Guide d’achat des solutions SOAR

Tout ce que vous devez savoir avant d’acheter une solution d’orchestration, d’automatisation et de réponse de sécurité

splunk>
turn data into doing®

Sommaire

Il n'a jamais été aussi opportun d'investir dans une solution d'orchestration, d'automatisation et de réponse de sécurité (SOAR). Car l'époque où les équipes de sécurité devaient réagir manuellement aux incidents est révolue. Désormais, ces dernières peuvent travailler plus intelligemment, et pas plus dur, en automatisant les tâches répétitives, en augmentant la productivité et la précision des analystes ainsi qu'en protégeant mieux l'entreprise.

Trop souvent, les équipes de sécurité sont submergées de tâches sans valeur ajoutée qui accaparent les analystes, la gestion des opérations de sécurité impliquant de nombreuses tâches monotones, routinières et répétitives, en particulier pour les analystes de niveau 1. En parallèle, il manque plus d'un million de professionnels de la cybersécurité possédant les connaissances et l'expertise nécessaires pour satisfaire aux besoins RH des centres d'opérations de sécurité (SOC) du monde entier.

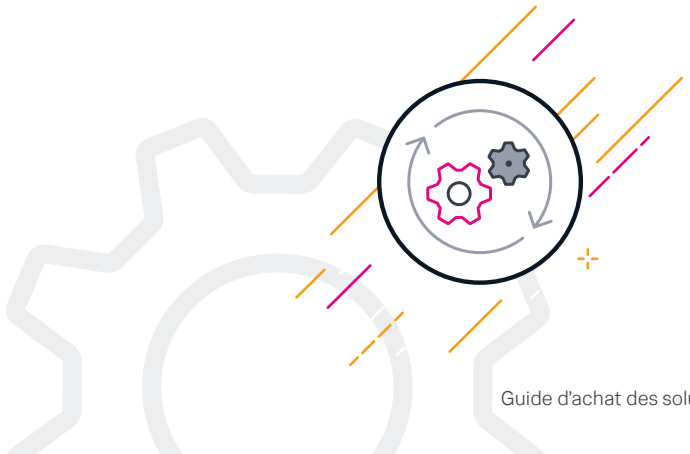
Sans compter que sur le terrain, les défis sont multiples.

- **Multiplication des alertes :** face à des centaines (voire des milliers) d'alertes de sécurité à gérer, les équipes de sécurité peuvent rapidement être débordées. Concrètement, cela se traduit par une augmentation des retards dans le traitement des incidents de sécurité et une certaine saturation des analystes face aux alertes.
- **Multiplication des produits spécialisés cloisonnés :** les équipes doivent jongler entre des outils de sécurité séparés, avec des contrôles statiques et indépendants et sans aucune interopérabilité. Inévitablement, cela génère des failles de sécurité que les attaquants peuvent (et n'hésitent pas à) exploiter.
- **Manque de compétences :** assurer la dotation en personnel d'un SOC n'est pas une mince affaire. Les analystes qualifiés se font rares et on observe un turnover extrêmement élevé dû à un marché de plus en plus concurrentiel. Résultat, les organisations qui consacrent du temps et des ressources à la formation des analystes et à l'établissement des connaissances institutionnelles sont confrontées à des pertes.
- **Processus insuffisants :** la plupart des équipes de sécurité ne parviennent pas à établir des workflows et des procédures d'exploitation normalisées (PEN) pour différents types d'événements de sécurité. Et sans cette rigueur opérationnelle, les analystes sont incapables d'agir rapidement et résolument lorsqu'ils doivent répondre à une attaque.
- **Manque de vitesse :** lorsque le temps moyen de détection (MTTD) est trop long, les attaquants ont tout le loisir de s'infiltrer et de dérober des données. En pratique, le traitement d'une alerte par un analyste peut prendre de quelques minutes (scénario idéal) à des semaines ou des mois (voire plus). Mais un délai de réponse qui se compte en mois est généralement trop long pour les menaces graves, et il en va parfois de même pour les délais de réponse qui se comptent en semaines.

Dans ces conditions, les équipes de sécurité ont de plus en plus de mal à identifier et à contrer les menaces. Les entreprises ont donc besoin d'une solution performante, flexible et rapide, qui exploite la puissance de l'automatisation.

Avec le SOAR, les analystes peuvent répondre à toute menace, quelle que soit sa taille. De fait, grâce à la codification des workflows dans des procédures automatisées, il ne faut que quelques secondes à une solution SOAR robuste pour exécuter une série d'actions à l'échelle de l'infrastructure de sécurité d'une entreprise, de la détonation de fichiers à la mise en quarantaine d'appareils. Exécutées manuellement, ces opérations prendraient des heures voire des jours.

De votre côté, vous pouvez également bénéficier des avantages du SOAR. Notre « Guide d'achat des solutions SOAR » vous aidera à cerner les critères clés pour évaluer les options qui s'offrent à vous. Ainsi, vous pourrez faire le meilleur choix pour vous et les opérations de sécurité de votre entreprise, en faisant gagner du temps à vos analystes qui pourront se consacrer à des tâches à plus haute valeur ajoutée (et profiter d'une pause déjeuner plus longue).



Qu’est-ce que le SOAR ?

Une solution SOAR élimine les tâches fastidieuses qui accaparent habituellement le temps et les ressources d’une équipe de sécurité. Grâce au SOAR, les équipes de sécurité peuvent traiter davantage d’incidents, analyser les problèmes de près, gagner du temps sur les tâches de sécurité stratégiques et améliorer la sécurité globale de l’entreprise.

