LIVRE BLANC

Les cinq fonctionnalités essentielles d'un SOC orienté analyse

splunk>
turn data into doing™

À mesure que le volume et la complexité des cyberattaques s'accélèrent, les centres d'opérations de sécurité (SOC) sont devenus le centre d'attention pour réunir les personnes, les processus et les technologies nécessaires à la défense et à la réponse d'une organisation aux attaques. Cependant, la plupart des responsables IT et commerciaux ne connaissent pas vraiment leur niveau réel de vulnérabilité aux risques. Ils n'ont pas de visibilité sur l'ensemble des vulnérabilités potentielles qui pourraient être exploitées, et encore moins de moyen de les corriger.

Mais les entreprises peuvent se tenir informées des menaces modernes en adoptant un SOC orienté analyse. Un SOC efficace peut améliorer la capacité de détection et de réaction face aux incidents d'une organisation, tout en accélérant et en améliorant sa position de sécurité.

L'ancien SOC

Le rôle que joue un SOC dans la prévention des cyberattaques est relativement simple. Plutôt que de répondre aux cyberattaques de manière non coordonnée, un SOC permet aux organisations IT de fournir rapidement un contexte en centralisant la gestion de la sécurité autour d'un ensemble bien défini de processus.

Un SOC s'appuie également sur la gestion des modifications, la maintenance des dispositifs de sécurité ainsi que sur le suivi des journaux et des événements principalement gérés par une plateforme de gestion des informations et des événements de sécurité (SIEM). La plupart des organisations IT dépendent déjà de la sécurité et d'environnements IT ayant dépassé la capacité de gestion manuelle par l'humain.

Une étude récente de Gartner a révélé qu'un **SOC orienté informations** améliore considérablement la position de sécurité globale d'une organisation en offrant des capacités d'obtention d'informations sur les menaces, d'analyse, d'automatisation et d'investigation via une plateforme de sécurité adaptative.

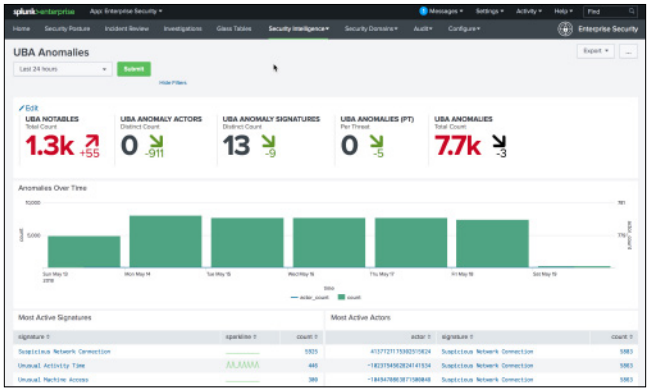
Les fonctionnalités essentielles d'un SOC orienté analyse

Selon Gartner, **les cinq fonctionnalités essentielles** pour disposer d'un SOC intelligent ou orienté analyse sont les suivantes : l'analyse avancée, l'intelligence des menaces, l'automatisation, la capacité à traquer et à investiguer proactivement et l'adoption d'une architecture de sécurité adaptative.

L'évolution d'un SOC	
SOC virtuel commun	SOC composé d'analystes à distance sans installation dédiée.
NOC/SOC multifonctionnel	Lorsque les organisations combinent des capacités opérationnelles comme le NOC ou l'assistance technique.
SOC de commande	Un SOC qui coordonne les autres SOC. Il est souvent utilisé dans les entreprises multinationales.
SOC cogéré	Commun lorsqu'un MSSP exerce une partie des fonctions du SOC.
SOC d'urgence	Organisé comme un service de pompiers volontaires : lorsqu'un incident survient, une équipe est réunie pour l'analyser et y faire face.

