

Top 5 des scénarios d'utilisation de Splunk Enterprise Security

splunk>
a CISCO company

Les événements de sécurité sont difficiles à détecter et à prendre en charge rapidement. Un analyste de sécurité peut passer plusieurs minutes (parfois des jours) sur une alerte. Maintenant, multipliez cela par les milliers d'alertes de sécurité à gérer : vous comprenez qu'il y a bien trop de tickets et trop peu d'analystes. Vous entrevoyez le problème ?

Nous devons aider les équipes de sécurité à réduire leur temps de réponse de même que le nombre d'alertes qu'elles reçoivent. Nous pouvons commencer par leur donner une meilleure visibilité sur leur environnement pour qu'elles puissent détecter et prendre en charge les menaces plus rapidement. Mieux encore, une réponse automatisée peut drastiquement réduire les délais de triage des alertes.

On limite ainsi le terrain pour les menaces insidieuses et difficiles à détecter comme les logiciels malveillants, ainsi que les dommages qu'elles peuvent causer, pour le plus grand bonheur de nos analystes de sécurité stressés.

En conclusion ? Les analystes ont besoin de deux choses : moins d'alertes et une méthode de travail plus intelligente et unifiée. Autrement dit, il faut accélérer les investigations en misant sur des agents dotés d'IA et obtenir une visibilité complète sur les environnements cloud, sur site et hybrides. Armées d'une solution

adaptée, les équipes de sécurité peuvent réduire le volume d'alertes jusqu'à 80 %, maximiser la productivité des analystes et faire face aux événements en toute confiance.

C'est là que **Splunk Enterprise Security** (ES), notre solution de gestion des événements et des informations de sécurité (SIEM) de pointe, s'avère utile. Splunk ES est la plateforme SecOps de référence basée sur l'IA. Elle unifie le SIEM, le **SOAR** (orchestration, automatisation et réponse de sécurité), l'**UEBA** (analyse du comportement des entités et des utilisateurs), la threat intelligence et l'ingénierie de détection, et intègre l'IA tout au long du workflow de détection des menaces, d'investigation et de réponse (**TDIR**).

Conséquence : des résultats plus rapides, des risques réduits et une résilience renforcée à l'ère de l'IA agentique. Dans ce guide concis, nous allons passer en revue cinq grands scénarios d'utilisation des utilisateurs de Splunk. Qu'il s'agisse d'éliminer la fatigue liée aux alertes ou d'unifier la visibilité et l'automatisation à grande échelle, ces exemples montrent comment les équipes de sécurité peuvent obtenir rapidement des résultats, où qu'elles en soient dans leur parcours de sécurité.

1. Réduisez le nombre d'alertes grâce aux alertes basées sur le risque et à l'IA agentique

La plupart des centres d'opérations de sécurité (SOC) sont submergés de faux positifs et de doublons, et ce bruit incessant dissimule des menaces bien réelles. Les analystes sont souvent contraints de passer d'un outil à l'autre et s'épuisent à suivre des pistes qui sont souvent autant d'impasses.

Splunk Enterprise Security élimine les tâches manuelles qui ralentissent les analystes en mettant en place un système d'alertes basées sur le risque. Ce système attribue un score de risque aux utilisateurs et aux entités, puis déclenche une alerte en cas de dépassement de certains seuils de risque et de comportement. Résultat : des faux positifs réduits de 80 %.

Pour le SOC, c'est un excellent moyen d'optimiser la détection des menaces : la réduction du volume d'alertes augmente le nombre de vrais positifs et met en évidence les menaces plus sophistiquées, comme les attaques low and slow qui échappent à la plupart des recherches de corrélation. Cela permet de libérer du temps et des ressources pour isoler les menaces réelles (souvent complexes) et aligner les opérations sur les principaux frameworks de cybersécurité.

Et si vous ajoutez à cela l'IA agentique, le bruit devient tout à coup bien plus supportable. L'IA agentique représente une nouvelle phase pour l'automatisation de la sécurité ; cette fois, l'IA ne se contente plus d'assister les analystes, elle agit en leur nom. Les analystes retrouvent leur concentration, les investigations sont plus rapides et les équipes peuvent accroître leurs capacités sans embaucher une foule d'intervenants. En mettant l'IA au cœur des solutions SOAR modernes, les organisations automatisent les tâches répétitives, elles enrichissent les alertes en temps réel, et c'est l'ensemble du workflow TDIR qui devient plus agile.

Pour résumer, l'automatisation pilotée par l'IA analyse des volumes considérables de données télémétriques en quelques secondes, hiérarchise les alertes en fonction du score de risque, recommande des mesures de correction et orchestre les workflows couvrant plusieurs outils, ce qui se traduit par une baisse drastique des temps moyens de détection (MTTD) et de réponse (MTTR).

