

Défense d'Active Directory

Comment protéger l'un des
systèmes les plus critiques
et les plus ciblés au sein
des environnements actuels

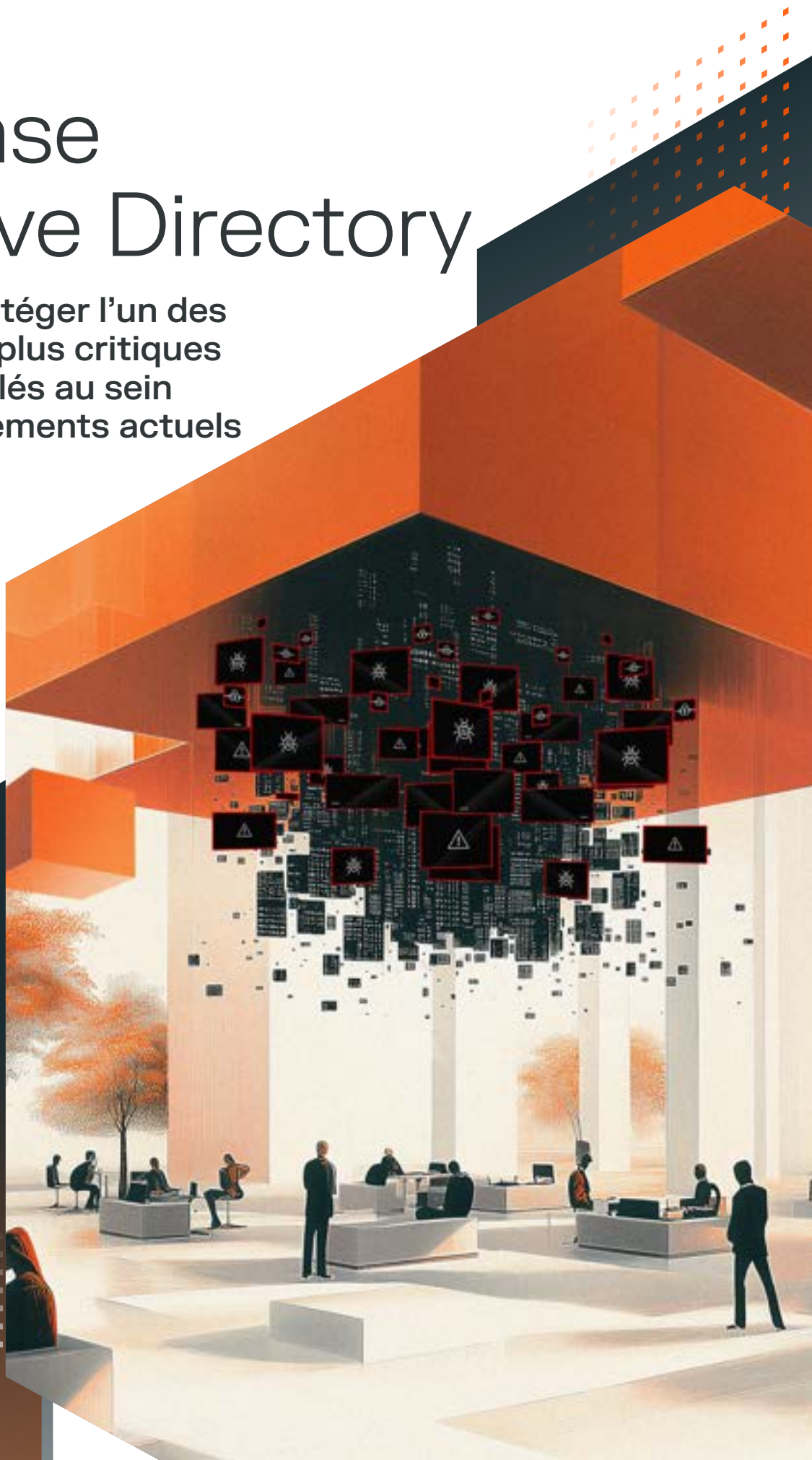


Table des matières

Un véritable enjeu de sécurité pour les environnements actuels	3
Une technologie héritée mais incontournable.....	3
Modèles d'identité hybrides.....	3
Contrôleurs de domaine : une voie royale vers le contrôle d'Active Directory.....	5
Compromissions réelles impliquant Active Directory.....	6
De la compromission au contrôle : déroulement des attaques.....	7
Exploitation des ressources locales (LOTL) : des attaques qui se fondent dans l'environnement.....	8
Compromission, élévation de privilèges, déplacement, et le cycle se répète.....	8
Gravité des menaces pour Active Directory.....	9
Les attaquants connaissent votre environnement, parfois mieux que vous.....	9
La plupart des outils de sécurité ne surveillent pas les bonnes activités.....	10
BloodHound : ce que les cybercriminels peuvent voir.....	10
Les pare-feux n'ont pas été pensés pour ce type de menace.....	11
Repenser les défenses : microsegmentation et contrôle des déplacements latéraux.....	12
Microsegmentation : confinement des attaques avant qu'elles n'atteignent Active Directory.....	13
Conclusion.....	14



Un véritable enjeu de sécurité pour les environnements actuels

Active Directory continue de jouer un rôle central dans la gestion des identités de la plupart des environnements. Il permet de déterminer les utilisateurs autorisés à se connecter, les systèmes auxquels ils ont accès, de même que les relations de confiance entre les utilisateurs, les appareils et les applications. Lorsque tout fonctionne, personne ne le remarque. Mais une compromission de ce service engendre un risque majeur pour les systèmes et données critiques.

Les cybercriminels en sont pleinement conscients, parfois davantage que certains responsables de la sécurité. Ils ne considèrent pas Active Directory comme une infrastructure, mais comme le chemin le plus rapide vers le contrôle total. Compromettre Active Directory permet à un acteur malveillant de se déplacer, d'élever ses privilèges, d'établir une persistance et de mener des activités illicites en toute impunité, des mois durant. Une simple intrusion peut donner lieu à un contrôle total sur le domaine.

Voilà pourquoi Active Directory demeure l'un des systèmes les plus ciblés des environnements actuels, et pourquoi sa défense exige une approche particulière. Active Directory est certes une technologie héritée, mais n'en reste pas moins incontournable.