Analyse avancée et machine learning

Une plateforme de sécurité moderne associe outils qualitatifs avancés axés sur des algorithmes de machine learning, outils d'exploration de données et simulations avec des approches traditionnelles d'interrogation et de consultation des données. Les informations de sécurité doivent être appliquées de manière cohérente et complète pour identifier les nouvelles menaces émergentes dans le contexte de tout changement inhabituel dans le comportement de l'utilisateur final.



Splunk® Enterprise Security (ES) intègre des analyses avancées via des algorithmes et des techniques de machine learning pour identifier les anomalies et les modèles qui peuvent accélérer les enquêtes et les découvertes. Le machine learning permet non seulement de repérer les tendances et les aberrations, mais également d'éliminer le « bruit » généré par tous les événements se produisant sur de grandes quantités de données. Ces techniques de machine learning peuvent également être adaptées à l'aide de la **boîte à outils de machine learning de Splunk** et de **Splunk User Behavior Analytics**.

Intelligence des menaces

Les équipes de sécurité doivent être en mesure d'utiliser l'intelligence des menaces tactiquement et stratégiquement. Il ne suffit pas de recueillir des informations sur l'intelligence des menaces dans le cadre d'un effort systématique pour éliminer les vulnérabilités.

Les indicateurs de menace potentielle, tels que les hachages de fichiers, les adresses IP, les valeurs de registre, les noms de service, les processus, les URL, les attributs d'e-mail et les attributs de certificat, comme le nom commun ou le numéro de série, doivent être mis en corrélation avec les vulnérabilités identifiées, les sources de menace, etc.

Splunk ES inclut un cadre pour recueillir l'intelligence des menaces qui recueille, rassemble et déduplique automatiquement les flux de menaces provenant d'un vaste ensemble de sources. Le cadre se compose d'entrées modulaires qui collectent et assainissent les données d'intelligence des menaces et les demandes générant des recherches pour réduire les données et optimiser les performances.

Le cadre comprend également un certain nombre de tableaux de bord d'audit permettant d'avoir une vue d'ensemble de l'extraction, la normalisation, la persistance et l'analyse de l'intelligence des menaces.

Il donne accès à plus de 30 sources prêtes à l'emploi, avec prise en charge des normes STIX/TAXII, OpenIOC et Facebook. Il inclut également des tableaux de bord des activités et des artefacts de menace qui peuvent être déployés pour identifier rapidement les différents types de menace.

Cadre d'intelligence des menaces

Automatisation

Dès que possible, les organisations IT doivent automatiser les fonctions de sécurité selon leur profil de risque. La semi-automatisation est parfois nécessaire parce qu'un ancien SOC peut nécessiter un effectif important.

En matière de cybersécurité, le choix des outils à utiliser ne doit pas se faire lors d'une intrusion. La réponse à une attaque doit être déclenchée en quelques secondes pour éviter la perte d'autres données. Pour des raisons juridiques, les organisations doivent veiller à ne pas polluer la piste d'audit ou à ne pas invalider les preuves en se basant uniquement sur des processus manuels biaisés.

Splunk ES comprend un cadre commun pour interagir avec les données et appeler des fonctions.

Le cadre "Adaptive Response" **fait partie de Splunk Enterprise Security** et permet d'optimiser la détection des menaces et les mesures correctives grâce à des contextes axés sur les flux de travail.

Adaptive Response peut être utilisé pour l'automatisation afin d'éliminer les tâches de routine, d'accélérer la détection et d'uniformiser les réponses. Le cadre offre la possibilité d'enregistrer et de configurer des actions de réponse automatisée ou assistée, permettant aux organisations d'exploiter efficacement leurs produits de sécurité existants, dont les pare-feu, les IDS/IPS, les points de terminaison, l'intelligence des menaces, la réponse aux incidents et l'identité. Splunk ES fait alors office de plateforme centrale d'informations sur la sécurité.

Les analystes peuvent également automatiser les actions ou les examiner individuellement pour obtenir rapidement plus de contexte ou prendre des mesures adaptées dans un écosystème de sécurité multi-fournisseurs.

