Les 10 fonctionnalités essentielles d'un **SOC moderne**

La plateforme Data-to-Everything dans le centre des opérations de sécurité (SOC)

splunk>
turn data into doing™

Sommaire

La plateforme Data-to-Everything dans le centre des opérations de sécurité (SOC)

Nous vivons dans un monde d'innovation sans précédent. La technologie transforme des industries entières, mondialise les activités et démultiplie l'efficacité de la main d'œuvre. Mais nous n'avons fait qu'effleurer la surface. L'innovation poursuit sa progression exponentielle, et personne ne peut prédire ce que nous serons en mesure de réaliser, ni des conséquences que nous pourrions subir par la suite.

Le nombre d'appareils connectés approche rapidement les 80 milliards, l'automatisation s'ancre dans nos routines quotidiennes, et les changements dans notre monde ne feront que s'accélérer, élargissant inévitablement la surface d'attaque. Les services de sécurité sont contraints de gérer des données provenant de sources multiples, dans des formats différents et à des vitesses accrues : il est clair que de nombreuses entreprises ne sont pas prêtes à relever les défis actuels et futurs en matière de données.

Votre entreprise a besoin de visibilité pour identifier les activités, et de contexte pour mieux comprendre les risques réels. Le fait de disposer de plus de données sur les systèmes et les personnes qui les utilisent permet, en fin de compte, de mieux comprendre comment gérer les risques.

C'est pour cette raison que les entreprises dépensent des milliards de dollars et d'innombrables heures pour tenter d'extraire la valeur de leurs données, et de colmater les vulnérabilités de sécurité exposées grâce à une vision globale de leur infrastructure. Elles créent des lacs de données en intégrant d'innombrables systèmes qui créent des volumes de données considérables, et se fraient un chemin sur le réseau complexe d'outils conçus pour agréger, superviser et analyser ces données afin de relever leurs plus grands défis de sécurité.

Notre approche : Data-to-Everything

Il est indispensable que vous puissiez compter sur vos données pour chaque question de l'entreprise, chaque décision, chaque action. Mais dans un monde en évolution constante, de plus en plus connecté, qui produit toujours plus de données, le défi ne consiste pas seulement à tenir le rythme mais surtout à les transformer rapidement en informations et en actions. Les données existent dans une grande variété de formats et proviennent de sources diverses, que les entreprises auraient tout intérêt à exploiter pour mieux se protéger.

Pour optimiser votre pile de sécurité et donner à votre équipe les moyens de fonctionner au maximum de ses capacités, il faut une plateforme unique permettant de passer à l'action, de l'investigation à la supervision, en passant par l'orchestration et la correction. Ce doit être une plateforme robuste permettant à toute l'entreprise d'exploiter la puissance des données à travers un prisme unique et holistique. Cette approche se traduit par des investissements plus ciblés et plus intelligents dans les technologies, une complexité réduite et moins d'obstacles entre les données et l'action.

Nous appelons cela la plateforme **Data-to-Everything**. Elle constitue la base de tout centre d'opérations de sécurité moderne (SOC), en mobilisant les données de l'ensemble de votre entreprise pour vos scénarios de sécurité les plus urgents.

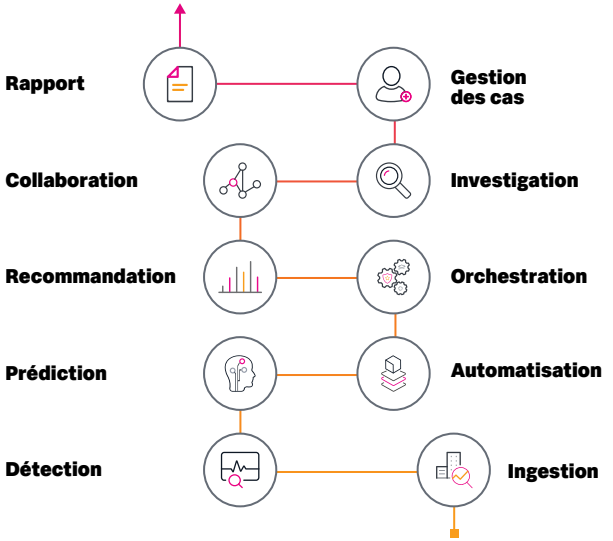
Bâtir un SOC moderne

Votre équipe de sécurité travaille dur sur la ligne de front : elle identifie, analyse et réduit les menaces auxquelles votre entreprise est exposée. Mais en dépit de ses efforts, le nombre d'incidents non traités augmente chaque jour. La réalité est simple : **il n'y a pas assez de professionnels qualifiés** pour analyser le volume d'incidents que la plupart des entreprises reçoivent.