2. Obtenez une visibilité haute fidélité sur vos données

Si le passage au cloud a représenté un vrai gain de flexibilité, il a également donné jour à des environnements de données aussi tentaculaires que cloisonnés. Les équipes de sécurité sont confrontées à un véritable dilemme : dupliquer les données, pour un coût de stockage exorbitant, ou tolérer des angles morts dangereux sur AWS, Azure, GCP, SaaS et en local. Splunk Enterprise Security comble ces lacunes et permet aux équipes de sécurité d'acheminer, de hiérarchiser et de consulter les données avec une grande souplesse, de façon à corrélérer la télémétrie des déploiements hybrides et multicloud au sein d'une plateforme unifiée. Elles obtiennent ainsi une visibilité complète pour un coût total de possession (TCO) plus faible et s'adaptent avec agilité à l'évolution de l'entreprise : fusions-acquisitions, introduction de nouvelles applications ou changement d'infrastructure. Splunk pérennise votre SOC en veillant à ce que chaque signal soit visible, contextualisé et exploitable.

3. Accélérez les investigations grâce aux workflows pilotés par l'IA

Les investigations sont souvent ralenties par le manque de coordination des outils et la lourdeur des processus manuels. Les analystes perdent un temps considérable à rassembler des preuves, à rédiger des requêtes et à produire des rapports, pendant que leurs adversaires progressent dans les systèmes. En intégrant directement l'IA au workflow TDIR, Splunk Enterprise Security transforme radicalement ce processus.

En employant simplement le langage naturel, les analystes peuvent désormais générer des recherches SPL complexes, résumer automatiquement les résultats et même recevoir des recommandations de marche à suivre. Dans le même temps, la gestion intégrée des cas permet de centraliser les notes, les fichiers et la threat intelligence : le contexte ne se perd jamais et les transferts d'une équipe à l'autre sont parfaitement transparents. Ce qui prenait des jours auparavant se fait aujourd'hui en quelques minutes. Les analystes se perfectionnent plus rapidement, la documentation devient cohérente et le SOC gagne en clarté et en rapidité au moment où il en a le plus besoin.

4. Misez sur l'automatisation à l'échelle du SOC et sur l'enrichissement contextuel

Dans de nombreux SOC, l'automatisation est puissante mais limitée, car souvent réservée aux spécialistes capables de gérer des déploiements SOAR complexes. Tous les autres sont débordés de tâches manuelles pénibles qui ralentissent les processus et augmentent le risque d'épuisement professionnel. Splunk Enterprise Security Premier change la donne en intégrant nativement le SOAR à ES pour mettre l'automatisation à la portée de chaque analyste.

Grâce à la création de playbooks assistée par IA, tous les profils d'utilisateurs peuvent décrire un workflow en langage naturel et demander à Splunk de le traduire en playbook testé et fonctionnel. Les agents de réponse autonomes de la plateforme confinent instantanément les menaces tout en informant les humains. En démocratisant l'automatisation à l'échelle du SOC, cette approche systématise la réponse, accélère le confinement et permet à chaque analyste d'apporter une contribution précieuse. Résultat : des interventions rapides et cohérentes à grande échelle et une sécurité renforcée, avec moins de tâches manuelles.

5. Combler les angles morts de la détection pour réduire le temps moyen de détection

Les acteurs malveillants évoluent sans cesse et les systèmes de détection parviennent rarement à suivre leur rythme. La plupart des SOC n'ont pas une image claire des tactiques contre lesquelles ils peuvent se défendre et les menaces tendent à prospérer dans ces angles morts. Splunk Enterprise Security leur donne la visibilité et la précision nécessaires pour garder une longueur d'avance.

Detection Studio accompagne tout le cycle de vie de l'ingénierie de détection : les équipes SOC peuvent ainsi tester, déployer et superviser des détections haute fidélité en toute confiance. Le mapping MITRE ATT&CK en temps réel montre avec précision les points forts et les faiblesses de la couverture, tandis que le contenu sélectionné par la Splunk Threat Research Team (STRT) et Cisco Talos tient les détections à jour face aux tactiques, techniques et procédures (TTP) émergentes. Le SOC comble proactivement les lacunes, renforce sa couverture et réduit le risque d'attaques invisibles, au lieu d'attendre le passage à l'acte de l'adversaire.

Vous souhaitez muscler votre jeu ?

Lancez-vous avec la plateforme SecOps optimisée par l’IA de Splunk.



Splunk, Splunk>, Data-to-Everything et Turn Data Into Doing sont des marques commerciales de Splunk Inc., déposées aux États-Unis et dans d’autres pays. Tous les autres noms de marque, noms de produits et marques commerciales appartiennent à leurs propriétaires respectifs. © 2025 Splunk LLC. Tous droits réservés.

