AYI NEDJIMI Consultants

# Threat Hunting Proactif : Techniques et Outils SOC 2026

Catégorie : SOC et Detection  Lecture : 10 min  Publié le : 12/03/2026  Auteur : Ayi NEDJIMI

*Guide complet de threat hunting proactif en 2026 : méthodologies, techniques de chasse aux menaces, outils, hypothèses de hunting et intégration SOC.*

## Résumé exécutif

Ce guide présente les méthodologies de threat hunting proactif en 2026 : formulation d'hypothèses de chasse structurées autour du framework MITRE ATT&CK, techniques d'investigation avancées incluant le stacking, le clustering, l'analyse de séries temporelles et l'analyse de graphes, outils spécialisés comme le SIEM, les notebooks Jupyter, Velociraptor, OSQuery et les règles YARA, et intégration du hunting dans les processus continus du SOC pour détecter ce que les règles automatiques du SIEM et de l'EDR manquent systématiquement. Les attaques les plus dangereuses sont précisément celles qui contournent les détections automatiques, et seule l'intelligence humaine combinée à une méthodologie rigoureuse peut combler cette lacune critique. Nous couvrons les quatre approches complémentaires de hunting et démontrons comment capitaliser chaque découverte sous forme de nouvelles détections automatiques créant un cycle vertueux d'amélioration.

Le **threat hunting proactif** représente l'évolution ultime des capacités de détection d'un SOC, passant d'une posture réactive (attendre les alertes) à une posture offensive (rechercher activement les compromissions). En 2026, les attaques les plus dangereuses sont précisément celles qui contournent les détections automatiques du SIEM et de l'EDR. Les APT (Advanced Persistent Threats) utilisent des techniques sur mesure, des outils personnalisés et des procédures opérationnelles adaptées à l'environnement cible pour rester sous le radar des détections basées sur les signatures et les règles. Le threat hunting comble cette lacune en mobilisant l'intelligence humaine, la créativité et la connaissance approfondie de l'environnement pour formuler et tester des hypothèses de compromission qui vont au-delà de ce que les outils automatiques peuvent détecter. Ce guide vous fournit une méthodologie structurée pour intégrer le threat hunting dans les activités de votre SOC, de la formulation d'hypothèses pertinentes à l'utilisation des outils et techniques de chasse les plus efficaces, en passant par la capitalisation des découvertes sous forme de nouvelles détections automatiques. Le threat hunting n'est pas réservé aux SOC de grande taille : avec la bonne méthodologie et les bons outils, même une équipe réduite peut conduire des hunts productifs qui découvrent des menaces que le SIEM ne verra jamais seul.

**Retour d'expérience :** Un programme de threat hunting structuré (2 hunts par mois, 1 analyste L3 dédié à 50%) dans un SOC de taille moyenne a permis de découvrir en 12 mois 7 compromissions actives non détectées par le SIEM et l'EDR, dont 2 présentes depuis plus de 90

jours. Les hypothèses les plus productives concernaient les communications C2 via des services cloud légitimes et l'abus de comptes de service avec des authentifications anormales. Chaque hunt a généré en moyenne 3 nouvelles règles de détection automatiques.

## Méthodologies de threat hunting

Le threat hunting repose sur plusieurs **approches méthodologiques** complémentaires. L'approche *hypothesis-driven* (basée sur les hypothèses) est la plus structurée et la plus efficace. Le hunter formule une hypothèse de compromission basée sur la threat intelligence, les rapports d'incidents du secteur ou sa connaissance de l'environnement, puis conçoit et exécute des requêtes pour la valider ou l'invalider. Exemple d'hypothèse : un attaquant utilisant le groupe APT29 pourrait communiquer via des services de stockage cloud légitimes pour masquer son trafic C2. Le hunter recherche alors dans les logs proxy les connexions vers des services de stockage cloud non approuvés par l'organisation, avec des patterns de communication réguliers caractéristiques d'un beacon. L'approche **IOC-driven** (basée sur les indicateurs) recherche des indicateurs de compromission spécifiques dans les données historiques. Quand un nouvel IOC de haute confiance est publié (hash de malware, domaine C2, IP d'infrastructure offensive), le hunter le recherche dans les données SIEM des dernières semaines ou mois pour vérifier si l'organisation a été exposée avant que l'IOC ne soit connu.