Une technologie héritée mais incontournable

Des années après l'adoption massive du cloud et la modernisation des systèmes d'identité, Active Directory est toujours bien présent. Bon nombre d'entreprises en dépendent toujours pour la gestion des identités on-premise et pour la synchronisation des utilisateurs et groupes avec Microsoft Entra ID afin d'étendre l'accès au cloud.

Cette persistance d'une technologie relativement ancienne est souvent qualifiée de « dette héritée ». Dans la pratique, elle sous-tend le fonctionnement de l'entreprise.

Active Directory prend encore en charge des environnements locaux de grande envergure et des systèmes critiques qui reposent sur des protocoles d'authentification tels que Kerberos et NTLM. Ces dépendances s'expliquent par le nombre d'applications, d'infrastructures et de services accumulés par les entreprises au fil des années, voire des décennies. Et tous reposent sur une couche d'identités partagée.

Résoudre ces dépendances prend des années et s'accompagne d'un véritable risque opérationnel. En conséquence, même les entreprises très avancées dans l'adoption du cloud continuent d'utiliser Active Directory dans le cadre d'un modèle d'identité hybride.



Les cybercriminels y voient une parfaite opportunité : un système que les équipes de sécurité voudraient remplacer par une solution plus moderne, mais qui reste profondément intégré à l'environnement, étroitement connecté et bénéficiant d'une confiance généralisée. Une cible idéale, en somme.

Particulièrement dans les environnements où la stabilité prime sur la rapidité.

Modèles d'identité hybrides

De nombreuses entreprises dépendent toujours d'applications héritées, de règles strictes relatives aux données et de systèmes essentiels dont elles ne peuvent se passer. Parallèlement, l'identité connaît une évolution rapide. Même des erreurs minimes peuvent interrompre les processus indispensables à l'activité.

Un schéma familier se dessine : des services d'identité cloud tels que Microsoft Entra ID gèrent les applications SaaS et cloud de même que les utilisateurs distants, tandis qu'Active Directory continue de prendre en charge de nombreux systèmes, applications et flux d'authentification internes. Pour la plupart des entreprises, il s'agit d'une configuration à long terme et non d'une phase de transition.



L'identité hybride étend la portée et la flexibilité, mais elle conserve souvent les relations de confiance et les chemins d'accès existants. Le cloud prend de l'ampleur, le périmètre évolue. Pourtant, au sein de nombreux environnements, Active Directory continue de servir de point d'ancrage aux connexions et aux accès.

Ce modèle hybride n'est pas sans risques. Au fur et à mesure de la modernisation des entreprises, les chemins d'identité — relations, autorisations et modèles de confiance — sont souvent conservés, à moins d'une refonte délibérée. Dans de nombreux cas, Active Directory reste l'autorité de référence pour la gestion des identités et les relations de confiance. Or, tout élément jouant un rôle central dans le contrôle des accès devient une cible de grande valeur¹.

C'est précisément ces nouveaux modes d'accès associés à un système de confiance que les cybercriminels cherchent à exploiter.

Identité hybride avec authentification directe

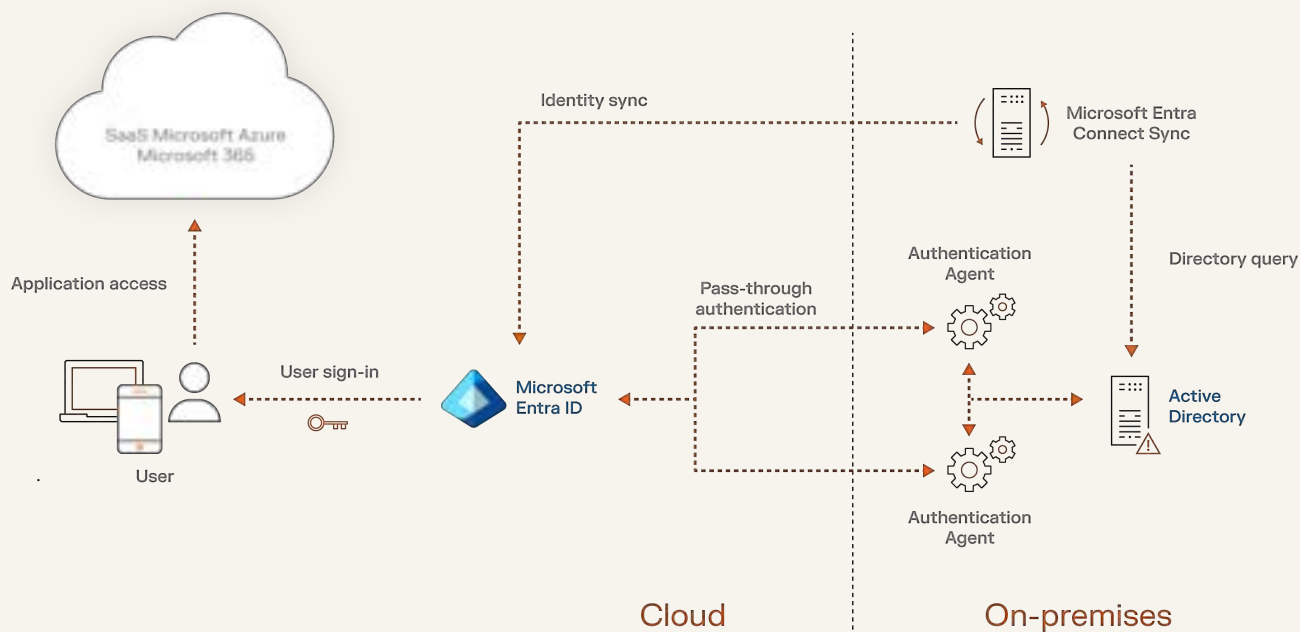


Figure 1. Les architectures d'identité hybrides étendent l'accès au cloud tout en continuant à s'appuyer sur Active Directory on-premise pour tout ce qui a trait à l'authentification de base et aux relations entre systèmes.

