AYI NEDJIMI Consultants

Use Cases SIEM : 50 Règles Détection Essentielles : Gui

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

Découvrez 50 règles de détection SIEM essentielles classées par tactique MITRE ATT&CK : cas d'usage concrets pour Splunk, Sentinel et Elastic.

Résumé exécutif

Ce guide présente 50 règles de détection SIEM indispensables classées par tactique MITRE ATT&CK, avec leur logique de détection, les sources de données requises et des conseils d'implémentation pour Splunk, Sentinel et Elastic Security. Les équipes de sécurité opérationnelle font face à des défis croissants : multiplication des surfaces d'attaque, sophistication des menaces persistantes avancées, et volumes de données qui dépassent les capacités d'analyse humaine. Dans ce contexte, une approche structurée et outillée devient indispensable pour maintenir une posture défensive efficace. Cet article propose une analyse technique approfondie, enrichie de retours d'expérience terrain et de recommandations concrètes pour les professionnels confrontés à ces enjeux au quotidien. Les architectures, méthodologies et outils présentés ici reflètent les pratiques observées dans les environnements de production les plus exigeants.

La qualité d'un **SIEM** se mesure avant tout à la pertinence de ses règles de détection. Un SIEM doté de milliers de règles génériques qui génèrent un tsunami de faux positifs est moins utile qu'un SIEM configuré avec 50 règles soigneusement sélectionnées, calibrées et maintenues qui détectent réellement les menaces pertinentes pour l'organisation. En 2026, le framework MITRE ATT&CK s'est imposé comme le référentiel universel pour structurer les capacités de détection d'un SOC. Mapper ses règles SIEM aux tactiques et techniques ATT&CK permet d'identifier les angles morts de détection et de prioriser les développements en fonction du paysage de menaces spécifique à son secteur d'activité. Ce guide présente 50 cas d'usage de détection essentiels, organisés par tactique ATT&CK, que tout SOC devrait implémenter comme socle minimal de détection. Pour chaque cas d'usage, nous détaillons la logique de détection, les sources de données nécessaires, les pièges à éviter et des conseils d'implémentation concrets applicables aux trois SIEM leaders du marché. L'objectif n'est pas l'exhaustivité mais la pertinence : ces 50 règles couvrent les techniques d'attaque les plus fréquemment observées dans les incidents réels et constituent le minimum vital d'un programme de détection efficace.

Retour d'expérience : L'implémentation structurée de 50 use cases SIEM alignés MITRE ATT&CK pour un SOC sectoriel santé a permis de passer d'une couverture de 12% des techniques ATT&CK pertinentes à 67% en 6 mois. Sur cette période, 8 incidents de sécurité confirmés ont été détectés par les nouvelles règles, dont 3 auraient été manqués avec l'ancienne configuration. Le taux de faux positifs a été maintenu sous 15% grâce à un tuning systématique post-déploiement.

Initial Access et Execution : détecter l'intrusion

Les tactiques **Initial Access** et **Execution** couvrent les premières étapes d'une attaque, où l'adversaire obtient un point d'entrée et exécute du code malveillant. Les règles de détection prioritaires pour Initial Access incluent la détection de **connexions depuis des pays inhabituels** (géolocalisation des IP d'authentification et comparaison avec le profil historique de l'utilisateur), la détection d'**authentifications par brute force** (seuil de tentatives échouées par compte ou par IP source dans une fenêtre temporelle), la détection d'**emails de phishing** contenant des pièces jointes suspectes ou des URL vers des domaines récemment enregistrés, et la détection d'**accès VPN depuis des IP de proxy ou VPN publics** qui peuvent indiquer l'utilisation de credentials volées. Pour l'Execution, les règles essentielles couvrent la détection d'**exécution PowerShell encodée en Base64** (indicateur classique de scripts malveillants), la détection de **processus enfants inhabituels** de Microsoft Office (Word lançant PowerShell ou cmd.exe), la détection d'utilisation de *Living off the Land Binaries* (LOLBins) comme certutil, mshta, regsvr32 et la détection de **scripts WMI ou scheduled tasks** créés à distance. Pour approfondir les techniques d'exécution furtive, consultez notre article sur les techniques Living off the Land.

Persistence et Privilege Escalation : détecter le maintien

Les tactiques de **Persistence** et **Privilege Escalation** sont critiques car elles indiquent qu'un attaquant cherche à maintenir son accès et à élever ses privilèges, signes d'une compromission active nécessitant une réponse urgente. Pour la Persistence, les règles essentielles incluent la détection de **création de comptes locaux ou domaine** non autorisée, la détection de **modification des clés de registre de démarrage automatique** (Run, RunOnce, services), la détection d'**ajout de tâches planifiées** suspectes (TaskScheduler Event ID 106 ou Sysmon Event ID 1 avec schtasks.exe), la détection de **modification des GPO** (Group Policy Objects) et la détection de **création ou modification de comptes de service** avec des SPN (Service Principal Names) inhabituels, indicateur potentiel de préparation au Kerberoasting. Pour approfondir cette technique, consultez notre article sur l'exploitation Kerberos.