L'approche **analytics-driven** (basée sur l'analyse statistique) recherche des anomalies dans les données sans hypothèse préalable. Le hunter utilise des techniques statistiques et de data science pour identifier des écarts significatifs par rapport aux baselines normales : utilisateurs avec des patterns d'authentification anormaux, processus avec des arborescences inhabituelles, systèmes communiquant avec des destinations nouvelles. L'approche **TTP-driven** (basée sur les tactiques, techniques et procédures) cible les comportements d'attaque documentés dans le framework MITRE ATT&CK en recherchant les artefacts spécifiques de chaque technique dans les données. Cette approche est systématique et reproductible, ce qui facilite la documentation et la capitalisation. Consultez notre article sur le threat hunting avec Sentinel pour des exemples concrets d'application de ces méthodologies dans un environnement Microsoft.

## Comment formuler des hypothèses de hunting productives ?

La qualité des **hypothèses de hunting** détermine directement la productivité de l'exercice. Une bonne hypothèse est spécifique, testable et pertinente pour le contexte de l'organisation. Pour formuler des hypothèses productives, exploitez quatre sources d'inspiration. La première source est la **threat intelligence** : les rapports sur les groupes d'attaquants ciblant votre secteur fournissent des TTP spécifiques à rechercher. Si un rapport indique que le groupe FIN7 utilise des macros Excel déclenchant du PowerShell encodé pour compromettre le secteur retail, formulez l'hypothèse : des macros Excel malveillantes pourraient avoir exécuté des commandes PowerShell encodées sur nos endpoints. La deuxième source est les **incidents récents** dans votre organisation ou votre secteur : chaque incident découvert soulève la question de savoir s'il existe d'autres compromissions similaires non encore détectées. La troisième source est les **résultats de Purple Team** : les techniques non détectées lors des exercices Purple Team sont des hypothèses de hunting prioritaires car elles confirment un angle mort de détection. La

quatrième source est l'*intuition experte* : un hunter expérimenté qui observe une anomalie subtile dans les données peut formuler une hypothèse originale que la threat intelligence n'avait pas identifiée.

Chaque hypothèse doit être formalisée avec une **structure standard** : description de la menace présumée, technique ATT&CK correspondante, sources de données nécessaires, requêtes de validation et critères de résultat positif ou négatif. Cette formalisation garantit la reproductibilité et facilite le partage entre hunters. Tenez un **registre des hypothèses** testées avec leurs résultats (positif, négatif, non concluant) pour éviter de répéter les mêmes hunts et pour identifier les catégories d'hypothèses les plus productives dans votre environnement. Consultez notre article sur les techniques Living off the Land pour des hypothèses basées sur l'abus d'outils système et sur l'exfiltration DNS/DoH pour des hypothèses de communication C2. Les référentiels de l'ANSSI fournissent des guides de chasse aux menaces adaptés au contexte français.

| Source d'hypothèse | Exemple d'hypothèse | Données requises | Technique ATT&CK |
|---|---|---|---|
| Threat Intelligence | C2 via cloud storage légitime | Logs proxy, DNS | T1071.001 |
| Incident récent | Autres comptes compromis par même vecteur | Logs auth, email | T1078 |
| Purple Team | DCSync non détecté pendant exercice | Security logs DC | T1003.006 |
| Anomalie statistique | Compte avec horaires d'activité anormaux | Logs auth | T1078 |
| Intuition expert | Service DNS inhabituel sur contrôleur | Sysmon, DNS | T1071.004 |

## Outils et techniques de hunting

Le threat hunting exploite un ensemble d'**outils et techniques** complémentaires. Le **SIEM** est l'outil principal du hunter, offrant l'accès aux données historiques de toutes les sources. Les langages de requête avancés (SPL dans Splunk, KQL dans Sentinel, EQL dans Elastic) permettent de formuler des recherches complexes. Les **notebooks d'investigation** (Jupyter Notebooks dans Sentinel, Splunk Notebooks) combinent code, visualisations et documentation dans un environnement interactif idéal pour le hunting exploratoire. L'EDR fournit des capacités de **recherche endpoint** en temps réel : interroger simultanément des milliers d'endpoints pour rechercher un fichier, un processus ou un artefact spécifique. Les outils de *threat hunting spécialisés* incluent Velociraptor pour la collecte forensique à distance à grande échelle, OSQuery pour l'interrogation SQL des endpoints, et YARA pour la recherche de patterns dans les fichiers et la mémoire.