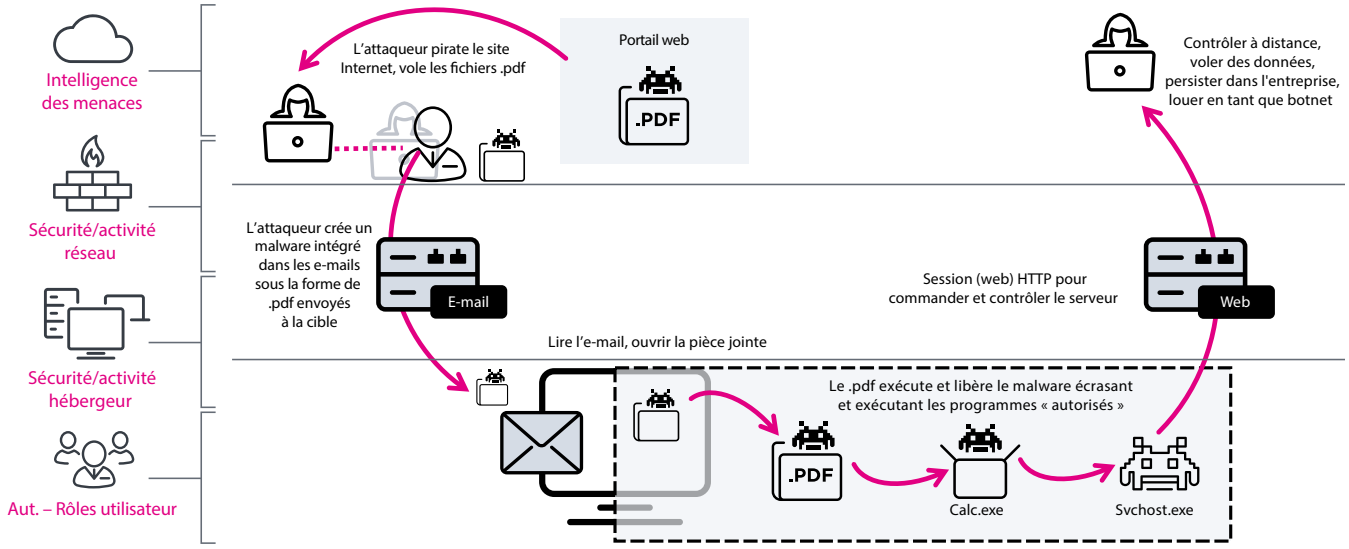
Splunk Adaptive Response

Traquer et investiguer proactivement

Si les défenses du périmètre de l'organisation ont déjà été franchies, les équipes de sécurité IT ont besoin d'outils facilitant la découverte des logiciels malveillants, où qu'ils se cachent dans l'organisation. La traque et l'investigation des logiciels malveillants nécessitent non seulement la possibilité de passer d'un ensemble de données à un autre, mais également de recouper et de mettre en corrélation leurs relations avec les autres entités, en plus d'être en mesure de visualiser l'activité historique.

En fonction de la maturité organisationnelle, du domaine et de l'expérience produit, Splunk ES peut être utilisée avec des données recueillies par des logiciels et du matériel de sécurité de réseau et de point de terminaison de tiers ainsi qu'un certain nombre d'applications d'informations de sécurité.

Splunk ES peut notamment aider les organisations dans la collecte automatique de renseignements sur les menaces et le partage d'informations entre les différents outils. La plateforme de Splunk peut également servir à opérationnaliser l'intelligence des menaces afin de mettre en place une plateforme automatisée de traque et de gestion des menaces. Splunk ES peut aider les organisations à passer d'une visibilité nulle des menaces à une plateforme riche et sophistiquée capable d'automatiser la traque des menaces en quelques semaines.