Si l’automatisation est une pratique courante dans la plupart des secteurs, la cybersécurité accuse sans doute un certain retard dans ce domaine. Cela étant, nous avons observé ces dernières années un changement de taille, porté par l’intérêt croissant des experts et l’augmentation du nombre de fournisseurs sur le marché du SOAR, ces derniers repensant leurs offres de sécurité existantes pour se lancer sur ce nouveau segment.

Compte tenu du positionnement des nouveaux fournisseurs, la définition du SOAR est devenue floue, ce qui a rendu les comparaisons difficiles. Pour plus de clarté, détaillons ensemble les différents composants du SOAR :

Orchestration de la sécurité

L’orchestration de la sécurité désigne la coordination par une machine d’une série d’actions de sécurité interdépendantes à l’échelle d’une infrastructure complexe.

Automatisation de la sécurité

L’automatisation de la sécurité désigne l’exécution d’actions de sécurité par une machine.

Réponse de sécurité

La réponse de sécurité désigne la coordination (basée sur des politiques) d’activités exécutées manuellement et par des machines pour les workflows d’événements, de cas et d’incidents.

Qu’est-ce que l’orchestration de la sécurité ?

L’orchestration de la sécurité désigne la coordination par une machine d’une série d’actions de sécurité à l’échelle d’un écosystème IT complexe. Cela permet de veiller à ce que tous les composants de cet écosystème (par exemple, une large gamme d’outils de sécurité indépendants) fonctionnent de concert, tout en automatisant les tâches entre les produits et les workflows. Pour résumer, l’orchestration permet aux équipes de sécurité d’automatiser des processus complexes à l’échelle de produits spécialisés disparates, maximisant ainsi la valeur ajoutée du personnel, des processus et des outils de sécurité.

L’orchestration de la sécurité permet :

- de coordonner collectivement et automatiquement les workflows entre les outils ;
- de contextualiser les incidents de sécurité en agrégeant des données provenant de différentes sources ;
- de mener des investigations plus approfondies et plus pertinentes.

Qu’est-ce que l’automatisation de la sécurité ?

L’automatisation de la sécurité désigne l’exécution d’actions de sécurité par une machine, avec la possibilité d’analyser, de contrer et de neutraliser les menaces de façon programmatique, sans intervention humaine. Elle prend en charge une grande partie du travail des analystes, qui n’ont ainsi plus à gérer manuellement toutes les alertes au fur et à mesure qu’elles apparaissent ni à traiter manuellement chaque action ou tâche de sécurité.

L’automatisation de la sécurité permet :

- d’analyser les menaces dans votre environnement ;
- de trier les menaces potentielles en suivant les étapes, les instructions et les processus décisionnels qu’utilisent les analystes de sécurité pour analyser un événement et déterminer s’il s’agit d’un véritable incident ;
- de déterminer si un incident nécessite de prendre des mesures ;
- de contenir et de résoudre le problème ;
- d’automatiser les investigations des vulnérabilités et l’application de correctifs.

Qu’est-ce que la réponse de sécurité ?

La réponse de sécurité désigne la coordination, basée sur des politiques, d’actions automatisées et d’entrées manuelles pour les workflows d’événements, de cas et d’incidents. Les détails techniques d’un événement ou d’une alerte de sécurité doivent être organisés de sorte qu’un analyste puisse rapidement assimiler les informations disponibles, afin de mieux cerner l’ensemble du scénario de sécurité et de réagir en conséquence. En bref, un analyste de sécurité doit être en mesure d’initier de manière transparente des actions d’investigation, de confinement ou de réponse en fonction des données fournies.

Une fois que des alertes ou événements sont confirmés et remontés, un composant de gestion des cas doit prendre le relais et assurer un cycle de vie plus large et interfonctionnel, de la création à la résolution.

La réponse de sécurité permet :

- de confirmer plusieurs événements et de les faire remonter dans un seul cas ;
- de mapper de manière transparente les incidents aux processus existants d’une entreprise ;
- d’exécuter des actions d’investigation, de confinement ou de réponse en fonction de certaines données techniques ;
- de fournir un log des activités qui consigne toutes les actions exécutées pour un événement ou une alerte ;
- d’assurer un cycle de vie plus large et interfonctionnel, de la création à la résolution.

Quels sont les principaux scénarios d'utilisation du SOAR dans le domaine de la sécurité ?

Les scénarios d'utilisation suivants sont modélisés en fonction des workflows manuels existants et mettent en évidence des problèmes opérationnels courants. Ces workflows incluent généralement d'innombrables tâches manuelles nécessitant une coordination entre différents produits spécialisés.

Avant de commencer votre évaluation, vous devez identifier les scénarios d'utilisation potentiels spécifiques à votre organisation. Pour cela, vous devriez idéalement tenir compte de l'avis des parties prenantes impliquées dans vos opérations de sécurité, ainsi que de la direction. L'identification de ces scénarios d'utilisation stratégiques, même s'ils ne sont pas immédiatement mis en œuvre, est essentielle à la réussite de votre stratégie de sécurité.