¹ <https://techcommunity.microsoft.com/t5/microsoft-security-blog/your-identity-infrastructure-is-your-security-boundary/ba-p/256344>



Contrôleurs de domaine : une voie royale vers le contrôle d'Active Directory

Bien qu'Active Directory et les contrôleurs de domaine soient des entités distinctes, ils sont inséparables dans la pratique. Active Directory définit les identités, les autorisations et les relations d'approbation au sein de l'environnement. Les contrôleurs de domaine, quant à eux, hébergent cet annuaire et appliquent ses stratégies, notamment pour le traitement de l'authentification, la validation des accès et la réplication des données d'identité.

Le but ultime des cybercriminels est de prendre le contrôle des identités, pas d'un seul système. Active Directory est l'objectif final, les contrôleurs de domaine sont le moyen d'y parvenir. La compromission d'un contrôleur de domaine permet de prendre le contrôle de l'annuaire.

La figure 2 illustre cette relation. Les contrôleurs de domaine sont au cœur de l'authentification et de l'application des stratégies. Les utilisateurs, les terminaux et les applications dépendent d'eux pour fonctionner. Ce rôle central est crucial, et c'est précisément ce qu'exploitent les cybercriminels.

Lorsque des acteurs malveillants se déplacent dans l'environnement, ils suivent les chemins d'approbation existants. Ces chemins conduisent aux contrôleurs de domaine, faisant de ces derniers des cibles logiques lors des déplacements latéraux².

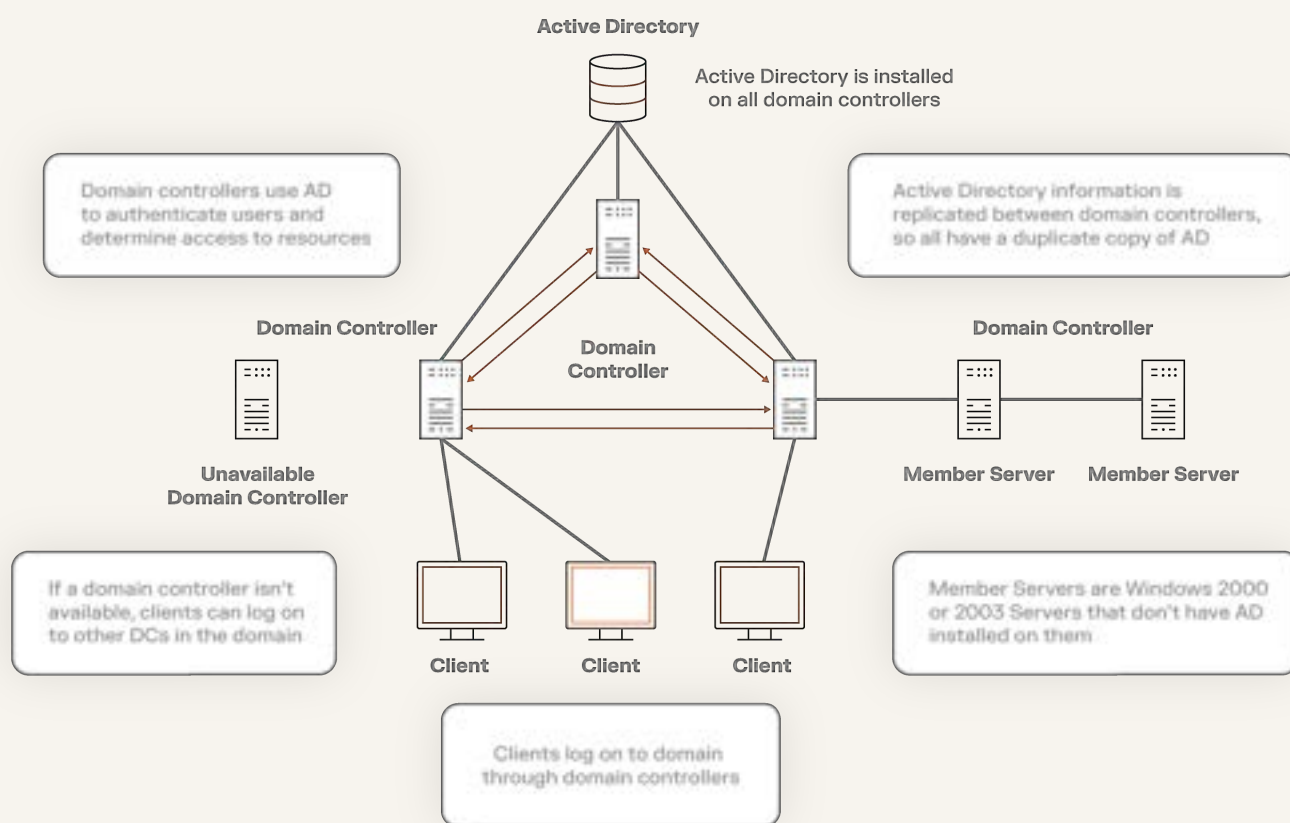


Figure 2. Modèle de connectivité des contrôleurs de domaine Active Directory

² https://www.sciencedirect.com/topics/computer-science/active-directory-user?__cf_chl_tk=I4eXbVwnEaTgiZ8x2cEkNln0KiP7fBWM3ImpHQlryJo-1777299782-1.0.1.1-L.ktuh6leFYCR7zZjQw9N58hT3ZUfUb10tDGFLY1alQ



