterns API cross-account et chaînage de rôles IAM.
- Command-and-control cloud-natif (tokens AWS STS, rôles Entra ID).

L'abus de comptes valides a représenté 35 % des incidents cloud en 2025. Les intrusions cloud-conscious ont progressé de 37 % d'une année sur l'autre, et de 266 % chez les acteurs étatiques.[1]

CE QUE VECTRA AI APPORTE

- Détection temps réel sur M365, Entra ID, AWS, Azure, GCP, fédération.
- Voit ce que la posture manque : qui fait quoi, maintenant.
- Corrélation comportementale identité / réseau / cloud.

[1] CrowdStrike 2026 Global Threat Report.

VECTRA

GARE À VOS GAPS

Sécurité du réseau

Quand le trafic paraît normal, mais ne l'est pas.

Email security : stoppe le spam, pas l'ingénierie sociale.

Bloque le mauvais connu. Manque la compromission post-phishing.

Les passerelles email sécurisées et les filtres anti-phishing bloquent les messages connus comme malveillants. Mais les attaquants utilisent du phishing soigné qui passe outre.

COMMENT LES ATTAQUANTS CONTOURNENT

- Envoient du phishing d'identifiants par SMS, LinkedIn ou email personnel, contournant les filtres d'entreprise.
- Utilisent des domaines lookalike ou la fatigue MFA pour amener les utilisateurs à livrer leurs identifiants.
- Exploitent la confiance, pas le malware. Aucune pièce jointe ou lien n'est signalé.

Les outils d'email security ne détectent pas la compromission de comptes après un phishing réussi.

Or c'est précisément là que se situent la plupart des breaches modernes.

Firewalls : contrôlent le périmètre, pas l'intérieur.

Restreignent au périmètre. Une fois passé, aveugles.

Accès initial	●
Exécution	○
Persistance	○
Élévation de privilèges	○
Évasion des défenses	○
Accès aux identifiants	○
Découverte	●
Mouvement latéral	○
Collecte	○
Commande et contrôle	●
Exfiltration	●
Impact	○

VISIBILITÉ : ● Partielle ● Totale ○ Aucune

Les firewalls traditionnels filtrent par IP, port, protocole. Les NGFW ajoutent inspection applicative et déchiffrement TLS. Une fois un utilisateur de confiance authentifié, le firewall a fait son travail.

COMMENT LES ATTAQUANTS CONTOURNENT

- Utilisent des protocoles autorisés (HTTPS, DNS, RDP) pour bouger sans être détectés.
- Opèrent sur des canaux chiffrés que les firewalls ne peuvent pas inspecter complètement.
- Exploitent les VPNs ou le SSO pour s'authentifier comme des utilisateurs de confiance.

Les firewalls ne détectent pas le C2 caché dans des protocoles approuvés, le mouvement latéral, ni les accès SaaS avec des identifiants valides.

IDPS : détecte les signatures, pas la furtivité.

La correspondance de signatures attrape les patterns connus, pas les attaquants sophistiqués.

Accès initial	●
Exécution	○
Persistance	○
Élévation de privilèges	○
Évasion des défenses	○
Accès aux identifiants	○
Découverte	◉
Mouvement latéral	◉
Collecte	○
Commande et contrôle	◉
Exfiltration	◉
Impact	○

VISIBILITÉ : ◉ Partielle ● Totale ○ Aucune

Les Intrusion Detection and Prevention Systems cherchent des patterns d'attaque connus. Les attaquants sophistiqués les utilisent rarement.

COMMENT LES ATTAQUANTS CONTOURNENT

- Charges personnalisées ou chiffrées qui échappent aux signatures.
- Living-off-the-land : outils et ports légitimes.
- Ralentissent l'activité pour passer sous les seuils.

Les IDPS échouent face aux techniques inédites et au mouvement est-ouest chiffré.

NAC : décide qui peut se connecter, pas ce qu'il fait ensuite.

Valide la posture de l'appareil et l'identité au moment de la connexion. Perd la visibilité une fois à l'intérieur.

