LIVRE BLANC

Les 10 fonctionnalités essentielles d'un SOAR de pointe

Répondez plus rapidement aux menaces grâce à l'orchestration et à l'automatisation de la réponse de sécurité

splunk>
turn data into doing

La cybersécurité évolue

Si vous interrogez les professionnels de la sécurité sur les défis auxquels ils sont confrontés dans le domaine de la cybersécurité, il y a de fortes chances que les mêmes thématiques reviennent. Elles sont nombreuses, mais en voici quelques exemples :

- pénurie de talents qualifiés en cybersécurité ;
- volume élevé d'alertes de sécurité ;
- trop de produits de sécurité ponctuels à gérer ;
- manque d'intégration entre les produits ;
- incapacité à faire évoluer les opérations de sécurité dans le temps ;
- augmentation des coûts et réduction des budgets ;
- sophistication croissante des logiciels malveillants ;
- lenteur de la détection des menaces et de la réponse.

Compte tenu de ces défis, il n'est pas surprenant que les équipes de sécurité se sentent constamment dépassées.

Beaucoup d'équipes se sont tournées vers les outils d'orchestration, d'automatisation et de réponse de sécurité (SOAR) pour y remédier. Une solution SOAR peut orchestrer les actions de sécurité (investigations, triage et réponse) entre les différents produits de sécurité de l'arsenal d'une équipe, et automatiser les tâches de sécurité répétitives généralement réalisées à la main.

Mais toutes les solutions SOAR ne se valent pas. Une solution SOAR de pointe offre un ensemble de fonctionnalités qui peuvent entièrement révolutionner l'approche de votre équipe en matière d'opérations de sécurité. Ces capacités vous permettront de :

- travailler plus intelligemment en automatisant les tâches manuelles et répétitives ;
- réagir plus rapidement et réduire les temps de séjour grâce à l'automatisation de la détection, de l'analyse et de la prise en charge des incidents ;
- aider votre équipe de sécurité à automatiser les opérations de sécurité et à libérer du temps pour se consacrer à d'autres activités stratégiques.

Nous présentons ci-dessous les 10 fonctionnalités essentielles d'une solution SOAR de pointe, qui aideront votre équipe de sécurité à reprendre le contrôle sur le désordre.

Les fonctionnalités essentielles d'un SOAR de pointe	
Orchestration	C'est la coordination, par des machines, d'une série d'actions de sécurité interdépendantes sur un écosystème IT complexe. Cette coordination se double de l'automatisation des tâches sur de multiples produits et workflows.
Automatisation	C'est l'exécution par une machine d'actions de sécurité ayant le pouvoir, par programmation, de détecter, analyser et prendre en charge les cybermenaces sans intervention humaine. L'automatisation de sécurité fait l'essentiel du travail de votre personnel de sécurité, en lui évitant de parcourir et traiter manuellement toutes les alertes qui surviennent.
Gestion des événements et des alertes	Une fois les données ingérées dans une solution SOAR, les alertes entrantes doivent être mises en file d'attente et hiérarchisées. L'investigation doit être réalisée au moyen d'actions manuelles ou automatisées pour atteindre le plus haut niveau possible de productivité et de précision.
Threat intelligence	Les équipes de sécurité doivent pouvoir exploiter la threat intelligence la plus récente sans épuiser leurs ressources. Une bonne threat intelligence doit également inclure des options de notation pour mettre en évidence les sources prioritaires pour les analystes.
Gestion des investigations et collaboration	La gestion des investigations doit adopter une vision plus large et interfonctionnelle du cycle de vie d'un incident, de sa création à sa résolution. Il doit être possible de confirmer, agréger et remonter plusieurs alertes et événements comme un seul cas. C'est un véritable atout pour l'efficacité de la collaboration et de la communication au sein de l'équipe de sécurité de l'organisation, ce qui accélère la résolution des événements de sécurité.