Compromissions réelles impliquant Active Directory

Année	Incident	Description	Impact sur l'AD / les identités	Vecteur de l'attaque
2017	Ransomware WannaCry	Ransomware à propagation autonome exploitant SMB	Propagation sur des systèmes joints par des domaines	Les relations d'approbation AD ont accéléré la propagation du ransomware.
2017	Attaque NotPetya	Malware destructeur camouflé en ransomware	Collecte d'identifiants et déplacement latéral via des outils de domaine	Une instance AD non protégée a favorisé la propagation rapide et destructive du malware.
2020	Attaque de la chaîne logistique de SolarWinds	Espionnage grâce à des mises à jour Orion compromises	Exploitation de tokens AD FS et SAML pour établir une persistance	La compromission des identités a permis un accès échappant à toute détection.
2020	Ransomware Ryuk / Conti	Campagnes de ransomware opérées par des humains	Collecte d'identifiants de connexion et prise de contrôle de domaines avant le déploiement	Le contrôle des domaines a précédé l'impact du ransomware.
2021	Microsoft Exchange ProxyLogon	Exploitation de vulnérabilités Microsoft Exchange	Accès système et vol d'identifiants conduisant à une compromission d'Active Directory	Des points d'accès ont conduit à une prise de contrôle d'identités.
2022 – 2023	Ransomware BlackByte	Ciblage d'infrastructures critiques	Utilisation d'Active Directory à des fins de déplacement latéral et de persistance	Renforce le rôle de l'identité comme vecteur d'attaque.
2023	Ransomware LockBit	Opérations de ransomware à l'échelle mondiale	Énumération de domaines et compromission de contrôleurs de domaine	L'identité a été ciblée avant le déploiement du ransomware.
2023 (divulgaration)	Activités du groupe Volt Typhoon	Persistance d'acteurs étatiques dans l'infrastructure	Exploitation des ressources locales (Living off the Land) tirant parti des relations d'approbation AD	L'exploitation furtive des identités a entraîné une compromission de grande envergure.



De la compromission au contrôle : déroulement des attaques

La plupart des attaques débutent modestement : un e-mail de phishing, un mot de passe réutilisé, un seul terminal compromis. Lors de la compromission initiale, l'accès du cybercriminel est limité et il ne possède aucun privilège au niveau du domaine.

C'est à partir de ce point d'infiltration que l'attaquant mène ses activités de reconnaissance. Il recherche des ressources liées aux identifiants dans le système compromis : hachages de mots de passe, tickets Kerberos et tokens d'authentification laissés en mémoire par des sessions utilisateur actives. Des outils natifs ou des frameworks courants peuvent extraire ces artefacts à partir de processus tels que le service LSASS (Local Security Authority Subsystem Service). Une fois en possession de ces artefacts, le cybercriminel peut s'authentifier auprès d'autres systèmes en usurpant l'identité de l'utilisateur, sans jamais avoir à craquer un mot de passe. En effet, ces identifiants disposent déjà de la confiance de l'environnement. (Voir figure 3.)

Des techniques telles que Pass-the-Hash et Pass-the-Ticket permettent au cybercriminel de se déplacer latéralement en tant qu'utilisateur légitime. Chaque étape lui permet d'accéder à de nouveaux systèmes et de collecter d'autres identifiants, ce qui le rapproche des contrôleurs de domaine et du contrôle total de l'environnement.

Techniques utilisées après la compromission initiale

Technique	Description
Attaques Pass-The-Hash / Pass-the-Ticket	Réutilisation de données d'authentification volées afin d'obtenir un accès
Exploitation d'erreurs de configuration	Exploitation des configurations erronées pour élever les privilèges d'accès
Exploitation des ressources locales (LOTL)	Utilisation des outils déjà présents pour échapper à la détection
Collecte d'identifiants de connexion	Extraction d'identifiants à partir de la mémoire ou des systèmes
Détournement de sessions / Exploitation de tokens	Vol ou falsification de tokens pour accéder aux systèmes
Reniflage réseau	Capture du trafic réseau pour collecter des identifiants



Figure 3. Les cybercriminels progressent d'un seul utilisateur compromis à un accès administrateur de domaine en réutilisant des hachages et des identifiants volés. Ils peuvent ainsi se déplacer latéralement sans devoir craquer de mots de passe.



Exploitation des ressources locales (LOTL) : des attaques qui se fondent dans l'environnement

Une fois en possession d'identifiants, l'acteur malveillant n'a pas besoin de ses propres outils. Les outils déjà installés (PowerShell, PsExec, WMI, SMB, RDP, WinRM, SSH) suffisent amplement pour se déplacer d'un système à un autre, interroger l'environnement et prendre progressivement le contrôle du domaine³. Cette exploitation des ressources locales, en anglais « Living off the Land » (LOTL), constitue désormais une technique dominante. Ainsi, une analyse réalisée en 2025 par Bitdefender sur plus de 700 000 incidents a révélé que 84 % des compromissions majeures impliquaient des techniques LOTL⁴.

Leur efficacité tient au fait qu'elles demeurent invisibles à la plupart des systèmes de défense. En effet, quoi de plus normal qu'une activité exploitant les ressources locales. Celle-ci s'exécute en mémoire, se fond dans les opérations habituelles et laisse moins de traces que les attaques basées sur des malwares.

Souvent supérieure à 200 jours, la durée d'implantation permet aux cybercriminels d'élargir leur accès par la compromission d'un système à la fois — passant d'un terminal à un serveur, d'un serveur à l'infrastructure pour terminer par les contrôleurs de domaine⁵. Le cycle est identique à chaque étape (compromission, élévation des privilèges et déplacement), puis il se répète.

Dans les environnements Active Directory, ce cycle est rapide puisque l'environnement est, par nature, extrêmement connecté.

Compromission, élévation de privilèges, déplacement, et le cycle se répète

Le déplacement latéral se déroule en deux phases ; l'attaque est donc paralysée si l'une des deux phases échoue. Son efficacité tient au fait qu'il demeure invisible à la plupart des systèmes de défense. En effet, quoi de plus normal qu'une activité exploitant des ressources locales.

Au sein de l'hôte. Avant de se déplacer, les cybercriminels renforcent leur position au sein du système déjà compromis. Pour ce faire, ils extraient des identifiants, élèvent les privilèges et exécutent des outils en mémoire pour échapper à la détection. S'ils ne peuvent pas obtenir un accès administrateur ou des identifiants réutilisables, le déplacement s'arrête là.

Entre les hôtes. Une fois en possession d'identifiants, les attaquants se déplacent entre les systèmes à l'aide de protocoles déjà approuvés dans l'environnement : SMB, PsExec, RDP, WinRM ou SSH. Un système compromis entraîne la compromission de nombreux autres. Les acteurs malveillants se déplacent d'un terminal à un serveur, d'un serveur à l'infrastructure afin de se rapprocher progressivement des contrôleurs de domaine.