Tri des alertes	Le tri des alertes valide et hiérarchise les alertes entrantes et contextualise les événements. Il inclut certains modèles et méthodologies pour éliminer les faux positifs, afin qu'ils ne soient pas traités ultérieurement.
Réponse aux incidents	La réponse aux incidents varie en fonction du type d'incident impliqué. Par exemple, la réponse à une tentative de phishing sera foncièrement différente de la réponse à une attaque par ransomware réussie.
Traque des indicateurs de compromission (IOC)	En automatisant la traque des IOC, les équipes peuvent exploiter les dernières informations issues de la threat intelligence sans épuiser leurs ressources. Elles peuvent également mettre en œuvre la notation des informations pour identifier les sources de threat intelligence à passer en revue.
Gestion des vulnérabilités	L'automatisation (et par la suite la standardisation) du cycle d'identification, de classification, de remédiation et d'atténuation des vulnérabilités est garante d'une plus grande efficacité et d'une meilleure cohérence.
Contrôle d'accès au réseau (NAC)	Le SOAR peut renforcer les stratégies de contrôle d'accès dynamique, par exemple en intégrant un système de détection qui n'était auparavant pas inclus dans la prise de décisions liées au NAC.
Gestion des utilisateurs	La gestion des utilisateurs garantit que des comptes spécifiques sont activés et désactivés rapidement et systématiquement afin d'éliminer les menaces internes ainsi que les usurpations de comptes ou d'identifiants.
Tests d'intrusion	Les activités telles que la découverte des ressources, la classification et la hiérarchisation des cibles sont automatisées, ce qui augmente la productivité de l'équipe en charge des tests d'intrusion.
Partage d'informations	Les organisations qui soutiennent des initiatives de partage d'informations peuvent s'appuyer sur des procédures exploitant l'automatisation. L'automatisation permet également d'augmenter la productivité des analystes et de fournir des informations sensibles beaucoup plus rapidement que les processus manuels.

Vous trouverez ci-dessous divers scénarios d'utilisation en lien avec le domaine de la sécurité, qui couvrent les investigations, l'enrichissement, le confinement et la remédiation : d'autres scénarios d'utilisation spécifiques au SOAR peuvent être liés à divers autres défis, les équipes de sécurité codifiant les critères de détection et d'automatisation. Pour obtenir des exemples supplémentaires, consultez notre e-book, 5 scénarios d'utilisation de l'automatisation pour Splunk SOAR.

Les bases du SOAR

Critères d'évaluation

Nos critères pour évaluer une solution SOAR sont organisés en trois catégories : **capacités clés**, **attributs de la plateforme** et **considérations métier**.

Capacités clés

Les capacités clés désignent les éléments fondamentaux (ou de base) d'une solution SOAR. Nous couvrirons chaque capacité et chaque composant, ainsi que les principales considérations à prendre en compte pour évaluer les options qui s'offrent à vous.

Orchestrateur

- **Ingestion de données**
  Les données de sécurité doivent être ingérées. Un orchestrateur permet d'ingérer et de compiler des données à partir de n'importe quelle source et dans n'importe quel format, tout en les conservant logiquement séparées. Si les données sont non structurées, l'utilisateur doit pouvoir utiliser un gestionnaire de données pour les interpréter et les rendre accessibles.
- **Prise de décision**
  Les utilisateurs doivent être en mesure d'appliquer des procédures d'automatisation à leurs sources de données. Par exemple, une procédure de phishing peut être appliquée à une source d'ingestion basée sur les e-mails, tandis qu'une procédure d'investigation de malware peut être appliquée à une source d'alerte SIEM.
- **Exécution des tâches**
  Un orchestrateur doit répartir les tâches automatisées au meilleur moment, en les transmettant au moteur d'automatisation en vue de leur exécution.
- **Supervision humaine**
  Un orchestrateur permet d'équilibrer l'automatisation avec la supervision humaine nécessaire. Habituellement, trois scénarios nécessitent l'intervention d'un analyste. 1) Lorsque l'approbation du propriétaire de la ressource est requise pour exécuter une action de sécurité sur une cible. 2) Lorsqu'un analyste doit vérifier l'équilibre entre sécurité et continuité de l'activité. 3) Lorsqu'un analyste doit renforcer la logique de prise de décision codifiée (par exemple, en cas d'erreur).
- **Gestion des données**
  Un orchestrateur doit veiller à ce que les données de sortie d'une action soient correctement analysées, normalisées et structurées afin que les actions futures puissent les utiliser. Il doit également prendre en charge la mise en cache des données pertinentes afin d'éviter de grever d'autres ressources.
- **Tolérance aux défaillances**
  Le SOAR interagit régulièrement avec de nombreux produits et services séparés. Pour autant, la disponibilité n'est pas toujours garantie. L'accès aux services externes peut être interrompu ou perturbé. Dans ce cas, un orchestrateur doit fonctionner de manière prévisible, en assurant la reprise des opérations de manière transparente, conformément à sa configuration.

Moteur d'automatisation

Le moteur d'automatisation est la clé de voûte de la plupart des solutions SOAR. Il reçoit des actions (ou des tâches) de la part de l'orchestrateur, puis y répond en conséquence. L'automatisation étant indépendante des interactions humaines, il est important de tenir compte de critères tels que l'évolutivité et l'extensibilité de la plateforme.

- **Évolutivité**
  Des scénarios d'utilisation supplémentaires sont ajoutés et automatisés au fil du temps. Pour faire face à cette augmentation de la charge de traitement, le moteur d'automatisation doit pouvoir s'adapter verticalement et horizontalement.
- **Extensibilité**
  La sécurité évoluant rapidement, de nouvelles fonctions doivent être prises en charge sans restructuration majeure. Le moteur d'automatisation doit être suffisamment flexible pour s'adapter aux capacités uniques de son environnement.