Mais un SOC moderne, basé sur une plateforme Data-to-Everything, bénéficie d'une visibilité sur l'ensemble de l'entreprise, créant ainsi une surface de travail commune pour tous les membres de l'équipe. Avec une suite unique intégrant de manière transparente les solutions d'autres fournisseurs pour augmenter les capacités existantes, l'analyste pourra consacrer son temps à des activités à valeur ajoutée, il n'aura plus besoin de basculer entre des dizaines de produits et tous les membres de l'équipe bénéficieront d'une surface de travail commune.

Et cette solution ne doit pas être assemblée de manière ponctuelle. La suite de sécurité doit également disposer de puissantes fonctionnalités d'analyse qui peuvent optimiser les capacités d'une petite équipe, leur donnant un aperçu des menaces potentielles pour leur éviter de perdre du temps sur de fausses alertes. Enfin, la suite peut exploiter les technologies avancées de machine learning (ML), d'automatisation et d'orchestration.

Pour créer un SOC moderne, les entreprises ont besoin d'une plateforme d'opérations de sécurité prenant en charge les 10 fonctionnalités suivantes :



10 fonctionnalités

1. Ingestion

Toutes les données sont importantes en matière de sécurité. Les données sont l'oxygène qui donne vie à un SOC. Les analyses et les algorithmes le respirent. La capacité à ingérer des données à grande échelle à partir de n'importe quelle source, structurée ou non structurée, est tout aussi importante. Vous devez également pouvoir organiser ces données pour les rendre utilisables par la machine ou par l'homme.

2. Détection

Une fois qu'un événement est entré dans le système, il est impératif que la suite d'opérations de sécurité puisse détecter l'événement. Dans ce cas, la détection se concentre sur les événements, ce qui diffère des solutions traditionnelles qui se focalisaient sur les fichiers ou le trafic réseau. Une suite d'opérations de sécurité peut exploiter une combinaison de règles de corrélation, de machine learning et de scénarios analytiques, pour n'en nommer que quelques-unes.

3. Prédiction

Imaginez que vous recevez une alerte 30 minutes avant de découvrir effectivement un événement de sécurité. Imaginez ce que cela représenterait pour votre SOC. La capacité à prédire un événement de sécurité permet au SOC de transmettre de manière proactive l'incident à un être humain ou de rationaliser une réponse grâce à un processus prédéfini. Il existe de nouvelles technologies prédictives très prometteuses qui fournissent aux analystes une alerte précoce, des précurseurs ou des indicateurs d'attaques plus importantes, et qui identifient les menaces inconnues avant qu'elles ne deviennent des risques plus importants.

4. Automatisation

L'automatisation est l'une des technologies les plus récentes au service des analystes SOC. La récente acquisition de Phantom par Splunk en est un excellent exemple. Les outils d'automatisation transforment des procédures d'exploitation standard en guides opérationnels numériques pour accélérer l'investigation, l'enrichissement, la détection, l'isolation et la correction.

Un SOC doté de capacités d'automatisation peut traiter davantage d'événements car les processus qui prenaient par exemple 30 minutes peuvent désormais être effectués en 40 secondes seulement. Dans l'évolution d'un SOC, l'automatisation n'est plus un choix mais bien un outil obligatoire.

5. Orchestration

Vous avez acheté des dizaines de produits pour faire fonctionner votre SOC par nécessité, non pas simplement parce que vous aviez un budget supplémentaire. La majorité de ces outils ont leur utilité et renforcent votre défense, mais ils ne changeront probablement pas. Cette situation est problématique car les menaces évoluent et les produits qui détectent les menaces doivent suivre le rythme dans un monde axé sur les API.

C'est là que l'orchestration entre en jeu. L'orchestration vous permet de brancher et de connecter tout ce qui se trouve à l'intérieur et à l'extérieur de votre SOC. Vous ne devez plus ouvrir de nouveaux onglets de navigateur, ni vous connecter à des solutions spécifiques distinctes pour chaque produit, et vous éliminez le copier-coller de plusieurs solutions. La possibilité d'orchestrer tous vos produits supprime les frais généraux, réduit la frustration et aide les analystes à concentrer leur énergie sur des tâches utiles.