Les deux phases se répètent : compromission, élévation de privilèges, déplacement, et le cycle recommence. Chaque cycle étend l'accès et rapproche les cybercriminels d'un contrôle total, en utilisant l'environnement lui-même, mais jamais aucun exploit.

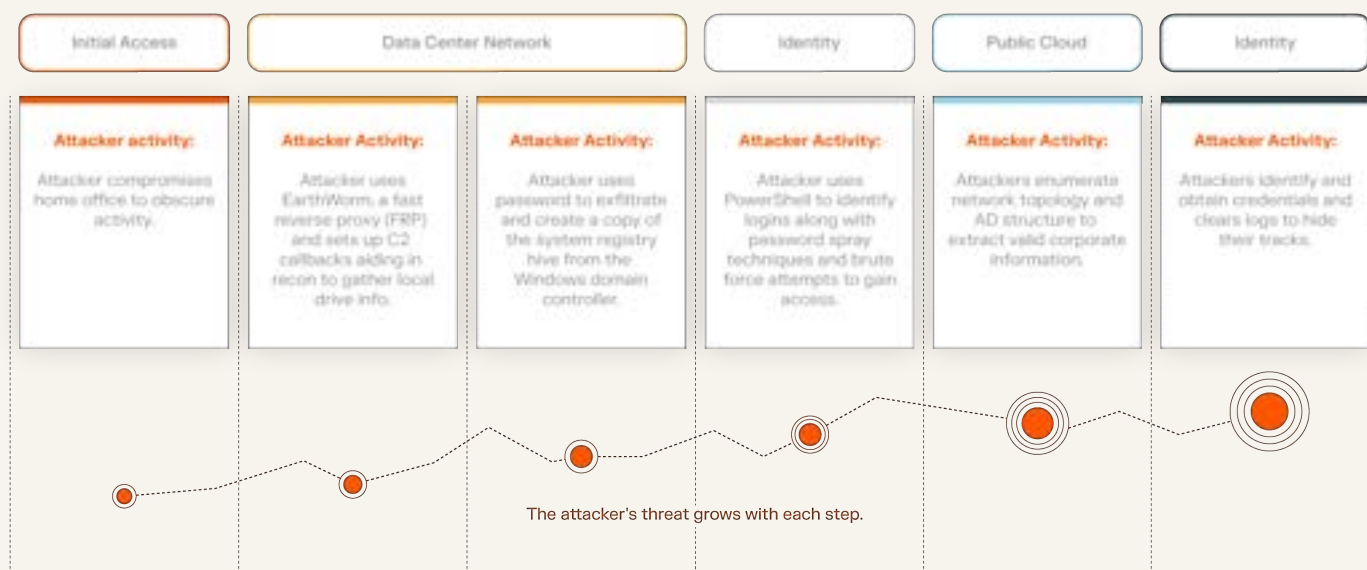


Figure 4. Simulation d'une attaque exploitant les ressources locales (LOTL) avec EarthWorm, un puissant outil open source de tunnellation en ligne de commande.

³ <https://www.illumio.com/fr/blog/modern-trojan-horse-how-attackers-live-off-the-land-and-how-to-stop-them>

⁴ Bitdefender. « 700,000 Security Incidents Analyzed: Living-off-the-Land Tactics ». Juin 2025.

⁵ IBM. « Cost of a Data Breach Report ». 2025.



Gravité des menaces pour Active Directory

La compromission d'un seul terminal permet d'obtenir un premier point d'ancrage. Prendre le contrôle d'Active Directory est le but ultime.

Une fois dans la place, les acteurs malveillants ne s'en remettent pas au hasard. Ils utilisent l'environnement lui-même pour progresser le plus rapidement possible et, dans la plupart des entreprises, cette voie rapide mène directement à Active Directory. Les cybercriminels tirent parti des outils déjà présents pour :

- Interroger AD afin de cartographier l'environnement
- Identifier les comptes à privilèges et les chemins d'accès
- Se rapprocher des contrôleurs de domaine
- Élever les privilèges d'accès sans déployer de malwares
- Atteindre les partages réseau et les systèmes de fichiers

Active Directory est l'élément qui leur permet d'atteindre tous ces objectifs. Il permet de mettre au jour la structure de domaines, les relations à privilèges ainsi que les informations qui aident à identifier les contrôleurs de domaine et à s'en rapprocher. Chaque étape s'appuie sur la précédente et toutes convergent vers la même cible : le contrôleur de domaine, au niveau duquel les stratégies d'identité sont appliquées et qui permet de prendre le contrôle de l'environnement.

L'attaque n'est pas complexe en soi. Elle fonctionne car l'environnement a été conçu pour assurer la connectivité et non le confinement.

Les attaquants connaissent votre environnement, parfois mieux que vous

Les acteurs malveillants n'avancent pas à tâtons dans Active Directory, ils le cartographient.

Avec les bons outils, ils peuvent analyser l'ensemble de l'environnement et identifier les relations importantes : qui a accès à quoi, quels sont les accès à privilèges et comment se déplacer entre les systèmes.

Leur examen met au jour ce que les équipes de sécurité ont rarement l'occasion de voir : le chemin le plus court vers la prise de contrôle. Pour les attaquants, la voie à suivre est claire. Pour les équipes de sécurité, c'est une inconnue. Elles envisagent leur rôle en termes d'événements. Les attaquants pensent en termes de relations.

De nombreuses entreprises ne bénéficient pas d'une telle visibilité. Elles s'appuient sur des journaux, des alertes et des données ponctuelles. Ces informations sont utiles, certes, mais incomplètes.