Gestion des alertes

Une fois vos données ingérées, les alertes entrantes sont mises en file d'attente et hiérarchisées. Les investigations sont ensuite effectuées à l'aide d'actions manuelles ou automatisées pour obtenir une productivité et une précision maximales.

Et pour faire remonter les bonnes informations au bon moment, l'interface doit organiser et trier les alertes dans un format facile à interpréter. Grâce à cela, les analystes peuvent éviter les recherches étendues, passer d'un contexte à l'autre et analyser rapidement les événements notables.

- **Détails des alertes**
  Les détails d'une alerte de sécurité doivent être organisés de manière à permettre à un analyste d'assimiler et de cerner rapidement un événement de sécurité. Cela inclut une vue organisée des données techniques pertinentes, notamment adresses IP, noms de domaine, hachages de fichiers, noms d'utilisateur, adresses e-mail et autres champs de données. L'utilisation d'un format standard tel que le CEF (Common Event Format) ou équivalent est très bénéfique pour l'échange de données.
- **Lancement d'actions**
  Les analystes de sécurité doivent être en mesure de lancer des actions manuelles lors de l'investigation d'une alerte, du confinement ou de la remédiation, et l'interface doit permettre aux utilisateurs d'exécuter une action en sélectionnant les données à utiliser. Les analystes doivent également pouvoir lancer une collection automatisée d'actions pour une alerte, ce que l'on appelle procédure (ou playbook).
- **Résultats des actions**
  Les résultats des actions doivent être disponibles dans un format concis (par exemple, tableau) ainsi que dans un format plus complet (par exemple, format de données standard JSON), afin d'être accessibles et faciles à visualiser.
- **Log des activités**
  Un log complet des activités consigne toutes les actions exécutées pour une alerte, qu'elles aient été lancées manuellement ou via une procédure d'automatisation. Les résultats doivent être affichés pour chaque action, avec un indicateur de réussite ou d'échec, ce qui démontre clairement que l'action a été entièrement exécutée.
- **Statut, gravité et sensibilité des alertes**
  Les alertes doivent comporter un indicateur de statut (par exemple, « nouvelle », « ouverte » ou « clôturée »), un indicateur de gravité et un indicateur de sensibilité (par exemple, Traffic Light Protocol ou TLP). Chaque indicateur doit être modifiable dans l'interface de gestion des alertes, ainsi qu'au sein d'une procédure.
- **Collaboration sur les alertes**
  L'interface doit permettre aux analystes de collaborer sur les alertes, de les commenter et de fournir des informations sur celles-ci ainsi que sur toutes leurs données pertinentes ou diverses.

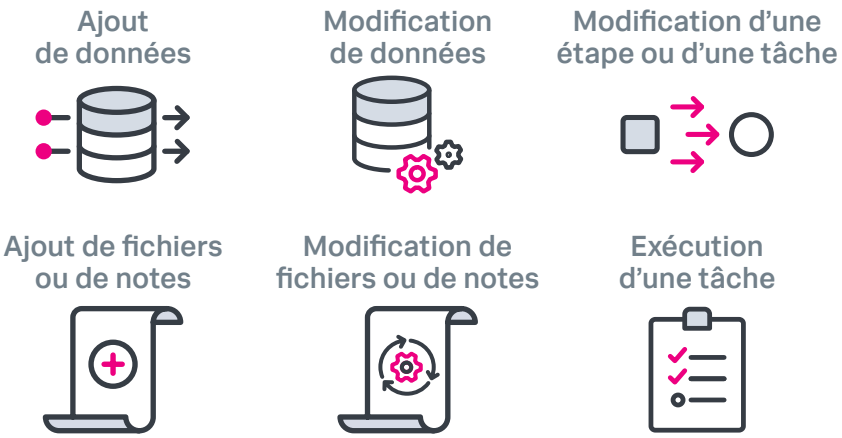
Gestion des cas

La gestion des cas adopte une vision plus large et interfonctionnelle du cycle de vie d'un incident, de la création à la résolution. Plusieurs alertes et/ou événements peuvent être confirmés, agrégés et remontés au sein d'un seul cas. Alors que la gestion des alertes est généralement technique et singulière, la gestion des cas peut également intégrer des étapes non techniques dans le processus.

En outre, le volume global des cas est généralement beaucoup plus faible que celui des alertes, avec des chiffres qui dépassent rarement la barre de la dizaine.

- **Organisation des données de cas**
  Toutes les données relatives à un cas particulier doivent être agrégées par le composant de gestion des cas. L'affichage de ces informations au sein d'un emplacement unique permet aux utilisateurs de tout assimiler sans avoir à changer de contexte.
- **Ajout de données à un cas**
  Pour chaque cas, il faut ajouter les données techniques pertinentes (par exemple, données source, résultats des actions). Les données non techniques pertinentes (notes, mémos, e-mails, captures d'écran, enregistrements ou tout autre fichier pertinent) doivent également être incluses.
- **Association des cas aux alertes**
  Idéalement, l'interface de gestion des cas doit être reliée à l'interface de gestion des alertes pour chaque alerte. Cet aspect est particulièrement pratique si et quand un analyste détermine qu'une information nécessite une investigation plus approfondie ou qu'il faut prendre une action de confinement.
- **Mappage aux processus existants**
  La plupart des organisations ont des procédures d'exploitation normalisées (PEN) pour la réponse aux incidents, les urgences, les sinistres et autres situations critiques. La gestion des cas doit permettre à l'utilisateur de définir ses processus et workflows, qui sont composés de plusieurs étapes, chaque étape comportant une ou plusieurs tâches et chaque tâche pouvant être affectée à un propriétaire, puis de les enregistrer comme modèle.
- **Audit des activités**
  Les informations nouvelles ou mises à jour, y compris les mises à jour de statut, doivent être consignées dans une piste d'audit et faciles à exporter.

