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

Au cœur du centre des opérations de sécurité (SOC) orienté données

splunk>
turn data into doing

Sommaire

Transformez vos données en actions dans le centre des opérations de sécurité

Au cours des trois dernières années, un climat d'imprévisibilité pesant a entraîné des changements radicaux dans notre façon de vivre et de travailler. Pour les organisations privées ou publiques, la transformation numérique n'est plus seulement une priorité, elle est devenue urgemment impérative. De plus, ce sont les technologies cloud accélérées et la puissance des données qui sont à l'origine de la majorité des innovations stratégiques. Les équipes de sécurité se retrouvent non pas dans le périmètre mais bien à l'épicentre et s'efforcent de suivre le rythme de la transformation et de s'adapter aux défis de la pandémie, aux tensions géopolitiques, à la pénurie importante de talents, aux attaques plus sophistiquées et à l'augmentation des violations.

Pour réussir dans ce monde imprévisible, les organisations résilientes investissent dans des solutions de sécurité puissantes, flexibles et rapides, renforcées par les données. Un centre des opérations de sécurité orienté données permet aux organisations de se protéger, de s'adapter et de répondre rapidement à toute perturbation en élevant des barrières face aux menaces en constante évolution.

Comment surmonter ces défis et puiser dans la puissance de toutes ces données ? Tout commence par la modernisation de votre centre des opérations de sécurité (SOC).

De nos jours, les analystes SOC sont confrontés à des données provenant de multiples sources, sous différents formats et à des vitesses accrues. Pourtant, la plupart des SOC n'abordent pas encore la sécurité comme une problématique de données. Une sécurité efficace nécessite une visibilité sur la totalité de vos données, provenant de tous les systèmes, et sur les personnes qui les exploitent, ainsi qu'un contexte pertinent pour mieux comprendre et gérer les éléments qui représentent un risque réel. Il vous faut des solutions qui s'intègrent à de multiples systèmes et exploitent la quantité massive de données qu'ils créent. Vous avez également besoin de solutions pour gérer un réseau complexe d'outils conçus pour agréger, superviser et analyser le tout.

Approche orientée données de la sécurité

Dans un monde hybride, le défi n'est pas seulement de comprendre comment gérer toutes les données, mais aussi de comprendre comment les transformer en informations et en actions. Pour optimiser votre pile de sécurité et donner à votre équipe les moyens de fonctionner au maximum de ses performances, il faut une plateforme unique permettant de prendre des mesures informées, de la supervision à la correction, en passant par l'investigation et l'orchestration.

Sans compter qu'une simple plateforme de données holistique ne renforce pas uniquement la sécurité. Elle permet à l'organisation entière de puiser dans la puissance des données avec des investissements moindres et mieux ciblés dans la technologie, une complexité réduite et davantage d'opportunités d'innovation.

En faisant d'une plateforme orientée données la pierre angulaire d'un SOC moderne, vous pouvez rassembler les données de toute votre organisation pour mieux résoudre les problèmes de sécurité les plus urgents. Votre équipe doit avoir une visibilité de bout en bout pour sécuriser les environnements complexes. Pour cela, vous devez posséder une plateforme conçue pour importer et normaliser les flux disparates de toute l'entreprise puis fournir des informations à partir de ces données, sans aucun échantillonnage. Surtout que les outils schema-on-read et d'indexation distribuée peuvent accélérer et faciliter la collecte et l'analyse de données provenant de n'importe quelle source.

Au sommet de cette plateforme, un SOC moderne nécessite des outils de sécurité intégrés qui utilisent la threat intelligence et des analyses avancées basées sur les risques pour fournir des informations exploitables en cas de besoin. Ces outils vont jusqu'à hiérarchiser les incidents par risque organisationnel pour que rien n'échappe à votre équipe. Vous avez aussi la possibilité de libérer vos analystes de sécurité pour travailler plus intelligemment en automatisant les tâches répétitives, et ainsi répondre aux menaces en un clin d'œil.

Idéalement, en plus de toute cette intelligence artificielle, un SOC moderne offre également la possibilité de faire appel, en direct, à des experts en sécurité humains qui vous aideront à suivre l'évolution rapide des menaces majeures qui pourraient autrement passer inaperçues.