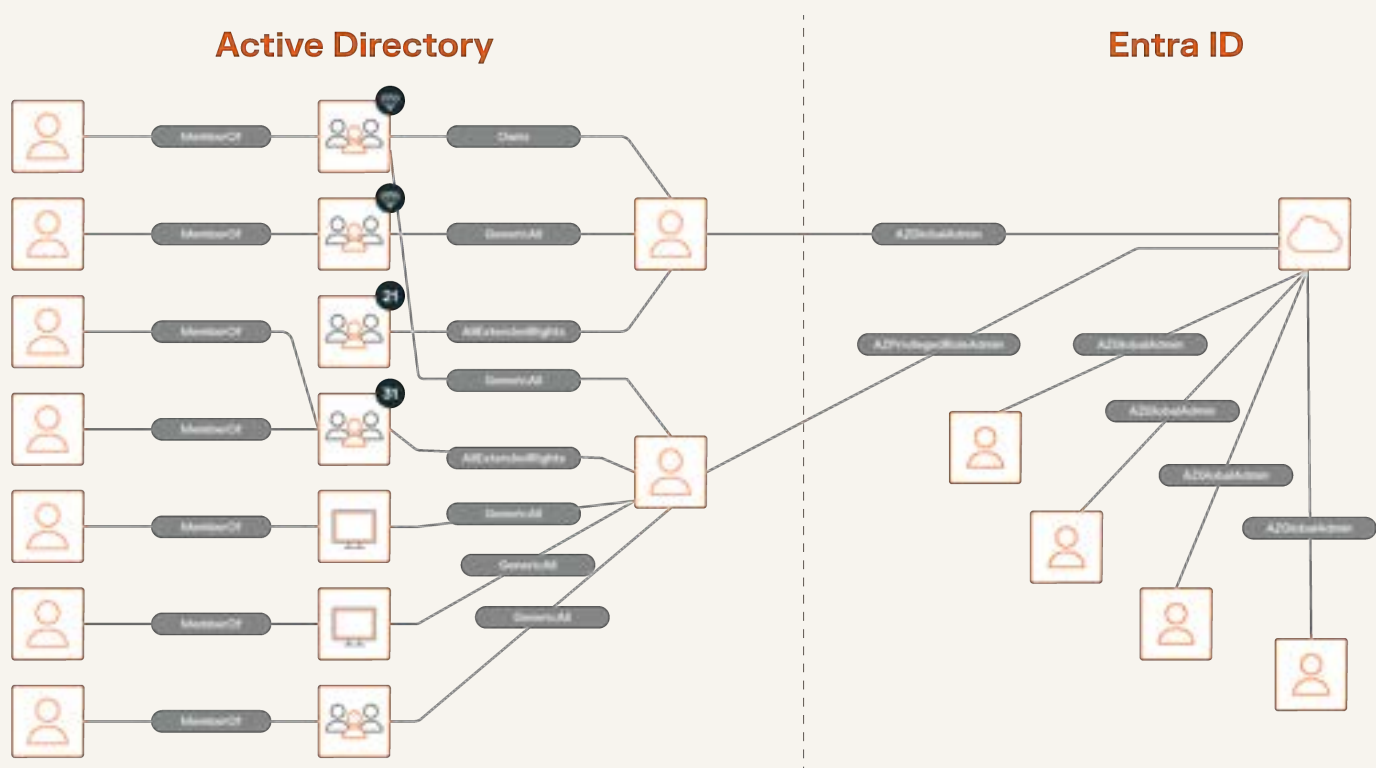


Figure 5. Des outils de modélisation de graphes d'attaque comme BloodHound cartographient les relations d'identité au sein d'Active Directory, mettant au jour des voies cachées pouvant mener à l'élévation des privilèges et au contrôle du domaine.



Outils utilisés par les attaquants pour cartographier l'environnement

Les acteurs malveillants ne progressent pas à l'aveugle. Ils emploient des outils spécialisés pour comprendre les identités, les accès et les relations :

- **BloodHound.** Cartographie les relations AD et les voies d'attaque.
- **SharpHound.** Utilisé avec BloodHound, collecte les données.
- **PingCastle.** Audite la posture de sécurité d'Active Directory et les risques d'exposition.
- **PowerView.** Énumère les domaines, les utilisateurs et les autorisations via PowerShell.
- **ADFind.** Interroge Active Directory pour identifier les objets et les relations.
- **CrackMapExec.** Automatise la validation des identifiants, l'exécution à distance et la découverte des déplacements latéraux.
- **Mimikatz.** Extrait les identifiants (mots de passe, hachages, tickets) et permet d'élever les privilèges.
- **Rubeus.** Exploite les tickets Kerberos (attaques Pass-the-Ticket, demandes de tickets).

La plupart des outils de sécurité ne surveillent pas les bonnes activités

Une fois les attaquants dans la place, les équipes de sécurité sont confrontées à un tout autre problème. La question n'est plus de savoir *comment une attaque se produit*, mais de disposer de la visibilité nécessaire pour *détecter l'attaque en cours et la bloquer*.

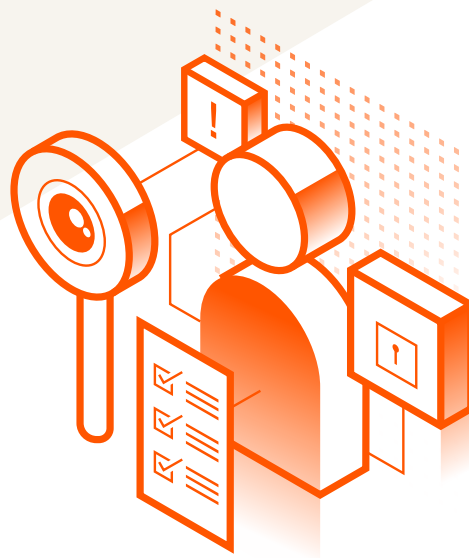
La plupart des environnements d'entreprise sont denses, avec des milliers de systèmes, d'identités et d'autorisations qui interagissent en temps réel. Les équipes de sécurité surveillent ces activités à l'aide de journaux et d'alertes qui capturent les événements (connexions, accès aux fichiers, exécution de processus), mais pas les relations entre eux.

C'est à ce niveau que la visibilité fait défaut. Sans une vue complète sur les communications entre les systèmes et les flux d'accès, les équipes peuvent voir chaque arbre, mais certainement pas la forêt.

Pour remédier à ce manque de visibilité, il faut aller au-delà des signaux isolés. Quatre capacités priment avant tout :

- **Visibilité sur les déplacements latéraux** pour voir les interconnexions entre les systèmes et les voies effectivement utilisées.
- **Contexte comportemental** pour distinguer les activités normales de celles présentant un risque.
- **Priorisation des risques** pour identifier les connexions et les voies d'accès les plus critiques en cas de compromission.
- **Confinement rapide** pour bloquer les communications ou isoler les systèmes en quelques minutes et non plusieurs heures.