Accès initial	●
Exécution	○
Persistance	○
Élévation de privilèges	○
Évasion des défenses	○
Accès aux identifiants	○
Découverte	○
Mouvement latéral	○
Collecte	○
Commande et contrôle	○
Exfiltration	○
Impact	○

VISIBILITÉ : ● Partielle ● Totale ○ Aucune

Les solutions Network Access Control valident la posture de l'appareil et l'identité avant d'accorder l'accès. Une fois l'utilisateur connecté, le NAC perd la visibilité.

COMMENT LES ATTAQUANTS CONTOURNENT

- Utilisent des charges personnalisées ou chiffrées qui échappent aux signatures.
- Vivent du terrain : outils et ports légitimes uniquement.
- Exploitent des appareils non gérés ou BYOD qui passent à travers les vérifications de posture.

Le NAC ne détecte ni le mouvement latéral, ni le trafic suspect, ni le comportement post-authentification.

SSE : le périmètre moderne, avec les vieux angles morts.

Le remplaçant du stack firewall + VPN historique.

Accès initial	●
Exécution	○
Persistance	○
Élévation de privilèges	○
Évasion des défenses	○
Accès aux identifiants	○
Découverte	○
Mouvement latéral	◉
Collecte	○
Commande et contrôle	◉
Exfiltration	◉
Impact	○

VISIBILITÉ : ◉ Partielle ● Totale ○ Aucune

Le Security Service Edge consolide secure web gateway, zero-trust network access, CASB et firewall-as-a-service en une plateforme cloud. Le SSE a remplacé le stack firewall + VPN historique dans beaucoup d'entreprises mais il hérite du même angle mort que tous les outils périmétriques ont toujours eu.

COMMENT LES ATTAQUANTS CONTOURNENT

- Détournent identifiants ou appareils de confiance pour passer sans alerte.. ZTNA approuve la connexion parce que l'identifiant est valide.
- Bougent entre systèmes de confiance, hors champ NAC.. Le SWG voit l'hôte de destination, pas l'activité malveillante dans la session.
- Exploitent appareils non gérés ou BYOD passant les contrôles de posture.
- Exfiltrent via des connexions SaaS-vers-SaaS sur lesquelles le SSE n'a aucune visibilité.

Le SSE remplace le firewall, pas la couche de détection manquante derrière.

Le même argument « Vectra comble l'angle mort » s'applique aux environnements protégés par SSE comme à ceux protégés par un firewall historique.

Le gap de la sécurité réseau et comment Vectra AI le comble.

LE GAP DE LA SÉCURITÉ RÉSEAU

Vos outils réseau actuels se concentrent sur la prévention et le contrôle, pas sur la détection.

Ils manquent :

- Mouvement latéral entre workloads et régions, cloud et hybride.
- Command-and-control sur protocoles chiffrés ou de confiance.
- Exfiltration déguisée en trafic métier.
- Anomalies est-ouest, accès privilégié, usage d'identifiants.
- Comportement post-authentification dans les sessions SSE.

CE QUE VECTRA AI APPORTE

- Analyse temps réel : on-prem, cloud, SaaS.
- Détecte mouvement latéral, élévation, exfiltration, (y compris en chiffré, par métadonnées).
- S'intègre avec SIEM et SOAR pour des alertes haute fidélité.
- S'intègre avec Splunk, Palo Alto, Juniper, Fortinet.

VECTRA

GARE À VOS GAPS

Sécurité des identités

L'angle mort de la sécurité réseau

IAM : bloque l'accès non autorisé, pas l'accès détourné.

Fondation du Zero Trust. Présume la confiance une fois entré.

Accès initial	●
Exécution	○
Persistance	○
Élévation de privilèges	●
Évasion des défenses	○
Accès aux identifiants	○
Découverte	○
Mouvement latéral	○
Collecte	○
Commande et contrôle	○
Exfiltration	○
Impact	○

VISIBILITÉ : ● Partielle ● Totale ○ Aucune

Les outils IAM contrôlent qui peut se connecter, depuis où, avec quelles permissions. Les IdP modernes ajoutent du risk-based (voyage impossible, identifiants ayant fuité, appareils inhabituels) mais ces signaux opèrent au moment de l'authentification. Une fois la session ouverte, l'IAM présume la confiance. Le MFA bloque plus de 99 % des attaques d'identité, et pourtant l'identité a bondi de 32 % au S1 2025[1] : tokens volés, OAuth consenti, device-code, AiTM contournent le MFA.