Ensemble, ces outils assurent une posture de sécurité unifiée, englobant les environnements locaux, hybrides et multicloud. Un SOC réactif fondé sur une plateforme de données puissante apporte des capacités de détection des menaces, d'investigation et de correction plus performantes et plus rapides, tout en consolidant la résilience de votre entreprise et en stimulant ses capacités d'innovation.

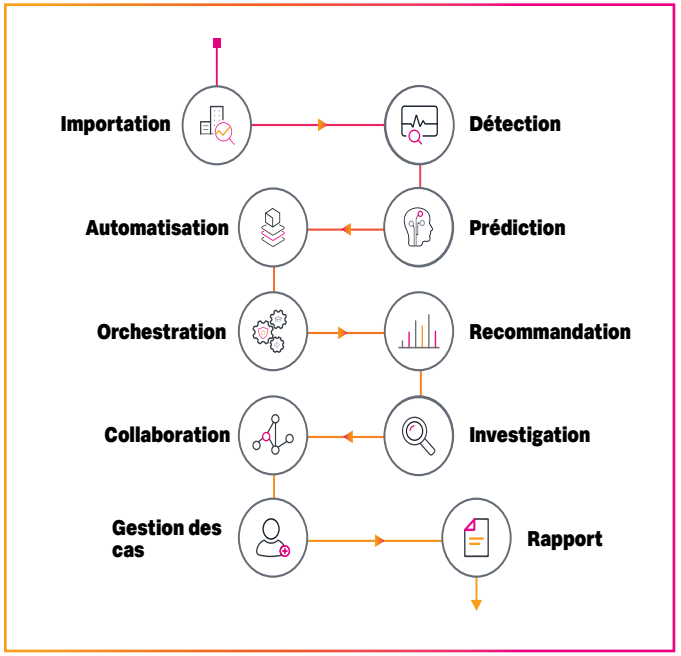
Bâtir un SOC moderne

Votre équipe de sécurité est en première ligne. Elle s'efforce sans cesse d'identifier, d'analyser et de réduire 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 rencontrent.

Mais un SOC moderne, basé sur une plateforme de données unifiée, bénéficie d'une visibilité sur l'ensemble de l'entreprise, et donc d'une surface de travail commune pour tous les membres de l'équipe. En dotant les opérations de sécurité d'une solution unique intégrant les outils des autres fournisseurs de façon transparente, vous épargnerez à votre équipe d'avoir à basculer entre des dizaines de produits. Ajoutez à cela une surface de travail unique pour tous les membres des équipes et vous pourrez libérer du temps à vos analystes pour qu'ils le consacrent à des choses plus importantes.

Un SOC moderne requiert des solutions unifiées et non pas des outils disparates et mal assemblés. Une solution de sécurité orientée données avec de puissantes fonctionnalités d'analyse contribue à optimiser les capacités d'une petite équipe, en leur donnant un aperçu des menaces potentielles pour leur éviter de perdre du temps sur de fausses alertes. Un SOC moderne orienté données est non seulement capable d'exploiter les technologies avancées du machine learning (ML), de l'automatisation et de l'orchestration, mais aussi de la threat intelligence, en une seule solution unifiée.

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. Importation

Comme les données constituent un problème de sécurité, elles sont toutes importantes pour la sécurité. Il est essentiel qu'un SOC moderne puisse importer et normaliser toutes vos données, depuis n'importe quelle source et à l'échelle de l'entreprise, afin de produire des informations. Vous avez également besoin de collecter et d'organiser facilement et efficacement ces données.

2. Détection

Lorsqu'un événement de sécurité survient, vous devez disposer d'outils voués à le détecter aussi vite et précisément que possible. Un SOC moderne peut vous aider à détecter les menaces grâce aux analyses du machine learning et apporter les informations clés nécessaires à votre équipe pour passer à l'action.