Avec une telle visibilité, les activités intervenant dans l'environnement gagnent en lisibilité. Sans elle, les équipes de sécurité consultent le journal des événements d'une attaque qu'ils ne peuvent pas réellement voir.



BloodHound : ce que les cybercriminels peuvent voir

Les cybercriminels ont souvent une meilleure vue sur Active Directory que les équipes de sécurité, notamment grâce à des outils comme BloodHound.

Cet outil open source permet de cartographier les voies d'attaque ; il ingère les données d'Active Directory (utilisateurs, groupes, autorisations et systèmes), et révèle comment un attaquant pourrait combiner ces relations pour prendre le contrôle du domaine.

Le résultat : un graphe illustrant exactement comment un utilisateur doté de privilèges peu élevés peut progresser de son point de départ jusqu'au contrôle total du domaine.

Les cybercriminels appréhendent un environnement sous cet angle particulier ; non sous la forme de systèmes isolés, mais d'un graphe connecté représentant les accès et les privilèges.

Sans une telle visibilité, il serait difficile d'identifier :

- Les comptes obsolètes ou à privilèges excessifs
- Les relations d'approbation cachées
- Les voies indirectes vers les contrôleurs de domaine

Ce qui paraît sécurisé de prime abord ne l'est pas nécessairement. En effet, dès lors qu'une partie maîtrise l'environnement mieux que l'autre, le déplacement latéral devient vite inévitable.





Les pare-feux n'ont pas été pensés pour ce type de menace

Même quand les entreprises sont conscientes des risques, elles sont confrontées à un autre problème : les atténuer n'est pas simple.

Active Directory se caractérise par des communications constantes. Les contrôleurs de domaine utilisent à la fois des ports statiques et dynamiques. Dans une grande entreprise, l'allocation dynamique des ports et les communications constantes entre les systèmes peuvent se traduire par des millions de voies de communication possibles.

On ne parle pas ici de quelques points d'entrée, mais bien d'une multitude d'accès à une multitude de ressources : charges de travail, services, relations d'identité et ainsi de suite. Et chaque accès représente une voie qu'un cybercriminel peut emprunter une fois qu'il s'est introduit dans le système.

Les contrôles traditionnels n'ont pas été conçus pour une telle échelle. Les pare-feux ont besoin de règles statiques, alors qu'Active Directory repose sur des communications dynamiques. Face à ce décalage, la plupart des entreprises choisissent de maintenir le fonctionnement des systèmes, ce qui revient à autoriser un accès interne étendu. L'environnement reste opérationnel, mais présente alors une surface d'attaque énorme.

Il existe une autre facette au problème. Les équipes IT ne conçoivent pas un environnement à partir de rien, elles en héritent. Au fil des années, et parfois des décennies, les couches s'accumulent : de nouveaux systèmes viennent se greffer aux anciens, et des services modernes sont connectés à l'infrastructure héritée. Les cybercriminels n'ont pas besoin de cibler le système le plus récent. Ils peuvent s'infiltrer par un point quelconque, puis se déplacer vers un élément plus ancien, moins surveillé mais néanmoins connecté à Active Directory.

Le problème perdure, car l'environnement protégé par les équipes de sécurité a été conçu pour la connectivité et non le confinement.



Repenser les défenses : microsegmentation et contrôle des déplacements latéraux

Si empêcher l'accès ne suffit plus, la perspective doit changer et se concentrer sur le déplacement plutôt que sur l'accès. (Voir figure 6.)

Les approches de sécurité modernes reflètent ce changement de paradigme et s'appuient sur les principes suivants :

- Toujours supposer une compromission
- Établir une visibilité basée sur un graphe ou une carte
- Surveiller les relations entre les systèmes
- Confiner rapidement les menaces
- Limiter les privilèges

Une approche Zero Trust est nécessaire pour contrôler la façon dont les systèmes communiquent — et pas simplement bénéficier d'une visibilité sur les événements. (Voir figure 7.)

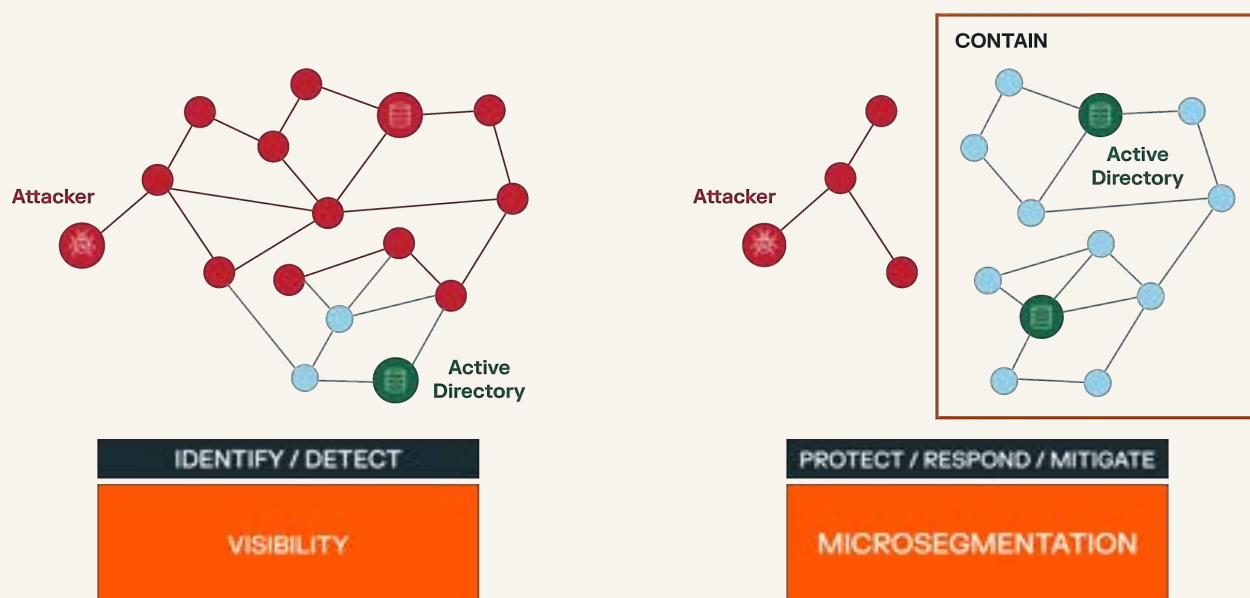


Figure 6. Une vue de l'environnement révèle les mouvements de l'attaquant, mais sans microsegmentation, il a toute liberté de se déplacer latéralement.