Les modifications apportées à un cas peuvent inclure les éléments suivants :



Gestion des procédures

La gestion des procédures contribue à la mise en œuvre et à la maintenance de procédures d'exploitation normalisées (PEN) à l'échelle d'une organisation (et parfois au-delà). Idéalement, ce composant intègre le contrôle des révisions/versions et la gestion des syndications.

- **Organisation des procédures**
  Les analystes doivent être en mesure de personnaliser les catégories concernant différents groupes de procédures. Les regroupements doivent être basés sur ce qui fonctionne le mieux, ou ce qui est le plus facilement applicable, au sein de l'organisation (par exemple, sensibilité, segments organisationnels, types de ressources, thèmes).
- **Fonctions personnalisées**
  En plus des fonctions prêtes à l'emploi (OOTB), les utilisateurs doivent pouvoir écrire des fonctions et/ou du code personnalisés. Ces fonctions doivent pouvoir être partagées entre plusieurs procédures, tout en offrant une gestion du code et un contrôle des versions centralisés.
- **Contrôle et distribution des révisions**
  Pour gérer les procédures avec succès, l'intégration à un système de contrôle des versions (VCS) est fortement recommandée. Au niveau du déploiement, un VCS contribue à la distribution systématique des procédures. Au niveau du développement, un VCS est important pour le suivi des modifications et la restauration potentielle des mises à jour.
- **Modifications en bloc des procédures**
  Il est probable que les rouages internes de chaque procédure soient uniques. Toutefois, au niveau administratif, bon nombre de procédures ont des points communs.

Un système de gestion des procédures doit permettre un certain nombre de modifications en bloc, parmi lesquelles :

Sources d'ingestion

Activation/désactivation de l'exécution automatique et activation/désactivation du fonctionnement en mode sans échec

Activation/désactivation de la journalisation améliorée

Définition du regroupement des procédures par catégorie

Éditeur d'automatisation

Les analystes peuvent codifier les processus au sein d'une procédure via un éditeur d'automatisation. Avec les éditeurs basiques de code source, cette tâche est difficile. Cependant, un éditeur visuel d'automatisation permet à tous les experts en sécurité, quelle que soit leur expérience en programmation, d'écrire des procédures au niveau du code source et de concevoir des procédures complètes et sophistiquées.

L'éditeur visuel doit respecter les normes BPMN (Business Process Modeling Notation), une notation graphique permettant de spécifier les processus métier. Le BPMN prend en charge des symboles intuitifs pour les utilisateurs métier, tout en offrant aux utilisateurs techniques différentes manières de représenter des processus très complexes.

- **Éléments de l'interface utilisateur**
  L'interface utilisateur doit commencer par un canevas permettant de concevoir des procédures visuelles. Cette partie de l'interface doit fournir une zone permettant de spécifier une action souhaitée (par exemple block_ip ou file_reputation). Une fois qu'une action est sélectionnée, des paramètres sont requis pour la configurer (l'action peut être saisie manuellement ou sélectionnée dans une liste). L'interface doit également disposer d'un espace de test et de débogage, avec une transition fluide entre le mode édition et le mode test, ainsi qu'une vue du code source.
- **Représentation du code basée sur des blocs**
  L'utilisation de blocs pour représenter des étapes pertinentes au sein d'une plateforme d'automatisation permet aux utilisateurs d'écrire des procédures complètes et complexes sans toucher au code source sous-jacent. Pour dicter un ordre d'exécution, les blocs doivent être connectés via différentes relations : un-à-un, un-à-plusieurs ou plusieurs-à-un.
- **Intégration d'interventions humaines dans le processus décisionnel**
  L'automatisation supervisée est une exigence classique. Dans ce cas, un utilisateur peut intervenir dans une séquence d'automatisation pour approuver, réviser ou augmenter l'exécution continue d'une procédure. L'auteur d'une procédure doit avoir la possibilité de spécifier qui doit être mis dans la boucle et d'indiquer le type de notification ou le niveau d'approbation souhaité, ainsi que le type d'erreur à générer en cas d'indisponibilité d'un ou de plusieurs services.
- **Échange d'informations sur les résultats des actions**
  L'interface de l'éditeur d'automatisation doit permettre de mettre à disposition de nouvelles informations sous forme d'entrées, de paramètres, d'actions en aval, de blocs de décision, etc. Les résultats des actions précédentes doivent être accessibles visuellement et sélectionnables à partir d'un menu déroulant lors de la saisie des paramètres d'une action en amont.
- **Accès au code source des procédures**
  Lors de la conception d'une procédure dans un éditeur visuel, le code source doit être généré en temps réel et accessible à l'auteur. Certains utilisateurs peuvent préférer rédiger tout (ou partie) de la procédure via une méthode traditionnelle qui repose sur le code source et qui peut être affichée à la place d'un éditeur visuel. Dans tous les cas, le passage entre le mode visuel et le mode code source doit être fluide.
- **Conception simultanée de procédures visuelles et non visuelles**
  Lors de la gestion du code source d'une procédure, l'éditeur d'automatisation doit permettre à l'auteur de modifier la procédure au niveau du code source et au niveau du bloc visuel. Parfois, l'auteur peut exiger que des blocs individuels (tels que des actions et des blocs de décision) soient modifiés au niveau du code source pour des personnalisations au-delà du champ d'application de l'éditeur visuel. Lorsque ces modifications sont effectuées, l'utilisateur doit pouvoir encore modifier la procédure visuellement.
- **Tests et débogage intégrés et journalisation d'exécution**
  Selon la norme du secteur, les environnements de développement intégrés (IDE) fournissent des capacités d'exécution et de débogage. Avec un éditeur d'automatisation, un utilisateur doit pouvoir exécuter des procédures pour une alerte de sécurité, puis observer l'activité d'exécution et les résultats. L'objectif est de permettre à l'auteur de modifier, de tester et de déboguer rapidement des procédures au sein d'une seule interface.
- **Mode sans échec**
  Un éditeur d'automatisation doit également fournir un mode sans échec pour les nouvelles procédures nécessitant des tests de pré-production. Ce mode simule l'exécution de cibles d'automatisation sans les modifier.