La ville de Los Angeles intègre le partage d'informations de sécurité en temps réel entre plus de 40 agences municipales

Pour protéger son infrastructure numérique, la ville de Los Angeles a besoin d'évaluer sa position de sécurité et d'intelligence des menaces pour ses services et ses parties prenantes.
Par le passé, les plus de 40 agences de la ville disposaient de mesures de sécurité disparates. Celles-ci compliquaient le regroupement et l'analyse des données. Los Angeles était à la recherche d'une solution SaaS évolutive de gestion des informations et des événements de sécurité (SIEM) pour identifier, hiérarchiser et réduire les menaces, gagner en visibilité sur les activités suspectes et évaluer les risques de toute la ville. Depuis le déploiement de Splunk Cloud et de Splunk Enterprise Security (ES), la ville a constaté plusieurs avantages, notamment :

- la création d'un centre des opérations de sécurité (SOC) à l'échelle de la ville ;
- l'obtention d'informations sur les menaces en temps réel ;
- la réduction des dépenses opérationnelles.

Le SOC intégré de la ville fait plus que recueillir des informations, il en fournit également. Il traduit les données de Splunk Cloud en informations utiles sur les menaces. La ville partage ses conclusions avec ses agences ainsi qu'avec des parties prenantes externes telles que le FBI, le département de la Sécurité intérieure, le Secret Service et d'autres organismes du maintien de l'ordre. Grâce à ces informations, la ville collabore avec les agences fédérales pour identifier les risques et développer des stratégies afin de prévenir les intrusions sur le réseau.

En associant son SOC intégré aux multiples fonctionnalités SIEM de Splunk Cloud et ES, Los Angeles a répondu à la demande de son maire en transformant son patchwork de mesures de sécurité en une stratégie de cybersécurité cohérente et globale.

Adopter une architecture de sécurité adaptative

Les architectures de sécurité statiques traditionnelles axées sur des contrôles de sécurité, des technologies préventives et des révisions stratégiques périodiques sont désuètes et inefficaces. Une architecture de sécurité adaptative telle que **décrite par Gartner** doit permettre de prévenir, de détecter, de réagir et de prévoir.

Les architectures de sécurité impliquent généralement de nombreuses couches d'outils et de produits qui ne sont pas conçus pour fonctionner ensemble, et les ponts mis en place par les équipes de sécurité entre les différents domaines comportent des lacunes. Pour mettre en place une bonne architecture de sécurité adaptative capable de prévenir, de détecter, de réagir et de prévoir, les organisations ont besoin :

- d'une corrélation entre toutes les données pertinentes pour la sécurité ;
- d'un aperçu des architectures de sécurité existantes ;
- de techniques analytiques avancées telles que le machine learning ;
- d'automatisation, dans la mesure du possible ;
- d'intégration à l'écosystème de sécurité avec un enrichissement bidirectionnel du contexte.

La plateforme Splunk comble ces lacunes grâce à son cadre **Adaptive Response**. Ce cadre, une interface commune pour automatiser la récupération, le partage et la réponse dans des environnements multi-fournisseurs, fait partie de Splunk Enterprise Security. Splunk ES permet aux équipes du SOC de mettre en œuvre avec succès une architecture de sécurité adaptative en permettant de mettre en corrélation toutes les données pertinentes pour la sécurité, d'obtenir des informations à partir des architectures de sécurité existantes, d'accéder à des analyses avancées, d'automatiser les mesures correctives et de partager de manière bidirectionnelle les renseignements de sécurité avec des produits et services tiers. Grâce à cela, le SOC peut détecter, répondre, prévoir et prévenir plus efficacement les problèmes de sécurité.

Un SOC moderne pour combattre les menaces modernes

La plupart des SOC existants sont obsolètes et fondés sur d'anciennes plateformes SEIM incapables de faire face à la quantité de données qui doit être analysée ou de suivre le rythme des changements rapides dans un environnement IT moderne.