Figure 7. Conception du confinement à l'aide de la microsegmentation Zero Trust.

Le but n'est pas de remplacer complètement l'environnement, mais de contrôler la façon dont les systèmes se connectent. Lorsque les connexions sont sous contrôle, les possibilités de déplacement sont limitées. Et si les déplacements sont restreints, les attaques ne peuvent plus se propager.

Quand une compromission est en cours, les outils réactifs n'ont qu'une utilité limitée : les dommages se propagent plus vite que le temps nécessaire à l'investigation des alertes. Une visibilité continue permet aux équipes de sécurité de détecter les déplacements latéraux au moment où ils se produisent. Il s'agit ici d'identifier et de confiner les menaces en temps réel, afin de réduire le délai dont dispose le cybercriminel pour s'infiltrer plus avant dans votre réseau.

Microsegmentation : confinement des attaques avant qu'elles n'atteignent Active Directory

La phase initiale d'une compromission décide rarement de son résultat. C'est ce qui se passe ensuite qui est déterminant.

Un identifiant compromis ne provoque pas de dommages en soi, mais il offre une liberté de mouvement à l'origine de tous les soucis ultérieurs. Lorsque les acteurs malveillants peuvent se déplacer sans contrainte, l'environnement lui-même devient une arme ; s'ils sont bloqués, l'attaque est paralysée. C'est là toute la différence entre un incident mineur et une prise de contrôle totale du domaine.

Limitation de l'impact dès le départ

Les systèmes ne doivent pas tous nécessairement communiquer avec Active Directory. Toutefois, dans de nombreux environnements, les voies permettant d'atteindre Active Directory sont trop nombreuses pour que les équipes de sécurité puissent toutes les identifier ou les contrôler. C'est là qu'entre en jeu la microsegmentation. Elle limite les charges de travail autorisées à communiquer avec les contrôleurs de domaine, ainsi que les emplacements d'origine des communications. Même avec des

identifiants valides, un attaquant ne peut pas atteindre Active Directory par le biais d'une voie ou d'un système inattendus. La limitation des voies d'accès diminue l'exposition et donc l'impact.

Surveillance de l'utilisation réelle d'Active Directory

La plupart des attaques frappent sans sommation. Elles utilisent des identifiants et des protocoles de confiance, et peuvent donc échapper facilement à la vigilance des outils basés sur des signatures. C'est leur comportement qui les trahit, or celui-ci n'est significatif que si vous disposez d'une base de référence.

Pour comprendre la façon dont Active Directory est *normalement* utilisé, il faut pouvoir cartographier les systèmes interrogeant Active Directory, les emplacements à partir desquels les comptes s'authentifient, ainsi que les protocoles gérant le trafic légitime entre les différentes charges de travail. Toute cela n'est possible qu'avec une base de référence clairement établie. Sans elle, les anomalies n'ont rien d'anormal.

En revanche, grâce à elle, les déplacements des cybercriminels se détachent du lot, même s'ils utilisent des identifiants légitimes.

Détection des déplacements avant toute prise de contrôle

Un certain laps de temps s'écoule entre l'accès initial et la prise de contrôle totale du domaine. C'est au cours de cette période qu'il est possible de stopper les attaques, pour autant que vous puissiez les voir prendre forme.

Si vous avez établi une base de référence, certaines signatures spécifiques peuvent signaler un déplacement latéral en cours :

- Un système interrogeant Active Directory pour la toute première fois
- Une hausse subite des demandes d'authentification
- Un trafic RDP ou SMB entre des charges de travail n'ayant jamais communiqué auparavant
- Des schémas d'accès se rapprochant des contrôleurs de domaine



Ces signatures révèlent une attaque en cours de formation plutôt qu'une attaque terminée. Une détection précoce fait toute la différence entre le confinement d'une compromission et la gestion de ses conséquences.

Confinement immédiat

Une fois la menace confirmée, la rapidité l'emporte sur l'investigation. La priorité n'est pas d'arrêter les systèmes, mais de bloquer tout déplacement du cybercriminel. Isoler une charge de travail compromise au niveau du réseau bloque instantanément son accès au reste de l'environnement, sans perturber les activités. La compromission est confinée, quel que soit le stade de la chaîne d'attaque auquel elle est détectée — avant la propagation des identifiants, avant l'interrogation des contrôleurs de domaine et, surtout, avant l'objectif final de prise de contrôle d'Active Directory.

Conclusion

Bloquer chaque point d'accès n'est pas une perspective réaliste. Les acteurs malveillants trouveront toujours le moyen de s'infiltrer, que ce soit au travers d'un e-mail de phishing, d'un mot de passe volé ou d'un serveur dépourvu de correctifs. Ce point n'est plus à débattre.

L'important est de savoir ce qui se passera ensuite. Une compromission qui atteint Active Directory peut déboucher sur une prise de contrôle totale du domaine. Une compromission bloquée dès la première charge de travail reste une compromission. La maîtrise des déplacements latéraux au sein de l'environnement sera le facteur déterminant.

Confiner les compromissions avant qu'elles n'atteignent Active Directory relève de la discipline opérationnelle, et non de la démarche théorique. C'est ce qui ramène une catastrophe potentielle au rang d'incident gérable.

Vous ne pouvez pas bloquer chaque compromission, mais vous pouvez éviter les catastrophes.

Découvrez comment Illumio bloque les menaces ciblant Active Directory avant qu'elles ne se propagent.

Essayez Illumio Segmentation dès aujourd'hui.