COMMENT LES ATTAQUANTS CONTOURNENT

- Volent des identifiants valides ou des tokens de session, puis se connectent comme un utilisateur légitime.
- Se déplacent latéralement avec des comptes sur-privilégiés ou des politiques mal configurées.
- S'authentifient via des fournisseurs d'identité de confiance, y compris des connexions fédérées et le SSO.
- Ciblent le cookie ESTSAUTHPERSISTENT et autres artefacts de session qui contournent entièrement le MFA.

L'IAM applique des politiques de connexion. Il ne surveille pas ce que font les identités après authentification.

97 % des attaques d'identité sont des attaques par mot de passe[1]. Le MFA stoppe l'attaque par mot de passe. Rien dans l'IAM ne stoppe l'abus post-authentification qui suit.

[1] Microsoft Digital Defense Report 2025 :

PAM : protège les comptes à privilèges, s'ils sont connus.

Restreint l'accès privilégié. Mais l'attaquant n'en a pas toujours besoin.

Accès initial	○
Exécution	○
Persistance	○
Élévation de privilèges	●
Évasion des défenses	○
Accès aux identifiants	◐
Découverte	○
Mouvement latéral	○
Collecte	○
Commande et contrôle	○
Exfiltration	○
Impact	○

VISIBILITÉ : ◐ Partielle ● Totale ○ Aucune

Les solutions PAM restreignent la manière dont les utilisateurs accèdent aux systèmes critiques : coffres de mots de passe, enregistrement de session, accès just-in-time. Mais les attaquants n'ont pas toujours besoin d'un compte à privilèges pour escalader.

COMMENT LES ATTAQUANTS CONTOURNENT

- Volent identifiants ou tokens de session, puis se connectent en utilisateur légitime.
- Bougent latéralement avec comptes sur-privilégiés ou politiques mal configurées.
- S'authentifient via fournisseurs d'identité de confiance, fédération et SSO inclus.(des rôles avec des privilèges effectifs mais non signalés comme « privilégiés »).

Le PAM ne détecte pas l'abus d'identité qui ne correspond pas aux périmètres de privilèges prédéfinis.

UEBA : calcule le risque, mais ne voit pas en temps réel.

De plus en plus une fonctionnalité dans le SIEM/XDR plutôt qu'une catégorie autonome.

Accès initial	●
Exécution	○
Persistance	●
Élévation de privilèges	●
Évasion des défenses	●
Accès aux identifiants	●
Découverte	●
Mouvement latéral	●
Collecte	○
Commande et contrôle	○
Exfiltration	●
Impact	○

VISIBILITÉ : ● Partielle ● Totale ○ Aucune

L'UEBA construit des profils de comportement normal et attribue des scores de risque quand les utilisateurs s'en écartent. Il dépend de données complètes et met souvent trop de temps à réagir. Gartner ne maintient plus de Magic Quadrant UEBA distinct.

COMMENT LES ATTAQUANTS CONTOURNENT

- Imitent un comportement utilisateur normal (même localisation, même appareil, même pattern d'accès).
- Agissent lentement ou en dehors des heures, en évitant les pics visibles.
- Exploitent des sources de logs incomplètes, empêchant l'UEBA d'avoir la vue d'ensemble.

L'UEBA retarde la détection et ne fournit pas de visibilité temps réel sur le mauvais usage de l'identité.

Le gap de sécurité de l'identité et comment Vectra AI le comble.

LE GAP DE LA SÉCURITÉ DE L'IDENTITÉ

La plupart des outils se concentrent sur le contrôle d'accès ou le scoring de risque, pas sur le comportement d'attaquant. L'ITDR est apparu pour observer ce que l'IAM ne voit pas.

Ils ne voient pas :

- Abus d'identifiants sur SaaS et cloud.
- Élévation de privilèges dans Entra ID ou Exchange Online.
- Abus de relations de confiance entre IdP.
- Mouvement latéral identitaire sans toucher l'endpoint.

CE QUE VECTRA APPORTE

- AD, Entra ID, M365 / Exchange Online, Azure / AWS, rôles IAM cloud, identité fédérée.
- Détection des abus de privilèges SaaS (délégation, OAuth).
- Détection de manipulation de fédération (trust, usurpation de rôle).
- Mauvais usage d'identifiants en hybride, , même MFA passé.