Métriques et rapports	Les métriques et les rapports sont indispensables pour comprendre et quantifier à peu près tout, et les solutions SOAR ne font pas exception. Ce sont les métriques qui permettent d'évaluer l'efficacité d'une solution SOAR et d'identifier les améliorations pouvant doper le retour sur investissement.
Mobilité	Il est essentiel pour une solution SOAR d'offrir des capacités d'accès, d'interactivité et de contrôle de la plateforme sur l'appareil mobile des analystes. Ils pourront ainsi exécuter des playbooks en déplacement, examiner les artefacts de sécurité et trier les événements sans ouvrir leur ordinateur portable, répondre aux notifications et rester joignables à tout moment.
Évolutivité	Une solution SOAR doit évoluer avec votre organisation. Comme de nouveaux scénarios d'utilisation viennent régulièrement s'ajouter au fil du temps, la plateforme doit être conçue de manière à permettre une évolution verticale (augmentation du CPU et de la RAM) et horizontale (augmentation du nombre d'instances de serveur du déploiement).
Ouverture et extensibilité	Une solution SOAR doit être conçue dans une optique d'ouverture et d'extensibilité. Elle doit aisément accueillir de nouveaux scénarios de sécurité, produits, actions et playbooks.
L'appui de la communauté	Une solution SOAR doit prendre en charge un modèle communautaire reposant sur un écosystème ouvert pour le développement d'applications. C'est un puissant facteur de succès à long terme car cela évite la dépendance vis-à-vis des fournisseurs, et permet de changer facilement de technologie sans altérer les playbooks automatisés.

Examinons de plus près chacune de ces fonctionnalités :

Orchestration

Lorsqu'une équipe de sécurité répond à un incident, elle utilise une multitude d'outils de sécurité différents. Chacun de ces outils joue un rôle différent dans un workflow défini. Vous pouvez, par exemple, demander à VirusTotal de vérifier la réputation d'un fichier, utiliser votre pare-feu pour bloquer une adresse IP, puis utiliser votre outil de sécurité de point de terminaison pour bloquer un exécutable. Sans orchestration, l'équipe de sécurité coordonnerait ces workflows manuellement. Mais une solution SOAR peut s'intégrer à tous ces outils de sécurité déployés via des API, puis coordonner leurs différents workflows pour détecter, analyser ou traiter des incidents de sécurité spécifiques. Pour faire une analogie, si vos outils de sécurité sont les instruments d'un orchestre symphonique, votre solution SOAR en est le chef d'orchestre : elle s'assure que chaque instrument joue en synchronisation et à temps.

Pour évaluer une solution SOAR, il faut rechercher une fonction d'orchestration capable de diriger et superviser toutes les activités liées à un scénario de sécurité donné du début à la fin. Elle doit aussi pouvoir importer des données de sécurité à partir de n'importe quelle source de données, dans n'importe quel format. De plus, un orchestrateur doit également faire en sorte que les données de sortie d'une action soient correctement lues, normalisées et structurées afin que les prochaines actions puissent les exploiter.

Automatisation

Pour la plupart des analystes en sécurité, une journée de travail déborde de tâches et d'opérations répétitives et lassantes. Ces actions sont réalisées manuellement par l'équipe. L'automatisation à l'aide de playbooks doit permettre à l'équipe de sécurité d'exécuter tout un ensemble d'actions de ce type en quelques secondes plutôt qu'en quelques minutes ou plusieurs heures, certaines prennent même des jours ou des semaines. Prenons l'exemple des investigations de phishing : elles nécessitent généralement plusieurs actions réparties sur quatre à cinq outils de sécurité différents, et prennent environ 40 minutes si elles sont effectuées manuellement. Avec un playbook automatisé, elles devraient désormais prendre moins d'une minute. De cette manière, une solution SOAR peut considérablement réduire le temps moyen de détection (MTTD) et le temps moyen de réponse (MTTR).

Les playbooks doivent être faciles à créer et à modifier. L'éditeur d'automatisation est l'outil qui permet à un analyste ou un responsable de codifier des processus sous la forme de playbooks d'automatisation. L'éditeur doit permettre à la fois la modification du code source et l'édition visuelle. De cette façon, tous les membres de l'équipe de sécurité, quelles que soient leurs préférences et leur expertise en matière de code, pourront créer des playbooks complets et sophistiqués. Lors de la création du playbook dans un éditeur visuel, le code source du playbook résultant doit être généré en temps réel et être accessible à l'auteur. Il doit être possible de basculer entre modification du code source et éditeur visuel en toute transparence.

Gestion des événements et des alertes

Juste après l'importation des données, la gestion des événements et des alertes doit mettre les événements et alertes entrants en file d'attente et les hiérarchiser. Les alertes peuvent ainsi être rapidement consultées et traitées efficacement, sans recherche approfondie ni changement de contexte. Les événements et les alertes doivent inclure un indicateur d'état (nouveau, ouvert ou fermé), un indicateur de gravité et un indicateur de sensibilité à code couleur pour faciliter l'assimilation des informations. Les attributs techniques d'un événement ou d'une alerte de sécurité doivent être organisés de manière à permettre une compréhension rapide du scénario de sécurité. Vous devez notamment disposer d'une vue organisée des données telles que les adresses IP, les domaines, les hashes de fichiers, les noms d'utilisateur et les adresses e-mail. Un analyste de sécurité doit être en mesure de lancer sur ces données des actions d'investigation, de confinement ou de réponse (ou une série d'actions, sous la forme de playbooks), en toute fluidité.