6. Recommandation

À ce stade, les événements ont transité par une machine. Imaginez que la plateforme qui alimente le SOC puisse indiquer aux analystes les actions qu'ils doivent réaliser. Le SOC de nouvelle génération peut faire exactement cela en formulant une recommandation. Cela peut prendre la forme d'actions individuelles ou de procédures. Les recommandations sont utiles de deux manières : 1) elles instruisent les nouveaux analystes et leur apprennent ce qu'ils doivent faire lorsqu'une menace similaire se présente à nouveau, et 2) elles servent de vérification aux analystes expérimentés, ou de rappel d'un accélérateur pour les assister dans ce qu'ils devraient déjà savoir.

7. Investigation

Nous nous attendons à ce que 90 % du travail des analystes de niveau 1 soit automatisé dans un avenir proche. Qu'advient-il du reste du travail ? Inévitablement, une analyse humaine détaillée et précise est nécessaire pour terminer le travail. Des outils de sécurité intuitifs renforcent les capacités humaines d'un analyste et lui permettent de donner la priorité à ce qui doit vraiment être investigué.

8. Collaboration

La sécurité est un sport d'équipe qui demande coordination, communication et collaboration. Dans un environnement SOC, rien ne peut être abandonné. Les événements doivent être traités dans les moindres détails et les équipes doivent avoir des fonctionnalités ChatOps ou la capacité de collaborer et de connecter les outils, les personnes, les processus et l'automatisation dans un lieu de travail transparent.

Les informations, les idées et les données sont mises au premier plan. Cela permet aux équipes de sécurité de mieux collaborer, d'inviter des personnes extérieures au SOC à participer aux alertes, de partager des informations urgentes et importantes avec des pairs, et enfin de coopérer en tant qu'industrie.

9. Gestion des cas

Des incidents se produisent même lorsque nous faisons de notre mieux pour les éviter. L'important, c'est que lorsque des incidents surviennent, les équipes de sécurité soient munies de tous les outils nécessaires pour gérer le processus de réponse. Les équipes doivent s'assurer de disposer de plans de réponse, de workflows, de collectes de preuves, de communication, de documentation et de chronologies. La gestion des cas est donc devenue une fonctionnalité de base du SOC nouvelle génération.

10. Rapport

On ne peut pas gérer ce qu'on ne mesure pas. Nous vivons dans un monde piloté par les données et il en va de même pour la sécurité. C'est pourquoi vous pouvez désormais mesurer tous les aspects du processus de sécurité. Le fait de disposer des bons outils d'établissement de rapports fournit des informations sur ce qui fonctionne. Ainsi, les équipes de sécurité peuvent mesurer avec précision où elles se trouvent et où elles doivent aller. Aujourd'hui, le défi auquel les SOC sont confrontés est leur dépendance à un nombre trop élevé de plateformes, ce qui rend impossible l'obtention de rapports précis.

Splunk entre en jeu

La plateforme Splunk, aussi connue sous le nom de Splunk Cloud ou Splunk Enterprise, est votre point de départ. Splunk est une plateforme personnalisable d'analyse de données qui transforme les données machine en résultats commerciaux tangibles. Contrairement aux autres alternatives open source, Splunk Cloud et Splunk Enterprise vous permettent d'exploiter vos investissements technologiques existants. Vous pouvez tirer parti de toutes les données générées par vos systèmes, applications et appareils informatiques, de sécurité et d'entreprise, pour investiguer, superviser, analyser et agir en temps quasi réel.

Mais plus spécifiquement, la suite Splunk Security Operations Suite réunit les meilleures technologies SIEM, UEBA et SOAR au sein d'une surface de travail commune, pour armer le SOC moderne.

Splunk Enterprise Security (ES) est une solution SIEM axée sur l'analyse qui fournit une supervision de la sécurité en temps réel, une détection avancée des menaces, une investigation et un examen des incidents, ainsi qu'une réponse aux incidents pour une gestion efficace des menaces.