Pression réglementaire : la détection devient la preuve.

La conformité est continue, et la conformité continue exige une détection continue.

Les classeurs de politiques et les attestations annuelles ne satisfont pas une obligation de notification d'incident en 24 heures. Si votre stack ne voit pas l'attaque, aucun cadre de conformité ne corrige le problème.

NIS2 (UE)

En vigueur depuis octobre 2024

Exige des mesures techniques appropriées pour la détection et la réponse aux incidents. Impose le signalement des incidents significatifs dans les 24 heures suivant la prise de connaissance. L'article 21(2)(b) exige explicitement une capacité de gestion des incidents.

DORA (UE financier)

En vigueur depuis janvier 2025

Le chapitre II exige la résilience opérationnelle. Les fenêtres de signalement des incidents liés aux TIC sont courtes. Attendu : une preuve continue que la détection fonctionne, pas un audit ponctuel.

SEC Cyber Disclosure

En vigueur depuis décembre 2023

Les sociétés cotées doivent divulguer les incidents cyber matériels dans les quatre jours ouvrés suivant la détermination de la matérialité. Cela exige de comprendre ce que les attaquants ont fait (c.-à-d. une détection qui voit le comportement d'attaquant).

La question de la conformité est désormais une question de détection.

Conclusion

Comblez vos gaps avant qu'ils soient exploités.

On ne peut pas défendre ce qu'on ne peut pas voir.

Les attaquants d'aujourd'hui ne s'appuient pas sur le malware. Vos outils traditionnels n'ont pas été conçus pour ça.

Les attaquants exploitent des identifiants, tirent parti de misconfigurations SaaS, manipulent la confiance d'identité et se déplacent à travers les workloads cloud sans être vus.

Les outils traditionnels ne voient pas cette activité, non parce qu'ils sont défectueux, mais parce qu'ils n'ont pas été conçus pour ça.

- L'EDR ne voit pas l'abus d'identité dans M365.
- CASB et SASE ne voient pas le mouvement latéral cloud.
- Le SIEM n'alerte pas sur ce que l'amont ne voit pas.

Pendant ce temps, votre SOC se retrouve avec trop d'alertes, pas assez de contexte, et aucune visibilité réelle sur l'infrastructure hybride.

Comment Vectra AI complète votre stack.

Et ce que mesurent les clients qui le déploient. IDC Business Value Study, 2025.

CAPACITÉ DE SÉCURITÉ	CE QUI MANQUE	CE QUE VECTRA AI APPORTE
Détection des menaces sur l'endpoint	Aveugle au réseau et au cloud	Détection temps réel sur tout le trafic (sans agent)
Détection des menaces d'identité	Aucune visibilité post-authentification	Détecte le mauvais usage de comptes valides et l'élévation de privilèges
Visibilité sur les menaces cloud	Aveugle au comportement d'attaquants hybride	Détecte le mouvement cloud-natif, hybride, SASE, SaaS, IaaS
Détection du mouvement latéral	Invisible sur l'hybride	Détection temps réel du mouvement latéral
Réduction du bruit	Fatigue d'alertes	Clarté du signal pilotée par l'IA, détections haute fidélité

CE QUE VECTRA APPORTE, DE MANIÈRE MESURABLE — IDC 2025

391 %
ROI sur 3 ans

6 mois
de payback

3,4 M$
de bénéfice annuel

40 %
de SOC plus efficace

60 %
de temps en moins sur les alertes

69,4 %
de breaches en moins

99,9 %
de perte de productivité évitée

Source : IDC Business Value Study of Vectra AI, avril 2025

Vectra AI comble vos gaps de sécurité.

Observabilité. Signal. Contrôle. Et des résultats concrets, mesurés chez de vrais clients.

Observabilité

Vectra AI analyse en continu l'activité réseau pour révéler chaque identité, appareil et agent IA en temps réel, afin que les équipes SecOps sachent toujours qui fait quoi sur leur réseau.

Signal

En corrélant et en contextualisant l'activité dans les environnements hybrides, Vectra AI aide les équipes à prioriser le risque réel, investiguer plus vite, chasser avec confiance et stopper les attaques avant impact.