La plateforme doit enfin fournir un journal d'activité complet affichant un enregistrement de toutes les actions exécutées à la suite d'une alerte, qu'elles aient été initiées manuellement ou via une procédure d'automatisation. Chaque action doit présenter ses résultats en indiquant clairement s'il s'agit d'un échec ou d'une réussite.

Threat intelligence

La threat intelligence est essentielle pour aider les analystes à comprendre les actions de l'acteur malveillant et atténuer tout dommage supplémentaire pour l'entreprise. Il existe plusieurs types d'informations (stratégiques, techniques et opérationnelles) qui sont collectées et consolidées à partir de sources externes et internes. Une fois les informations agrégées en un seul endroit, les données sont ensuite évaluées dans le contexte de leur source et de leur fiabilité, puis analysées pour déterminer quels éléments de données sont importants pour aider à prendre des décisions rapides et efficaces.

De nombreuses équipes de sécurité utilisent aujourd'hui la threat intelligence pour fournir à leurs analystes un contexte et des éléments d'information pertinents pour les aider à comprendre la menace. Mais bien souvent, ils doivent naviguer parmi une multitude d'interfaces différentes pour comprendre les liens entre toutes ces informations. Même les flux de threat intelligence peuvent envoyer une quantité écrasante d'indicateurs qu'il serait impossible de suivre manuellement. Grâce à l'orchestration et à l'automatisation, les équipes de sécurité visualisent rapidement les informations agrégées sur une même plateforme et prennent des décisions rapides et éclairées qui peuvent être automatisées sans aucune interaction humaine.

Gestion des investigations et collaboration

Une fois les alertes ou les événements confirmés et remontés, un composant de gestion des investigations doit prendre le relais et ouvrir un cycle élargi et interfonctionnel allant de la création à la résolution. La solution SOAR va considérer plusieurs événements, les confirme, les regrouper et les transformer en un seul cas. L'interface de gestion des investigations doit permettre l'ajout de données techniques pertinentes telles que les données source de l'alerte et les résultats des actions. L'interface doit aussi prendre en charge l'ajout de données non techniques utiles : notes, mémos, e-mails, captures d'écran, enregistrements et autres fichiers quelconques pouvant avoir une importance pour l'investigation. Chaque modification de l'investigation doit être consignée dans une trace d'audit exportable.

Il doit aussi être facile d'associer la gestion des investigations aux processus existants d'une organisation. De nombreuses organisations ont créé des procédures opérationnelles standards (SOP) pour la réponse aux incidents. La fonctionnalité de gestion des investigations doit donner à l'utilisateur les moyens

de définir des étapes calquées sur ses processus, et de les enregistrer comme modèles. Il doit pouvoir décomposer la SOP en plusieurs étapes comprenant chacune une ou plusieurs tâches, qui seront ensuite attribuées à différents propriétaires. L'interface doit fournir une indication de la progression et de l'état de l'investigation.

Une solution SOAR de pointe doit intégrer des fonctionnalités de collaboration. Parallèlement au workflow d'investigation ou de réponse, elle peut inclure une messagerie instantanée ou offrir la possibilité d'ajouter des notes aux investigations et de les partager, permettant ainsi la collaboration en contexte. En adjoignant la messagerie et les notes en temps réel aux informations sur les événements, les alertes et les cas, les analystes atteignent un niveau de connaissance de la situation qui permet une résolution efficace et rapide des incidents de sécurité. Ces fonctions produisent également une piste d'audit facile à suivre. Les étapes de la collaboration sont idéalement enregistrées et organisées parallèlement aux données d'événement et aux actions pertinentes qui ont été capturées. Les choses sont très différentes si votre communication se fait sur un outil externe, séparément des informations du workflow de votre solution SOAR.

Métriques et rapports

Une équipe de sécurité doit pouvoir mesurer facilement l'état de ses opérations de sécurité, dans une optique d'amélioration continue. Il est donc impératif de disposer de métriques et de rapports fiables. Ils aident l'équipe de sécurité à comprendre l'impact de l'automatisation et à identifier les améliorations pouvant augmenter le retour sur investissement.