3. Prédiction

Imaginez que vous recevez une alerte 30 minutes avant de découvrir un événement de sécurité. Imaginez ce que cela représenterait pour votre SOC. En ayant la possibilité de prédire un événement de sécurité, le SOC peut porter proactivement l'incident à l'attention d'un analyste humain, ou déclencher une réponse standardisée, basée sur un processus prédéfini. Il existe de nouvelles technologies prédictives émergentes qui fournissent aux analystes une alerte précoce, signalent les précurseurs ou les indicateurs d'attaques plus importantes, et identifient les menaces inconnues avant qu'elles ne deviennent des risques réels.

4. Automatisation

L'automatisation est l'une des technologies les plus récentes au service des analystes SOC. Les organisations sont à des stades différents de leurs parcours d'automatisation. Mais en matière d'opérations de sécurité, plus votre SOC est capable d'automatiser les tâches triviales et manuelles, mieux c'est. Les outils d'automatisation de la sécurité transforment les procédures d'opérations standard en playbooks numériques pour accélérer l'investiation des menaces, l'enrichissement, la recherche, le confinement et la correction. Ils achèvent ces processus en 40 secondes environ, contre 30 minutes auparavant. Grâce à l'automatisation, vos analystes peuvent se concentrer sur les priorités qui requièrent l'intelligence humaine.

5. Orchestration

Au fil du temps, vous avez certainement été contraint d'acheter des dizaines de produits pour faire fonctionner votre SOC. Et ce n'était pas parce que vous aviez un budget supplémentaire. Pour la plupart, ces outils sont fonctionnels et consolident votre défense, mais ils n'ont pas évolué au rythme des menaces et d'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 n'avez plus besoin d'ouvrir de nouveaux onglets de navigateur, ni de vous connecter à des solutions spécifiques pour chaque produit, ou encore de copier-coller des informations entre différentes solutions. La possibilité d'orchestrer tous vos produits élimine les efforts superflus, réduit la frustration et aide les analystes à concentrer leur énergie sur des tâches utiles.

6. Recommandation

Lorsqu'un SOC orienté données atteint ce stade, l'ensemble des données utiles pour la sécurité (donc toutes sans exception) sont importées et filtrées par l'intelligence artificielle et des playbooks automatisés, et elles sont étroitement évaluées et gérées par des outils orchestrés. Imaginez que la plateforme qui alimente le SOC puisse aussi indiquer à vos analystes les actions qu'ils devraient entreprendre. Les solutions destinées aux opérations de sécurité modernes en sont capables, grâce aux recommandations. Ces dernières peuvent se présenter sous la forme d'actions individuelles ou de playbooks et sont utiles dans deux cas : 1) pour les nouveaux analystes, la recommandation est un outil pédagogique qui leur permet d'apprendre à agir en cas de menace similaire, et 2) pour les analystes expérimentés, elle sert de seconde opinion ou de rappel.

7. Investigation

Il y a fort à parier que vos analystes SOC se noient dans un océan d'alertes et perdent tellement de temps à s'occuper d'alertes peu fiables qu'ils finissent par abandonner. Un SOC moderne les assiste dans la hiérarchisation des investigations et de la prise en charge des incidents avec précision, confiance et simplicité. Les technologies récentes, comme les alertes basées sur le risque, réduisent le « bruit » pour isoler les plus importantes et détecter les menaces complexes qui pourraient autrement passer inaperçues. Les solutions SOC orientées données automatisent le groupement d'événements connexes en un seul incident afin d'accélérer l'action et la résolution. Tout cela permet de conserver du temps et des ressources, de hiérarchiser les tâches et de fournir des outils coordonnés pour permettre aux analystes de se concentrer sur des investigations et des analyses précises et nuancées qui ne peuvent pas être automatisées.

8. Collaboration

La sécurité est un sport d'équipe qui nécessite coordination, communication et collaboration. Rien ne peut être laissé à l'abandon dans un environnement SOC : les événements doivent être traités complètement. La capacité à faire collaborer en temps réel l'ensemble des outils, des personnes et des processus, avec autant de visibilité et d'informations que possible, est essentielle pour les équipes. Une solution orientée données remplit cette mission et met des informations, des idées et des données clés au premier plan. Ces capacités permettent aux équipes de sécurité de mieux collaborer, d'inviter des personnes extérieures au SOC à participer à la prise en charge des alertes, de partager des informations urgentes et importantes avec des pairs, et enfin de coopérer en tant qu'industrie.

