AYI NEDJIMI Consultants

Détection du Mouvement Latéral : Guide Complet SOC 2026

Catégorie : SOC et Detection Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide expert sur la détection du mouvement latéral dans le SOC : techniques Pass-the-Hash, RDP, SMB, WMI et règles SIEM pour identifier la.

Résumé exécutif

Ce guide couvre les techniques de détection du mouvement latéral dans un SOC : identification des protocoles exploités par les attaquants (RDP, SMB, WMI, PsExec, PowerShell Remoting), règles de détection SIEM et NDR, et méthodologie d'investigation pour tracer la progression d'un adversaire dans le réseau interne de votre organisation. Le mouvement latéral est la phase la plus critique et la plus difficile à détecter de la kill chain, car les attaquants utilisent des protocoles d'administration légitimes pour se déplacer entre les systèmes compromis sans déclencher d'alertes classiques. Nous détaillons les stratégies de corrélation cross-source, l'analyse comportementale du trafic réseau et les Event IDs Windows indispensables pour construire des détections efficaces qui distinguent l'activité administrative normale de la progression furtive d'un attaquant sophistiqué à travers votre infrastructure.

Le **mouvement latéral** représente l'une des phases les plus critiques et les plus difficiles à détecter dans la kill chain d'une attaque. C'est durant cette phase que l'attaquant, ayant obtenu un premier point d'entrée, se propage à travers le réseau pour atteindre ses objectifs : accès aux données sensibles, contrôleurs de domaine, serveurs critiques. En 2026, les techniques de mouvement latéral se sont considérablement sophistiquées, exploitant des protocoles légitimes d'administration et des outils natifs du système d'exploitation pour se fondre dans le trafic normal. Les attaquants modernes n'utilisent plus des malwares facilement détectables pour se déplacer : ils réutilisent les identifiants volés, exploitent les relations de confiance entre systèmes et abusent des fonctionnalités d'administration à distance comme RDP, WMI, PowerShell Remoting et SMB. Cette utilisation de *Living off the Land* rend la détection particulièrement complexe car chaque action individuelle est techniquement légitime. C'est la corrélation de multiples signaux faibles et l'analyse comportementale qui permettent de distinguer un administrateur légitime d'un attaquant. Ce guide vous fournit les clés techniques et méthodologiques pour construire des détections efficaces du mouvement latéral dans votre SOC, en combinant les capacités du SIEM, du NDR et de l'EDR pour une couverture maximale de cette menace critique.

Retour d'expérience : L'implémentation de 12 règles de détection du mouvement latéral dans un SOC bancaire a permis d'identifier en 3 mois deux compromissions actives non détectées par les solutions EDR. Dans le premier cas, un attaquant utilisait des connexions RDP entre postes de travail avec des credentials volées depuis 6 semaines. Dans le second, un mouvement via WMI entre serveurs exploitait un compte de service dont le mot de passe n'avait pas été changé depuis 3 ans.

La détection du mouvement latéral par le **SIEM** repose sur plusieurs stratégies complémentaires. La première est la détection de **connexions anormales entre systèmes**. Établissez une baseline des connexions réseau normales (quel système se connecte à quel système, via quel protocole, à quelle fréquence) et détectez les écarts significatifs. Les connexions RDP ou SMB entre deux postes de travail qui n'ont jamais communiqué auparavant sont un signal fort de mouvement latéral. Cette approche nécessite des données de flux réseau (NetFlow, Zeek) ou des logs de pare-feu interne. La deuxième stratégie est la détection d'**authentifications suspectes**. Cherchez les patterns suivants dans les logs Security des contrôleurs de domaine et des endpoints : un même compte s'authentifiant sur un nombre inhabituel de machines dans un court laps de temps, des authentifications de type NTLM (Event ID 4624, Logon Type 3) depuis des sources inhabituelles, des authentifications avec des comptes de service depuis des postes de travail, et des authentifications administratives hors heures ouvrées.

La troisième stratégie est la détection de **création de services à distance** (Event ID 7045 sur la machine cible), caractéristique de PsExec et outils similaires. Filtrez les services créés avec des noms aléatoires ou des binaires exécutés depuis des répertoires temporaires. La quatrième stratégie est la détection de **processus suspects créés à distance** via WMI (Event ID 1 de Sysmon avec WmiPrvSE.exe comme parent process) ou via PowerShell Remoting (wsmprovhost.exe comme parent process). La cinquième stratégie est la *corrélation temporelle* : un mouvement latéral se traduit par une séquence d'événements sur plusieurs machines dans un intervalle court. Utilisez les capacités de corrélation de votre SIEM pour détecter des séquences comme : authentification réussie sur machine A, suivie dans les minutes suivantes d'une authentification du même compte sur machine B, puis sur machine C. Cette accélération des connexions est un indicateur fort de progression latérale. Consultez les règles de détection disponibles dans le standard Sigma pour des exemples concrets implémentables dans Splunk, Sentinel ou Elastic.