Pour la **Privilege Escalation**, les règles prioritaires couvrent la détection de *DCSync* (réplication Active Directory depuis un poste non-contrôleur de domaine, Event ID 4662 avec GUID spécifiques), la détection d'**ajout de membres aux groupes à hauts privilèges** (Domain Admins, Enterprise Admins, Schema Admins, Event ID 4728/4732/4756), la détection de **modification des permissions DACL** sur des objets AD sensibles, la détection d'**exploitation de certificats** via ADCS (demandes de certificats avec des templates vulnérables) et la détection de **token impersonation** via des processus à privilèges élevés. Chacune de ces règles nécessite des sources de données spécifiques : les logs Security des contrôleurs de domaine sont indispensables pour la détection AD, tandis que les logs Sysmon ou EDR sont nécessaires pour la détection de manipulation de tokens. Consultez nos articles sur le DCSync et les attaques ADCS pour les détails techniques de ces détections.

Tactique ATT&CK	Nombre de règles recommandées	Sources critiques	Priorité
Initial Access	6-8 règles	Proxy, Email, VPN, Azure AD	Haute
Execution	5-7 règles	Sysmon, EDR, PowerShell logs	Haute
Persistence	6-8 règles	AD Security, Sysmon, EDR	Critique
Privilege Escalation	5-7 règles	AD Security, Sysmon, ADCS	Critique
Defense Evasion	5-6 règles	Sysmon, EDR, AV logs	Haute
Lateral Movement	5-7 règles	AD Security, NDR, Firewall	Critique
Collection/Exfiltration	4-5 règles	Proxy, DNS, DLP, NDR	Haute
Command and Control	4-5 règles	Proxy, DNS, NDR	Haute

Lateral Movement et Exfiltration : détecter la progression

La détection du **mouvement latéral** est souvent le maillon faible des SOC car elle requiert une corrélation cross-source sophistiquée. Les règles essentielles incluent la détection de **connexions RDP ou SMB anormales** entre postes de travail (les postes de travail ne devraient normalement pas se connecter entre eux), la détection d'**utilisation de PsExec ou d'outils similaires** (services créés à distance avec des noms caractéristiques), la détection de **Pass-the-Hash et Pass-the-Ticket** (authentifications NTLM de type 3 depuis des sources inhabituelles, utilisation de tickets Kerberos forgés), la détection d'**accès administratif à distance** via WMI ou WinRM depuis des postes non autorisés, et la détection d'**exploitation de protocoles de partage de fichiers** pour accéder à des partages sensibles. Pour l'**exfiltration**, les règles prioritaires couvrent la détection de **volumes de données sortants anormaux** vers des destinations externes (baseline du trafic normal par utilisateur ou par système), la détection d'**exfiltration via DNS** (requêtes DNS vers des domaines à haute entropie ou avec des sous-domaines anormalement longs), la détection d'**upload vers des services de stockage cloud** non autorisés (shadow IT) et la détection d'**utilisation de protocoles de tunneling** (ICMP tunneling, DNS over HTTPS vers des résolveurs non approuvés). Consultez notre article dédié sur l'exfiltration DNS et DoH et notre guide sur les attaques Silver Ticket pour des règles de détection spécifiques.

Comment structurer son programme de détection avec ATT&CK ?

Le framework MITRE ATT&CK fournit une **méthodologie structurée** pour construire et évaluer un programme de détection. La première étape est l'**évaluation de la couverture actuelle** : mappez chaque règle SIEM existante à la technique ATT&CK correspondante et visualisez la couverture sur la matrice ATT&CK. Cela révèle immédiatement les angles morts. La deuxième étape est la **priorisation basée sur les menaces** : identifiez les groupes d'attaquants (threat actors) qui ciblent votre secteur d'activité via les rapports de threat intelligence et les données ATT&CK, et concentrez vos développements sur les techniques qu'ils utilisent le plus fréquemment. La troisième étape est le **développement itératif** : déployez les nouvelles règles

par lots de 5 à 10, laissez une période de stabilisation de 2 à 4 semaines pour le tuning, puis passez au lot suivant. La quatrième étape est la **validation continue** : testez régulièrement vos règles avec des exercices de purple team ou des outils d'émulation d'adversaire (Atomic Red Team, Caldera) pour vérifier qu'elles détectent effectivement les techniques ciblées dans votre environnement réel. Le standard Sigma facilite ce processus en permettant d'écrire des règles portables qui peuvent être converties automatiquement en SPL, KQL ou EQL selon votre SIEM.