Framework d'application

Le framework d'application offre une interface extensible pour les nouvelles intégrations, en connectant la plateforme à l'un des milliers de produits spécialisés actuellement disponibles sur le marché.

- **Écosystème ouvert**
  Une solution SOAR peut perdre de sa valeur au fil du temps si elle ne parvient pas à s'intégrer aux offres nouvelles ou populaires sur le marché. Pour prendre en charge ces types d'intégration, elle doit adopter un écosystème ouvert afin de promouvoir le développement d'applications. Les nouvelles technologies doivent également être rapidement intégrées sans nécessiter de modification de la solution de base.

- **Développement d'applications**
  Le développement d'applications est un composant clé d'un écosystème ouvert, car il permet aux utilisateurs d'intégrer plusieurs technologies pour prendre en charge leurs procédures. Une solution SOAR doit être en mesure de rationaliser le développement d'applications au sein du produit lui-même, de sorte que les utilisateurs puissent visualiser, tester, étendre et modifier les applications existantes, ainsi que créer des applications entièrement nouvelles, le tout à partir de l'interface utilisateur.

Indicateurs et reporting

Les indicateurs et le reporting sont nécessaires pour cerner et quantifier pratiquement tout, et les solutions SOAR n'y font pas exception. Et si l'automatisation promet une augmentation des performances et de la productivité, les indicateurs permettent d'évaluer ce qu'il en est réellement et d'identifier les améliorations possibles.

- **Tableaux de bord flexibles**
  Les indicateurs de réussite varient ; ils sont généralement spécifiques à une organisation ou à une partie prenante et peuvent dépendre de nombreux facteurs. C'est pourquoi les utilisateurs doivent pouvoir organiser leurs indicateurs de performance clés (KPI) de la façon la plus pertinente pour leur organisation. Une solution SOAR doit donc permettre de personnaliser et d'organiser ces données en conséquence.

- **Reporting sur les performances**
  Une organisation qui prend le virage de l'automatisation souhaite le plus souvent gagner en efficacité. D'où la nécessité de cerner les gains quantitatifs de performances et les économies de ressources pour justifier cet investissement.

  Voici quelques exemples d'indicateurs devant faire l'objet d'un reporting :
  - le temps moyen de résolution (MTTR) ;
  - la durée moyenne de réaction (MDT), qui correspond à la période entre une compromission et l'application d'une réponse appropriée ;
  - gains de temps dont bénéficient les analystes grâce à l'automatisation ;
  - le nombre d'équivalents temps plein (ETP) gagnés grâce à l'automatisation ;
  - les gains de temps moyens résultant de l'exécution d'une procédure ;
  - les économies réalisées (coût ETP x ETP gagnés).

- **Reporting sur l'efficacité de la sécurité**
  L'automatisation doit également améliorer l'efficacité de la sécurité ainsi que la posture de sécurité globale de l'organisation. Dans cette optique, déterminer le nombre total d'alertes de sécurité gérées et la vitesse à laquelle elles sont gérées est aussi important pour justifier un investissement.

  Voici quelques exemples d'indicateurs devant faire l'objet d'un reporting :
  - MTTR et MDT ;
  - nombre total d'alertes ouvertes ;
  - alertes ouvertes par jour/heure/semaine/mois ;
  - alertes clôturées par jour/heure/semaine/mois ;
  - performances par rapport aux accords de niveau de service (SLA).

- **Intégration des applications et performances des procédures**
  Identifier les procédures les plus fréquemment utilisées permet de déterminer dans quels domaines réaliser de nouveaux investissements. Idéalement, la conception des procédures devrait permettre de clôturer automatiquement les faux positifs ou les vrais positifs fiables.

  Pour repérer les lacunes relatives à l'automatisation et évaluer l'efficacité des intégrations d'outils, les indicateurs suivants doivent faire l'objet d'un reporting :
  - alertes clôturées via l'automatisation (par heure, jour, semaine, mois ou autre période) ;
  - intégrations d'applications les plus actives ;
  - actions les plus actives (manuelles et automatisées) ;
  - procédures les plus actives ;
  - durée d'exécution des procédures ;
  - durée d'exécution des actions.

- **Charge de travail des analystes**
  Si l'automatisation vise à combler les lacunes liées aux ressources humaines, une solution SOAR exige tout de même l'intervention d'un analyste pour de nombreuses opérations quotidiennes. C'est notamment le cas pour le tri manuel et les situations où d'autres actions sont nécessaires en cas d'alerte ou quand des approbations humaines sont ajoutées dans la procédure afin de mettre en place une « automatisation supervisée ».