Technique	Protocole	Source de détection	Event IDs clés	Difficulté détection
Pass-the-Hash	NTLM/SMB	Security logs DC	4624 (Type 3), 4776	Élevée
Pass-the-Ticket	Kerberos	Security logs DC	4768, 4769, 4771	Élevée
PsExec	SMB	Security + System cible	7045, 4624, 5145	Moyenne
RDP latéral	RDP (3389)	Security + TermServ	4624 (Type 10), 1149	Moyenne
WMI à distance	DCOM/RPC	Sysmon + Security	Sysmon 1, 4624	Élevée
PowerShell Remoting	WinRM (5985/6)	PowerShell + Security	4103, 4104, 4624	Moyenne

Le rôle du NDR dans la détection latérale

Le **NDR (Network Detection and Response)** apporte une dimension complémentaire essentielle à la détection du mouvement latéral. Là où le SIEM dépend des logs générés par les systèmes (qui peuvent être désactivés ou manipulés par un attaquant avancé), le NDR analyse le **trafic réseau brut** et détecte les anomalies comportementales indépendamment de la coopération des endpoints. Le NDR excelle dans la détection de patterns de trafic anormaux : un poste de travail qui scanne méthodiquement un sous-réseau, des connexions SMB vers des partages administratifs (C$, ADMIN$) depuis des sources inhabituelles, du trafic RDP interne entre systèmes qui ne communiquent normalement jamais, ou des volumes de données transférés entre systèmes internes excédant les baselines historiques. Les solutions NDR modernes comme Darktrace, Vectra et Corelight utilisent des algorithmes de *machine learning non supervisé* pour modéliser le comportement normal de chaque système et détecter les écarts sans nécessiter de signatures ou de règles manuelles.

L'intégration NDR-SIEM est particulièrement puissante pour la détection du mouvement latéral. Le NDR détecte les **anomalies de trafic** et le SIEM les corrèle avec les **événements d'authentification**, permettant de transformer un signal faible (connexion SMB inhabituelle) en un incident de haute confiance (connexion SMB inhabituelle + authentification avec un compte compromis + horaire anormal). Pour les organisations qui ne peuvent pas investir dans un NDR commercial, le déploiement de **Zeek** (ex-Bro) en open source sur des points stratégiques du réseau fournit une visibilité réseau précieuse à moindre coût. Les logs Zeek ingérés dans le SIEM permettent des détections basées sur les métadonnées de connexion sans nécessiter de deep packet inspection. Pour comprendre les techniques de communication furtive que le NDR doit détecter, consultez notre article sur l'exfiltration DNS/DoH.

Pourquoi le mouvement latéral est-il si difficile à détecter ?

La difficulté de détection du mouvement latéral tient à plusieurs facteurs fondamentaux. Le premier est l'**utilisation de protocoles légitimes** : RDP, SMB, WMI et PowerShell Remoting sont des outils d'administration normaux utilisés quotidiennement par les équipes IT. Distinguer un administrateur légitime qui se connecte à distance d'un attaquant utilisant les mêmes outils avec des credentials volées est un défi analytique majeur. Le deuxième facteur est le **volume de trafic** : dans un réseau d'entreprise de 10 000 postes, des millions d'événements d'authentification sont générés chaque jour, et le mouvement latéral ne représente qu'une infime fraction de ce volume. Le troisième facteur est l'**absence de signature unique** : contrairement à un malware qui peut être identifié par son hash, le mouvement latéral ne laisse que des traces comportementales subtiles qui varient selon le contexte. Le quatrième facteur est la **capacité d'adaptation des attaquants** : les attaquants avancés connaissent les détections déployées et adaptent leurs techniques en conséquence, utilisant par exemple des protocoles moins surveillés ou opérant pendant les heures de forte activité pour se fondre dans le bruit. Consultez notre article sur les relais NTLM pour comprendre une technique spécifique de mouvement latéral particulièrement furtive.