Les techniques de hunting les plus productives incluent le **stacking** (empilage de données pour identifier les valeurs rares : quels processus parents sont les moins fréquents pour cmd.exe ? Quelles destinations réseau sont contactées par un seul poste ?), le **clustering** (regroupement de données similaires pour identifier les outliers qui n'appartiennent à aucun cluster connu), le **time series analysis** (analyse des séries temporelles pour détecter les beacons C2 caractérisés

par des patterns réguliers avec jitter), et le **graph analysis** (analyse des relations entre entités pour visualiser les chemins d'attaque et les connexions suspectes). Le standard Sigma facilite le partage de requêtes de hunting entre SIEM. Consultez notre comparatif DFIR pour les outils d'investigation complémentaires et notre article sur les attaques Golden Ticket pour un exemple de hunting sur les techniques Kerberos.

## Pourquoi le threat hunting trouve-t-il ce que le SIEM manque ?

Le threat hunting détecte ce que le SIEM manque pour plusieurs raisons fondamentales. Premièrement, les règles SIEM sont **déterministes** : elles détectent des conditions prédéfinies et manquent tout ce qui ne correspond pas exactement à ces conditions. Un attaquant qui connaît (ou devine) les seuils de détection peut les contourner en restant juste en dessous. Le hunter, en revanche, applique un **jugement humain** contextuel qui peut identifier une activité suspecte même si elle ne déclenche aucune règle. Deuxièmement, les règles SIEM opèrent sur des **fenêtres temporelles limitées** (généralement minutes ou heures) et manquent les attaques qui se déroulent sur des semaines ou des mois à un rythme très lent (low and slow). Le hunter peut analyser des tendances sur des mois de données historiques pour identifier des progressions graduelles. Troisièmement, les règles SIEM sont des **patterns connus** : elles ne peuvent pas détecter les techniques inédites ou les variations non documentées de techniques connues. Le hunter, en appliquant une approche analytique créative, peut identifier des comportements suspects sans avoir besoin d'une signature préexistante.

La **capitalisation** est le pont entre le hunting et la détection automatique. Chaque hunt productif (qui découvre une menace ou une anomalie) doit être transformé en détection automatique : la requête de hunting qui a permis de découvrir la compromission est convertie en règle SIEM qui détectera automatiquement des occurrences futures de la même technique. Ce cycle verteux (hunt, découverte, automatisation) est le mécanisme principal d'amélioration continue de la couverture de détection du SOC. Un programme de hunting productif génère en moyenne 2 à 5 nouvelles règles de détection par hunt, enrichissant progressivement le corpus de détections automatiques. Consultez notre article sur la détection de l'évasion EDR/XDR pour des exemples de techniques qui échappent aux détections automatiques et nécessitent du hunting.

**Mon avis :** Le threat hunting est la discipline qui sépare les SOC qui surveillent de ceux qui protègent réellement. Trop de SOC se contentent de traiter les alertes SIEM sans jamais se demander ce qui leur échappe. Vous n'avez pas besoin d'une armée de hunters pour commencer : un analyste L3 motivé, dédié à 50% au hunting avec une méthodologie structurée et un accès aux données SIEM historiques, peut révolutionner la posture de détection de votre organisation en quelques mois. Le hunting est aussi un excellent outil de développement des compétences qui motive et retient les analystes les plus talentueux.