  Voici quelques exemples d'indicateurs à fournir pour évaluer la charge de travail des analystes impliqués dans le processus d'automatisation :
  - alertes attribuées à une personne ;
  - alertes clôturées par une personne ;
  - délai moyen d'approbation ;
  - nombre d'approbations en suspens ;
  - approbations requises (par heure, jour, semaine, mois ou autre période).

Attributs de la plateforme

Les attributs de la plateforme peuvent être de nature plus qualitative. En conséquence, les critères suivants sont évalués plus souvent par le biais d'observations et d'interactions avec la plateforme.

Options de déploiement

Une solution SOAR doit prendre en charge les déploiements sur site, cloud ou hybrides. Si certaines organisations préfèrent les solutions sur site, d'autres ne jurent que par le cloud. Le type de livraison ou de déploiement que vous choisirez dépendra en grande partie des besoins de votre entreprise et de ses exigences en matière de budget, de stockage et de sécurité, ainsi que de la meilleure façon de rationaliser les opérations de sécurité et de faciliter la transformation numérique à l'échelle de votre infrastructure existante.

Communauté

Idéalement, une solution SOAR doit prendre en charge un modèle communautaire en adoptant un écosystème ouvert pour le développement d'applications. Cela contribue à promouvoir la réussite à long terme en évitant la dépendance vis-à-vis d'un seul fournisseur. Autre point positif, les technologies peuvent facilement évoluer sans affecter négativement les procédures automatisées. Sans compter que la nature évolutive de la sécurité oblige les professionnels à travailler ensemble pour partager des procédures, des meilleures pratiques et des stratégies afin de faire face aux dernières menaces.

Une grande communauté active

La plupart des utilisateurs préfèrent s'appuyer sur les expériences d'autres utilisateurs partageant la même vision. Ainsi, une grande communauté active d'utilisateurs permet de partager des procédures et des applications, ou de réfléchir à de nouvelles idées pour de nouveaux scénarios d'utilisation dans le domaine de l'automatisation. Afin de favoriser de tels échanges d'idées, il est essentiel de mettre en relation les utilisateurs au sein de la communauté. Les outils de communication et de messagerie se révèlent particulièrement efficaces pour offrir une assistance technique et à la conception, pour répondre aux questions et pour trouver des solutions concernant les scénarios d'utilisation de l'automatisation.

Collaboration

La collaboration optimise l'exhaustivité des fonctionnalités, l'intégration des applications et les procédures automatisées qui répondent à un éventail de scénarios en constante évolution.

- **Collaboration au sein de la communauté**
  Le contenu des utilisateurs et des fournisseurs doit être accessible à partir d'un référentiel centralisé. Cela inclut les contributions techniques, telles que les procédures et les intégrations d'applications, ainsi que les contributions non techniques telles que les présentations, les notes techniques, les articles de blog et autres méthodes de documentation.
- **Collaboration à l'échelle de la plateforme**
  Une solution SOAR doit aider les utilisateurs à collaborer au sein de différents cercles de confiance. Pour cela, il faut qu'elle prenne en charge le partage d'informations sensibles entre des groupes privilégiés au sein de l'équipe de sécurité de l'entreprise.

Approche cognitive

Une solution SOAR cognitive met en application les connaissances des analystes ainsi que les observations précédentes afin d'orienter les décisions futures. Cet aspect est codifié dans un système sous la forme de procédures. Cette méthodologie est basée sur les statistiques d'exécution, les caractéristiques des données ingérées et les résultats des actions.

Ces informations peuvent être exploitées pour recommander des actions individuelles, des procédures ou un ensemble d'actions séquentielles constituant une procédure. Il est important de cerner les capacités cognitives actuelles d'une solution SOAR, ainsi que la stratégie cognitive et la feuille de route pour les itérations futures.

Automatisation fiable

En matière d'automatisation, les équipes adoptent généralement les scénarios d'utilisation un par un, ce qui leur permet de se fier progressivement au système. Afin de faciliter ce processus, une solution SOAR doit prendre en charge un ensemble de fonctionnalités permettant certaines interactions humaines avec les procédures automatisées. Concrètement, il faut pouvoir ajouter des analystes au sein d'un workflow par ressource (technologie ou outil de sécurité spécialisé) ou par action.

Au niveau des ressources, l'administrateur d'une ressource doit être averti à chaque fois qu'une action est exécutée sur cette ressource. Au niveau des actions, une invite doit être ajoutée dans une procédure automatisée afin de donner à l'utilisateur la possibilité de continuer, de suspendre ou d'abandonner la demande. Ce niveau de supervision permet aux utilisateurs de se fier aux étapes programmées au fur et à mesure.

Sécurité

Sans surprise, la sécurité est l'un des aspects les plus importants d'une solution d'automatisation et d'orchestration de la sécurité, cette dernière contenant des identifiants d'authentification et d'autres informations hautement sensibles. Une solution SOAR chiffre ces informations sensibles et prend en charge un puissant contrôle d'accès basé sur des rôles.