Mon avis : La détection du mouvement latéral est le véritable test de maturité d'un SOC. Les SOC qui ne détectent que les attaques bruyantes (phishing, brute force, malware connu) passent à côté des compromissions les plus graves. Investissez dans la corrélation cross-source (SIEM + NDR + EDR), déployez Sysmon sur vos endpoints et formez vos analystes à reconnaître les patterns de mouvement latéral. C'est là que se joue la différence entre un SOC qui détecte les scripts kiddies et un SOC qui détecte les APT.

Quelles sont les sources de données indispensables ?

La détection efficace du mouvement latéral nécessite un ensemble spécifique de **sources de données** correctement configurées. Les **logs Security des contrôleurs de domaine** sont la source la plus critique, fournissant les événements d'authentification Kerberos et NTLM pour l'ensemble du domaine. Assurez-vous que la politique d'audit capture les événements de logon/logoff (Event IDs 4624, 4625, 4634), les authentifications Kerberos (4768, 4769, 4771) et les accès aux objets sensibles (4662). Les **logs Sysmon** sur les endpoints sont essentiels pour la détection de processus suspects : création de processus avec filiation (Event ID 1), connexions réseau (Event ID 3), et accès à la mémoire de lsass.exe (Event ID 10, indicateur de credential dumping précédant le mouvement latéral). Les **logs de pare-feu interne** ou de microsegmentation fournissent la visibilité sur les flux est-ouest entre systèmes. Les **données NDR** (Zeek, Suricata ou solutions commerciales) enrichissent l'analyse avec les métadonnées protocolaires et les anomalies de trafic. Consultez notre guide forensics Windows pour les détails sur la configuration optimale de ces sources et référez-vous aux guides de l'ANSSI pour les politiques d'audit recommandées.

Méthodologie d'investigation du mouvement latéral

Quand un **mouvement latéral** est suspecté, l'investigation doit suivre une méthodologie structurée. L'**étape 1** est l'identification du patient zéro : à partir de l'alerte initiale, remontez la chaîne d'authentification pour identifier le premier système compromis. Cherchez l'événement d'authentification le plus ancien impliquant le compte suspect. L'**étape 2** est la cartographie de la propagation : identifiez tous les systèmes auxquels le compte compromis s'est connecté depuis la compromission initiale. Utilisez les logs d'authentification du SIEM pour tracer les connexions successives et construire un graphe de propagation. L'**étape 3** est l'évaluation de l'impact : pour chaque système touché, déterminez les actions effectuées par l'attaquant (exfiltration de données, installation de persistence, escalade de privilèges). L'**étape 4** est le confinement : isolez simultanément tous les systèmes compromis identifiés pour empêcher toute propagation supplémentaire, et révoquez les credentials compromises. L'*étape 5* est la remédiation : réinitialisez les mots de passe des comptes compromis, nettoyez les mécanismes de persistence installés et restaurez les systèmes à un état sain. Consultez notre article sur les attaques Golden Ticket pour les cas où le mouvement latéral a atteint les contrôleurs de domaine.

À retenir : La détection du mouvement latéral nécessite une approche multi-source combinant SIEM (logs d'authentification et de services), NDR (anomalies de trafic réseau) et EDR (processus suspects). Les signaux clés sont les connexions inhabituelles entre systèmes, les authentifications anormales et les créations de services à distance. La corrélation temporelle de ces signaux faibles est la clé pour identifier la progression d'un attaquant dans le réseau.

Si un attaquant volait aujourd'hui les credentials d'un administrateur de votre domaine, combien de temps votre SOC mettrait-il à détecter ses déplacements dans le réseau ?

Sources et références : MITRE ATT&CK · MITRE CAR

Perspectives et prochaines étapes

La détection du mouvement latéral va évoluer vers des approches de plus en plus basées sur l'analyse comportementale et le machine learning, capables de modéliser les patterns de communication normaux de chaque utilisateur et système pour détecter les écarts en temps réel. La microsegmentation réseau va progressivement limiter les possibilités de mouvement latéral en appliquant le principe du moindre privilège au niveau réseau. Pour améliorer vos capacités dès maintenant, déployez les 6 règles de détection décrites dans ce guide, activez les logs Sysmon sur vos endpoints critiques et conduisez un exercice de purple team ciblé sur le mouvement latéral pour valider l'efficacité de vos détections.

FAQ

Qu'est-ce que Détection du Mouvement Latéral ?

Le concept de Détection du Mouvement Latéral est détaillé dans les premières sections de cet article, qui couvrent les fondamentaux, les enjeux et le contexte opérationnel. Pour un accompagnement sur ce sujet, contactez nos experts.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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