9. Gestion

Même avec la meilleure équipe d'analystes et toutes ces capacités modernes orientées données, soyons réalistes. Les incidents de sécurité ne vont pas disparaître pour autant. Une chose est essentielle : quand les incidents surviennent, les équipes de sécurité doivent être munies de tous les outils nécessaires pour gérer le processus de réponse. Elles doivent disposer de plans de réponse et de workflows de collecte de preuves, de communication de documentation et de suivi chronologique. C'est pourquoi la gestion des incidents est devenue une fonctionnalité de base du SOC moderne.

10. Rapport

On ne peut pas gérer ce qu'on ne mesure pas. Nous vivons dans un monde orienté données et il en va de même pour la sécurité. C'est pourquoi vous pouvez désormais mesurer tous les aspects du processus de sécurité. Des outils de rapport performants fournissent des informations sur l'état des systèmes. Ainsi, les équipes de sécurité peuvent mesurer avec précision où elles en sont et où elles doivent aller. De nos jours, les SOC dépendent souvent de nombreuses plateformes différentes, ce qui empêche d'obtenir des rapports précis et rapides. À cause des défis considérables que les entreprises rencontrent dans le domaine de la conformité et l'exercice de leurs activités sur des marchés troublés, établir des rapports rapides et précis est plus important que jamais.

Splunk entre en jeu

Lancez-vous grâce à la plateforme Splunk®. Splunk est une plateforme unifiée pour la sécurité et l'observabilité. Avec Splunk, les organisations peuvent voir toutes leurs données, récupérer des informations rapidement, répondre avec précision, confiance et simplicité, et tout cela en une seule solution intégrée.

Splunk peut superviser et analyser les données en temps réel, depuis n'importe quelle source et à l'échelle de l'entreprise. Splunk fonctionne dans des environnements multicloud et hybrides. La plateforme fournit des outils d'investigation, d'analyse et d'orchestration robustes à vos analystes SOC pour qu'ils trouvent et corrigent les menaces rapidement et avec précision.

Unifiée et orientée données, la solution Splunk pour les opérations de sécurité rassemble des technologies de pointe pour la gestion des événement et des informations de sécurité (SIEM), l'analyse des comportements des utilisateurs (UBA) et l'orchestration, l'automatisation et la réponse de sécurité (SOAR). Elle intègre enfin la threat intelligence. Splunk s'aligne aussi avec les principaux frameworks comme MITRE ATT&CK, l'Institut national des normes et des technologies (NIST) et la cyber kill chain. Concernant le secteur public, Splunk est conforme aux exigences de sécurité gouvernementales telles que FedRAMP niveau modéré et IL5.

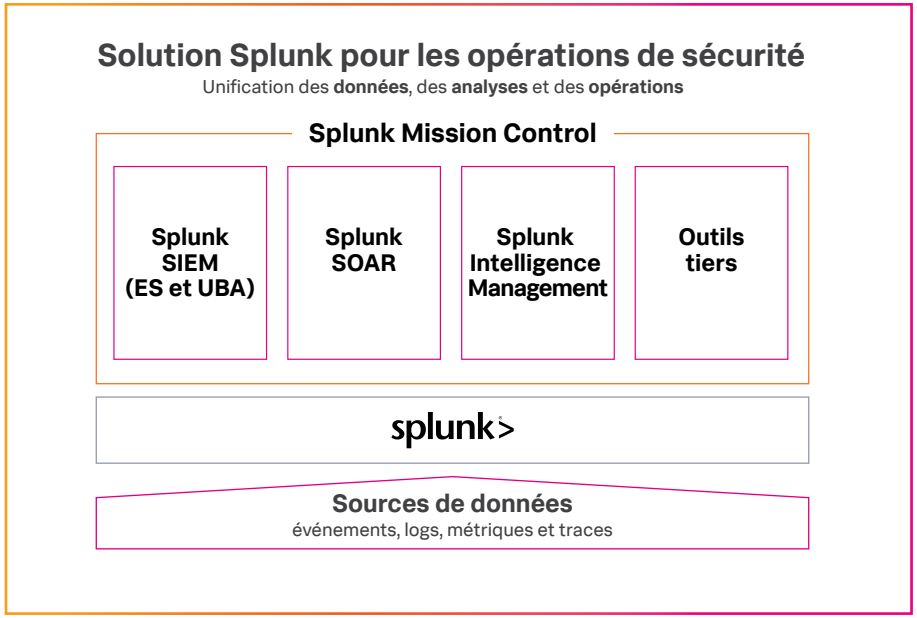
Splunk Enterprise Security (ES) est une solution SIEM orientée données rapide, puissante et flexible, tout en offrant une visibilité sur la position de sécurité de votre organisation pour vous protéger des menaces et réduire les risques à grande échelle. Offrant des capacités inégalées de recherche et de rapport, des analyses avancées, des alertes basées sur les risques, de l'intelligence intégrée et des contenus de sécurité prêts à l'emploi, Splunk ES accélère la détection et l'investigation pour permettre à vos analystes SOC d'évaluer rapidement l'ampleur des menaces urgentes et de passer à l'action. Splunk ES combine le machine learning, la détection des anomalies et les corrélations basées sur des critères, au sein d'une même solution d'analyse de sécurité.