SAIC construit un nouveau centre des opérations de sécurité de classe mondiale

SAIC est un intégrateur de technologies de premier plan, spécialisé dans les marchés de l'information technique, de l'ingénierie et de l'entreprise. L'entreprise avait besoin de mettre en place un SOC robuste et une équipe de réponse aux incidents informatiques (CIRT) pour se défendre contre les cyberattaques. Depuis le déploiement de la plateforme Splunk Enterprise, cette entreprise a constaté plusieurs avantages, notamment :

- l'amélioration de la position de sécurité et de la maturité opérationnelle ;
- plus de 80 % de réduction des délais de détection et de traitement des incidents ;
- une visibilité complète sur l'environnement de l'entreprise.

Après la scission de l'entreprise SAIC d'origine en deux entreprises en 2013 pour éviter les conflits d'intérêts organisationnels, SAIC a dû créer un SOC dans le cadre de son nouveau programme de sécurité. Bien que l'entreprise disposait de la plupart des outils de sécurité dont elle avait besoin, SAIC n'avait pas de solution SIEM pour consolider ses défenses. La solution SIEM traditionnelle utilisée par l'entreprise d'origine comme outil de base pour les enquêtes de sécurité présentait des limites. SAIC a complété le SIEM avec Splunk Enterprise en utilisant la plateforme pour la détection d'incidents via des recherches de corrélation et pour les enquêtes sur les incidents. Le personnel des opérations IT de SAIC utilise désormais également la solution Splunk pour la supervision du réseau, la gestion des performances, l'analyse des applications et le reporting.

Après avoir commencé à constituer son nouveau SOC, SAIC a décidé de s'appuyer sur Splunk comme plateforme unique d'informations de sécurité pour tous ses besoins de type SIEM, y compris la détection d'incidents, les investigations et le reporting pour la supervision, l'alerte et l'analyse en continu. SAIC a également acheté Splunk Enterprise Security (ES) pour ses recherches de corrélation pré-conçues, son flux de travail d'examen des incidents, ses rapports, ses tableaux de bord et ses flux d'intelligence des menaces. SAIC a commencé à indexer quotidiennement des centaines de Go de données dans la solution Splunk à partir de diverses sources de données, dont des systèmes de pare-feu, de détection des intrusions, d'antivirus et de scanner de vulnérabilité.

Au vu de la complexité des défis de sécurité auxquels chaque organisation est confrontée aujourd'hui, disposer d'un SOC est essentiel. La question à laquelle de nombreuses organisations sont confrontées est de savoir si elles doivent créer et gérer un SOC en interne ou si elles doivent s'en remettre à un fournisseur de services de sécurité gérés pour s'occuper de leur sécurité. La bonne réponse variera en fonction de la taille et de la nature du risque auquel chaque organisation peut être confrontée.

Quel que soit leur choix, chaque organisation aurait intérêt à évaluer sa position de sécurité en fonction des caractéristiques du SOC décrites par **Gartner**. De nombreuses organisations découvriront qu'elles ne sont pas aussi proactives en matière de sécurité IT qu'elles ne le pensaient. Bien que cela puisse poser problème, le temps et les dépenses nécessaires à la mise en place d'un SOC axé sur l'analyse ne sont pas aussi élevés qu'auparavant. Les capacités de sécurité IT qui étaient autrefois l'apanage des agences de sécurité gouvernementales et des entreprises du classement Fortune 100 sont aujourd'hui accessibles à toutes les entreprises, quelle que soit leur taille.

Vous souhaitez en savoir plus sur la façon dont les clients de Splunk utilisent Splunk Enterprise Security pour alimenter leur SOC axé sur l'analyse et améliorer leur position de sécurité ? Téléchargez notre **e-book client gratuit**.

Ou **contactez un expert Splunk**.

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

2020-Splunk-SEC-5-essential-capabilities-of-analytics-driven-SOC-107-WP_fr