## Quelles compétences pour devenir threat hunter ?

Le **threat hunter** combine un ensemble de compétences techniques et cognitives. Techniquement, il doit maîtriser au moins un langage de requête SIEM en profondeur (SPL, KQL ou EQL), avoir une connaissance approfondie des systèmes d'exploitation Windows et Linux (processus, services, registre, artefacts forensiques), comprendre les protocoles réseau et les techniques d'attaque documentées dans MITRE ATT&CK, et savoir scripter en Python pour automatiser les analyses complexes. Cognitivement, le hunter doit posséder une **curiosité insatiable** et une capacité à formuler des hypothèses créatives, un *esprit analytique rigoureux* capable de distinguer les anomalies significatives du bruit normal, une connaissance approfondie du **contexte de l'environnement** qu'il protège (quels sont les processus métier normaux, quels flux réseau sont attendus, quels comptes sont utilisés pour quoi), et une capacité de **persistence** car de nombreux hunts ne trouvent rien et il faut maintenir la motivation. Les certifications GCTI (GIAC Cyber Threat Intelligence) et GCFA (GIAC Certified Forensic Analyst) sont particulièrement pertinentes pour les hunters. La participation à des CTF orientés défense et l'analyse de rapports de threat intelligence sont d'excellents moyens de développer et maintenir ces compétences. Consultez notre guide forensique mémoire pour des compétences complémentaires essentielles au hunting avancé.

## Intégration du hunting dans le cycle SOC

Le threat hunting doit être **intégré dans les processus continus** du SOC plutôt que traité comme une activité ponctuelle et isolée. L'intégration suit un cycle en quatre étapes. L'**étape 1 (Planification)** est la sélection des hypothèses de hunting basée sur la threat intelligence, les incidents récents, les résultats de Purple Team et les angles morts de détection identifiés. Un planning trimestriel de hunts priorisés par pertinence et impact potentiel fournit un cadre structuré. L'**étape 2 (Exécution)** est la conduite des hunts selon la méthodologie choisie, avec documentation systématique des requêtes, observations et résultats. L'**étape 3 (Capitalisation)** transforme chaque hunt productif en amélioration concrète : nouvelles règles de détection SIEM, mise à jour des playbooks SOAR, enrichissement de la threat intelligence interne et partage des découvertes avec l'équipe SOC. L'**étape 4 (Mesure)** évalue l'efficacité du programme de hunting avec des métriques : nombre de hunts conduits, taux de hunts productifs (ayant découvert une menace ou un gap de détection), nombre de nouvelles détections générées et incidents découverts grâce au hunting.

**À retenir :** Le threat hunting proactif comble les lacunes des détections automatiques en mobilisant l'intelligence humaine pour rechercher activement les compromissions que le SIEM et l'EDR ne détectent pas. L'approche hypothesis-driven structurée autour de MITRE ATT&CK est la plus efficace. Chaque hunt productif doit être capitalisé sous forme de nouvelle détection automatique, créant un cycle vertueux d'amélioration continue. Un analyste L3 à 50% avec la bonne méthodologie suffit pour démarrer un programme de hunting productif.

Votre SOC recherche-t-il activement les compromissions cachées dans vos données, ou attend-il passivement que les alertes lui signalent les menaces que vos adversaires les plus sophistiqués ont déjà appris à contourner ?

**Sources et références :** MITRE ATT&CK · MITRE CAR

## Perspectives et prochaines étapes

L'avenir du threat hunting sera augmenté par l'IA qui assistera les hunters dans la formulation d'hypothèses, l'analyse de grands volumes de données et l'identification d'anomalies subtiles. Les plateformes de hunting collaboratif vont faciliter le partage de requêtes et de résultats entre organisations. L'automatisation progressive des hunts les plus reproductibles (scheduled hunts) va libérer les hunters pour les investigations les plus créatives et les plus complexes. Pour démarrer votre programme de hunting, identifiez votre analyste le plus expérimenté, allouez-lui 20% de son temps pour conduire un hunt par mois basé sur une hypothèse de threat intelligence, et capitalisez chaque découverte sous forme de nouvelle détection. Le premier hunt qui découvrira une menace non détectée justifiera à lui seul l'investissement dans le programme.

**Ayi NEDJIMI Consultants** — Expert cybersécurité offensive & intelligence artificielle

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