Pourquoi le tuning continu est-il indispensable ?

Une règle de détection déployée sans **tuning continu** se dégrade inévitablement avec le temps. Les environnements IT évoluent (nouveaux services, nouvelles applications, changements d'infrastructure), les attaquants adaptent leurs techniques pour contourner les détections connues, et les faux positifs s'accumulent jusqu'à ce que les analystes ignorent certaines catégories d'alertes. Le tuning est un processus continu qui comprend plusieurs activités. La **revue des faux positifs** : analysez chaque semaine les alertes classées comme faux positifs pour identifier des patterns récurrents qui justifient l'ajout d'exclusions ou l'ajustement de seuils. L'**analyse de couverture** : vérifiez mensuellement que les sources de données alimentant vos règles sont toujours connectées et que le volume de données est cohérent avec les attentes. La **mise à jour des seuils** : adaptez les seuils quantitatifs (nombre de tentatives de login, volume de données transférées) à l'évolution de votre environnement. La *validation de détection* : exécutez trimestriellement des tests de vos règles critiques pour vérifier qu'elles fonctionnent toujours correctement après les changements d'infrastructure et les mises à jour SIEM. Pour comprendre les techniques d'évasion que les attaquants utilisent pour contourner vos détections, consultez notre article sur l'évasion EDR/XDR.

Mon avis : La tentation est grande de vouloir couvrir 100% de la matrice ATT&CK, mais c'est une course sans fin qui disperse les efforts. Concentrez-vous sur les 50 règles de ce guide comme socle, stabilisez-les avec un taux de faux positifs inférieur à 15%, puis ajoutez progressivement des détections supplémentaires en fonction de votre threat landscape spécifique. 50 règles bien tunées et validées par purple team valent infiniment plus que 500 règles déployées par défaut et jamais ajustées.

Quelles erreurs éviter dans la conception des use cases ?

Plusieurs **erreurs récurrentes** compromettent l'efficacité des programmes de détection. La première est de **copier des règles sans les adapter** au contexte local : une règle qui détecte l'utilisation de PsExec est inutile si votre équipe d'administration utilise légitimement PsExec quotidiennement sans que l'exclusion soit configurée. La deuxième erreur est de **négliger les dépendances en données** : une règle qui requiert des logs Sysmon ne fonctionnera pas si Sysmon n'est pas déployé ou si sa configuration ne capture pas les événements nécessaires. Avant de déployer une règle, vérifiez que toutes les sources de données requises sont disponibles et correctement normalisées. La troisième erreur est l'**absence de documentation** : chaque règle doit être accompagnée d'une fiche documentant son objectif, sa logique, les sources requises, les faux positifs connus, les actions de réponse recommandées et le mapping ATT&CK. Sans cette documentation, le turnover des analystes entraîne une perte de

connaissance critique sur la raison d'être et le fonctionnement des détections. La quatrième erreur est de **déployer trop de règles trop vite** sans période de stabilisation, créant un pic d'alertes qui submerge les analystes et détruit leur confiance dans le SIEM.

À retenir : Un programme de détection efficace s'appuie sur 50 règles SIEM essentielles couvrant les principales tactiques ATT&CK, déployées progressivement avec un tuning rigoureux. La clé est de prioriser les techniques utilisées par les threat actors ciblant votre secteur, de valider chaque règle par des tests de purple team et de maintenir un taux de faux positifs inférieur à 15% grâce à un tuning continu. La qualité prime toujours sur la quantité.

Quel pourcentage de la matrice MITRE ATT&CK votre SOC couvre-t-il réellement avec des détections validées et tunées, en toute honnêteté ?

Sources et références : MITRE ATT&CK · MITRE CAR

Perspectives et prochaines étapes

L'avenir de la détection SIEM sera marqué par l'adoption croissante du Detection as Code (règles versionnées et déployées via CI/CD), l'utilisation de l'IA pour générer et optimiser automatiquement les règles de détection, et la convergence des détections SIEM, EDR et NDR dans des plateformes XDR unifiées. Pour progresser, commencez par évaluer votre couverture ATT&CK actuelle, identifiez les cinq techniques prioritaires non couvertes et implémentez les règles correspondantes en suivant la méthodologie décrite dans ce guide. Chaque règle ajoutée et validée est un pas de plus vers un SOC capable de détecter les attaques qui comptent.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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