L'automatisation est utilisée pour accroître l'efficacité de plusieurs fonctions du SOC (centre des opérations de sécurité). Il est donc essentiel de connaître le gain quantitatif de performance et les économies de ressources offerts par l'automatisation, et de pouvoir consulter ces informations sur un tableau de bord.

Une large sélection de métriques de performance devraient être disponibles dans une solution SOAR : temps moyen de résolution (MTTR), temps de séjour moyen (MDT), heures d'analystes économisées grâce à l'exécution automatisée, nombre d'équivalents temps plein (ETP) gagnés grâce à l'exécution automatisée, temps moyen économisé par exécution de playbook, économies réalisées (coût ETP x ETP économisés), nombre total d'alertes ouvertes, alertes ouvertes et fermées par jour (heure, semaine, mois) et performances par rapport aux accords de niveau de service (SLA). Toutes ces informations doivent être faciles à organiser et à agréger dans des rapports destinés aux dirigeants et aux RSSI afin de présenter rapidement l'état général des opérations de sécurité ainsi que les améliorations apportées par le SOAR.

Mobilité

Les solutions SOAR sont conçues pour réduire les temps de réponse. Pour réagir rapidement, les analystes de sécurité doivent être joignables lorsqu'un cas ou une alerte de sécurité nécessite une intervention humaine. Mais les analystes ne sont pas toujours assis à leur bureau devant leur ordinateur, prêts à répondre aux notifications à tout moment.

C'est pourquoi il est essentiel de fournir des capacités d'accès, d'interactivité et de contrôle sur l'appareil mobile des analystes. Ils pourront ainsi exécuter des playbooks en déplacement, examiner les artefacts de sécurité et trier les événements sans ordinateur portable, répondre aux notifications et rester joignables à tout moment.

Évolutivité

Une solution SOAR doit évoluer avec vous et votre organisation. Vous allez nécessairement ajouter de nouveaux scénarios d'utilisation au fil du temps, et ils vont accroître la charge de calcul qui pèse sur la plateforme.

Le moteur d'automatisation doit être conçu de manière à permettre une évolution verticale (augmentation du CPU et de la RAM) et horizontale (augmentation du nombre d'instances de serveur) pour optimiser les performances et protéger le retour sur investissement de l'automatisation.

Ouverture et extensibilité

Une solution SOAR doit être conçue dans une optique d'ouverture et d'extensibilité. On doit pouvoir lui incorporer facilement de nouveaux scénarios de sécurité, de nouveaux produits, de nouvelles actions et de nouveaux playbooks. Sans cela, le SOAR peut perdre de sa valeur avec le temps.

Avec un écosystème ouvert reposant sur des normes et un modèle de programmation communs, les équipes de sécurité se bénéficient dès le départ de plusieurs

avantages. Les nouvelles technologies doivent être rapidement intégrées dans la plateforme sans qu'il ne faille modifier le cœur de celle-ci, et sans affecter les playbooks automatisés. Les utilisateurs peuvent développer des intégrations supplémentaires sans l'autorisation du fournisseur SOAR ni cycles de développement. Ils peuvent par exemple écrire leurs propres intégrations, développer des applications maison ou créer une API d'accès anticipé à partir d'un fournisseur.

L'appui de la communauté

Le paysage de la sécurité évolue constamment et il faut donc qu'une communauté de professionnels travaillent ensemble et partagent des procédures, des bonnes pratiques et des stratégies pour faire face aux dernières menaces. Une solution SOAR doit appuyer un modèle communautaire robuste et faciliter le partage des intégrations d'applications et des procédures.

L'envergure de la base installée d'une plateforme est un bon indicateur du potentiel de collaboration de sa communauté. La plupart des utilisateurs apprécient de pouvoir puiser dans l'expérience de leurs confrères. Une communauté vaste et active offre la possibilité de partager des procédures et des applications, et d'échanger des idées pour de nouveaux cas d'usage de l'automatisation. De plus, l'implication du fournisseur dans la communauté est un signe fort d'engagement envers elle et envers la collaboration.

Le SOAR peut-il vous aider à améliorer vos opérations de sécurité ? Découvrez comment la technologie SOAR de pointe offerte par Splunk peut booster la productivité et l'efficacité de votre équipe de sécurité.

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

22-23997-Splunk-10 Essential Capabilities of a Best-of-Breed SOAR-WP-108