Contrôle

Vectra AI montre qui et quoi est sur votre réseau, quelle activité signale une attaque et où l'exposition évolue, pour que vous puissiez réduire le risque, gagner en efficacité et prouver la conformité.

TÉMOIGNAGE IDC · GROUPE COSMÉTIQUE INTERNATIONAL

« Avant Vectra AI, nous ne recevions aucune alerte et n'apprenions l'accès de la Red Team que par leurs rapports annuels, qui montraient systématiquement qu'ils avaient obtenu un accès domain admin et root. La première année avec Vectra, nous avons détecté, expulsé et complètement défait la Red Team. Vectra est mon outil de sécurité numéro un. »

La même équipe SOC fonctionne avec 7 équivalents temps plein (ETP). Leur référence dit qu'il en faudrait 14.

Télécharger le rapport

Auto-évaluation : quels sont vos gaps ?

Lisez chaque énoncé. Cochez la case si cela vous correspond. Les cases cochées représentent vos gaps.

GAP 1

Rien ne paraît anormal.

- [ ] Nous voyons PowerShell, RDP et WMI dans nos alertes EDR, et la plupart du temps nous supposons que c'est de l'activité d'admin.
- [ ] Nous n'avons pas de baseline documentée de ce à quoi ressemble un comportement d'admin « normal » dans notre environnement.
- [ ] Quand l'EDR signale un processus « potentiellement indésirable », des alertes restent parfois non revues plus d'une journée.
- [ ] Si un attaquant abusait de binaires signés et faisait du living off the land pendant deux semaines, nous ne sommes pas sûrs qu'on le remarquerait.
- [ ] Nos règles de détection ne distinguent pas de manière fiable les tâches planifiées créées par un attaquant des tâches légitimes.

GAP 2

L'authentification réussit.

- [ ] Le MFA est appliqué pour nos utilisateurs humains, mais nous sommes moins sûrs concernant les comptes de service et les workload identities.
- [ ] Notre principal signal de menace identité, c'est le score de risque de l'IdP (voyage impossible, appareil inhabituel).
- [ ] Nous n'ingérons pas les logs d'audit Microsoft 365, Entra ID ou Okta dans une couche de détection au-delà de l'IdP.
- [ ] Si un token de session était volé sur un appareil personnel infecté par un infostealer puis réutilisé, nous n'avons pas de détection spécifique.
- [ ] Quand un identifiant ou un facteur MFA est réinitialisé, rien ne surveille automatiquement le comportement du compte pendant les 24 heures suivantes.

GAP 3

Le mouvement est invisible.

- [ ] Notre détection réseau est uniquement nord-sud, nous ne voyons pas le trafic est-ouest entre workloads.
- [ ] Nous ne détectons pas de manière fiable le mouvement latéral SMB ou RDP entre segments quand la couverture EDR est inégale.
- [ ] Les appels API du plan de contrôle cloud (AWS STS assume-role, changements de rôles Entra ID) n'alimentent pas notre couche de détection en temps réel.
- [ ] Nous n'avons aucune détection pour les pivots d'apps OAuth entre plateformes SaaS sanctionnées.
- [ ] Quand nous citons le « dwell time » dans les rapports SOC, le chiffre vient d'une reconstruction post-incident, pas d'une mesure continue.

Comment lire votre score : 0–3 cochés = couverture significative. 4–7 cochés = l'angle mort vous expose de manière mesurable. 8–11 cochés = voie d'entrée principale des attaquants dans votre environnement. 12+ cochés = la détection est incomplète sur l'ensemble de la progression d'attaque.

À propos de Vectra AI

La plateforme Vectra AI protège les entreprises modernes en détectant et en stoppant les attaques sur le réseau, l'identité et le cloud, considérés comme une surface d'attaque unifiée. Elle combine la gestion de l'exposition aux menaces, la détection et la réponse pilotées par l'AI, et l'amélioration de la posture de sécurité pour réduire les risques avant le début des attaques et stopper les menaces en cours. Les équipes de sécurité obtiennent un signal clair, une réponse plus rapide et des améliorations mesurables en matière de résilience. Pour plus d'informations, rendez-vous sur www.vectra.ai.

VECTRA