Avec Splunk UBA, l'outil d'analyse des comportements des utilisateurs de Splunk, les organisations sont capables de détecter les menaces inconnues et les comportements anormaux en utilisant le machine learning. La détection des menaces avancées révèle les anomalies et les menaces inconnues ignorées par les outils de sécurité traditionnels. Des centaines d'anomalies peuvent être automatiquement reliées à une même menace : pour vos analystes de sécurité, c'est un gain d'efficacité considérable. De plus, les capacités d'investigation de pointe et les puissantes références comportementales permettant d'évaluer n'importe quelle entité, anomalie ou menace accélèrent les activités de traque.

Splunk SOAR, la solution Splunk d'orchestration, d'automatisation et de réponse de sécurité, permet à votre équipe de travailler plus intelligemment, de répondre plus vite et de renforcer les défenses de sécurité de l'organisation. Splunk SOAR automatise les tâches répétitives pour que votre équipe consacre son temps et son attention aux incidents et aux actions les plus urgents. La solution réduit les temps de séjour grâce aux investigations automatisées et diminue les délais de réponse grâce à des playbooks qui s'exécutent en un clin d'œil. Le SOAR s'intègre également à votre infrastructure de sécurité existante pour que chacun participe activement à la stratégie de défense, de façon harmonieuse.

Splunk Intelligence Management, l'outil Splunk de threat intelligence, automatise l'orchestration des données pour centraliser, normaliser et hiérarchiser les informations à chaque étape des opérations de sécurité. Il élimine les silos de données pour aligner l'efficacité de la sécurité sur les objectifs commerciaux en améliorant la cyber-résilience et l'efficacité opérationnelle. Splunk Intelligence Management permet à votre équipe de sélectionner facilement des flux d'informations : open source, fournisseurs d'informations premium et collecte des historiques d'événements et d'alertes. Elle peut ensuite appliquer des scores de priorité, des listes blanches et des filtres basés sur les types d'indicateurs ou les attributs, puis envoyer ces données préparées à des dépôts ou à une application désignée.

Splunk Mission Control est une expérience unifiée qui modernise et optimise vos opérations de sécurité. Cette solution cloud SaaS vous permet de détecter, gérer, analyser, rechercher, isoler et corriger les menaces et autres problèmes de sécurité de haute priorité sur l'intégralité du cycle de vie de l'événement, le tout à partir d'une même surface de travail. Toutes vos données de sécurité et vos outils sont intégrés dans Splunk Mission Control, qu'ils soient locaux ou cloud, pour opérer en tant que système de défense unifié contre les cybermenaces de tout genre.



Lancez-vous.

Découvrez comment la solution Splunk pour les opérations de sécurité peut vous aider à moderniser votre SOC.

22-18111-Splunk-10-Essential-Capabilities-of-a-Modern-SOC-109

splunk> turn data into doing