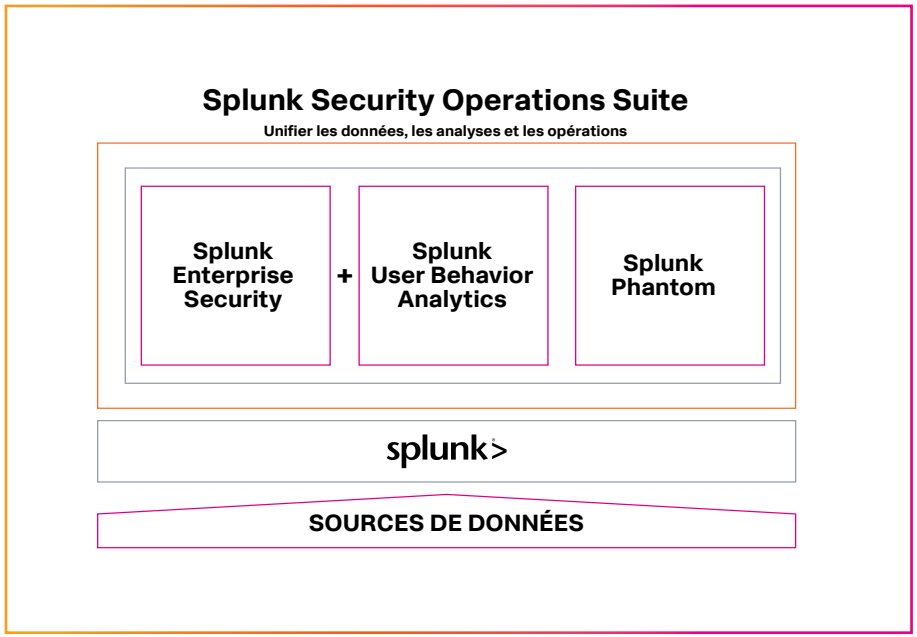
Grâce à **Splunk ES**, les équipes de sécurité bénéficient de capacités de détection des menaces, d'investigation et d'intervention plus rapides. Elles peuvent utiliser les frameworks et les workflows spécifiquement conçus pour accélérer la détection, l'investigation et la réponse aux incidents. Les équipes de sécurité peuvent également utiliser des tableaux de bord prédéfinis, des rapports, des capacités d'investigation, des catégories de cas d'utilisation, des analyses, des recherches de corrélation et des indicateurs de sécurité pour simplifier la gestion des menaces et la gestion des incidents. Elles peuvent ensuite utiliser ces capacités pour établir une corrélation entre les logiciels en tant que service (SaaS) et les sources sur site pour découvrir et déterminer l'étendue de l'activité des utilisateurs, de l'activité réseau, de l'activité des points de terminaison, de l'activité d'accès et de l'activité anormale.

Splunk User Behavior Analytics (UBA) est une solution fondée sur le machine learning qui détecte les menaces inconnues et les comportements anormaux des utilisateurs, des points de terminaison et des applications. Elle renforce votre équipe de sécurité existante et la rend plus productive en détectant des menaces qui passeraient inaperçues en raison du manque de personnes, de ressources et de temps.

Les équipes de sécurité peuvent utiliser **Splunk UBA** pour améliorer la visibilité et la détection des menaces. Plus précisément, elles peuvent détecter les menaces internes et inconnues à l'aide d'algorithmes de ML non supervisés que les produits traditionnels de sécurité n'auraient pas détecté. Elles peuvent automatiser la corrélation des comportements anormaux en menaces haute-fidélité à l'aide de visualisations sophistiquées de la kill chain. Cette capacité permet aux équipes de passer plus de temps à rechercher les menaces grâce aux alertes basées sur le comportement de haute-fidélité. Elles peuvent également identifier les dernières menaces sans interruption opérationnelle grâce aux mises à jour du contenu dynamiques par abonnement qui permettent aux équipes de sécurité de suivre l'évolution des dernières techniques de détection des menaces de manière proactive.

Splunk Phantom est une plateforme SOAR qui intègre les processus et les outils d'une équipe, leur permettant de travailler plus intelligemment, de répondre plus rapidement aux incidents et d'améliorer leurs défenses.

Phantom aide à maximiser les efforts des opérations de sécurité d'un SOC. Les équipes de sécurité peuvent automatiser les tâches répétitives pour optimiser leurs efforts et focaliser leur attention sur les décisions qui nécessitent vraiment un apport humain. Elles peuvent réduire les temps de séjour grâce à une détection et à une investigation automatisées, et réduire les temps de réponse grâce à des procédures qui s'exécutent à la vitesse de la machine. Phantom aide également les équipes de sécurité à intégrer leur infrastructure de sécurité existante de manière à ce que chaque élément participe activement à la stratégie de défense du SOC.



Lancez-vous.

Découvrez comment la suite Splunk pour les opérations de sécurité peut vous aider à moderniser votre SOC dès aujourd'hui.

10-Essential-Capabilities-of-a-Modern-SOC-106

splunk> turn data into doing™