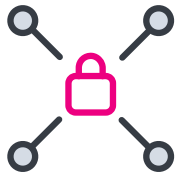
Voici quelques-unes des meilleures pratiques de sécurité relatives aux solutions SOAR :

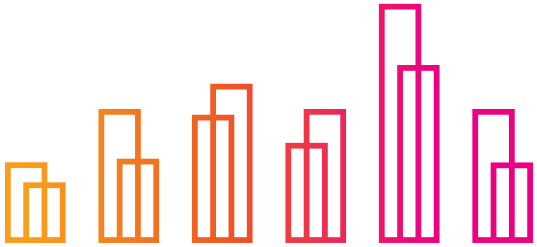
Chiffrement des identifiants de sécurité

Stockage des identifiants en dehors de la mémoire

Prise en charge des systèmes de gestion de l'authentification

Prise en charge de l'authentification multifacteurs





Évolutivité

Une solution SOAR doit pouvoir évoluer verticalement et horizontalement. Plus une organisation ajoute de scénarios d'utilisation au fil du temps, plus la charge de traitement de la plateforme augmente. La solution doit donc être conçue de manière à permettre une mise à l'échelle verticale en augmentant les ressources matérielles (par exemple, processeur et RAM) et une mise à l'échelle horizontale en augmentant le nombre d'instances de serveur qui soutiennent le déploiement.

Ouverture et extensibilité

La sécurité est en constante évolution, comme en témoigne la multitude de produits spécialisés disponibles actuellement. Dans ce contexte, une solution SOAR doit être conçue dans un souci d'ouverture et d'extensibilité. Elle doit facilement prendre en charge de nouveaux scénarios de sécurité, de nouveaux produits, de nouvelles actions et de nouvelles procédures.

Framework d'intégration ouvert

Grâce à un framework d'intégration ouvert, les technologies peuvent « entrer » dans la plateforme et en « sortir » sans affecter négativement les opérations automatisées. Les utilisateurs doivent également avoir la possibilité de développer des intégrations supplémentaires sans dépendre de leur fournisseur SOAR.

C'est notamment le cas pour les applications développées en interne, les API fournisseur personnalisées ou en version bêta ou l'extension des fonctionnalités de la plateforme d'automatisation. Ce framework ouvert doit suivre une norme et un modèle de programmation communs et être accompagné de nombreux documents et exemples.

Pas de restrictions d'interface

Certaines technologies exposent les interfaces à l'aide de différents protocoles ou méthodes (API REST, SSH, syslog, API personnalisées, etc.) Il est donc impératif qu'un framework d'intégration extensible n'impose pas de restrictions sur les types d'interface. Si la plateforme d'automatisation offre une connectivité avec une application ou un produit spécialisé, la méthode d'interface ne doit pas impacter l'intégration d'applications, ce qui permet d'utiliser n'importe quelle méthode d'interface.

Mobilité

Une solution SOAR est conçue pour accélérer les temps de réponse, c'est-à-dire pour limiter la durée d'implantation et réduire le temps moyen de résolution. Mais pour obtenir une réponse rapide, il faut que les analystes de sécurité soient joignables lorsqu'un cas ou une urgence de sécurité nécessite une intervention humaine. Or, ces derniers ne sont pas toujours assis derrière leur bureau avec leur ordinateur portable ouvert, prêts à répondre rapidement à des notifications.

C'est pourquoi il est important qu'une solution SOAR permette d'accéder à la plateforme, d'interagir avec elle et de la contrôler à partir des appareils mobiles des analystes. Les analystes peuvent ainsi exécuter les procédures en déplacement, examiner les artefacts de sécurité et trier les événements sans ordinateur portable, répondre aux invites depuis leur appareil mobile et être toujours joignables, qu'ils soient à leur bureau ou non.

Facilité d'utilisation

Bien que les logiciels d'entreprise soient très rarement simples, il est possible de limiter les frictions liées au déploiement et à l'utilisation d'une solution SOAR.

- **Installation et configuration**
  Le format des appliances virtuelles facilite le déploiement, car la plupart des organisations exploitent déjà la virtualisation avec d'autres infrastructures.
- **Intégration**
  Une solution SOAR peut grandement réduire la courbe d'apprentissage initiale en utilisant un processus d'intégration pour aider les utilisateurs à configurer les paramètres système, à se connecter à une source de données et à activer leurs premières procédures.
- **Accélération de l'adoption de l'automatisation**
  Une solution SOAR doit aider les utilisateurs à se lancer rapidement dans l'automatisation en fournissant un ensemble robuste et prêt à l'emploi de procédures automatisées. Et pour mettre en place l'automatisation sans tarder, il est également utile de permettre aux utilisateurs d'élaborer, de tester et de déployer rapidement des procédures automatisées.

Considérations métier

Indépendamment des performances de la technologie de base d'une entreprise, des considérations autres que les caractéristiques du produit peuvent fortement influencer la prise de décision d'un acheteur. C'est notamment le cas de l'offre marketing ainsi que des services qui viennent compléter la technologie de base pour donner vie au produit final.

Attributs de l'entreprise

Dans le cadre d'une décision d'achat, il est important de tenir compte du profil, de la qualité et du potentiel futur de l'entreprise que vous choisissez. Car en réalité, bon nombre de nouveaux fournisseurs proposant de nouvelles solutions sont voués à l'échec. Ainsi, vous devez miser sur une entreprise suffisamment performante pour tenir ses promesses.

Histoire de l'entreprise

Le fournisseur que vous choisissez doit avoir une grande expérience dans le développement de solutions de sécurité. Car si les systèmes d'orchestration, d'automatisation et de réponse de sécurité constituent un segment de marché relativement nouveau, leur origine remonte à de nombreuses années. Il est donc important de comprendre comment l'entreprise a été créée et pourquoi elle a décidé de se lancer dans le SOAR.

Capacité d'exécution

Vous avez tout intérêt à faire appel à une entreprise qui s'appuie sur une équipe de professionnels expérimentés, car la capacité d'exécution d'une organisation est souvent directement liée à l'expérience des membres de son équipe.

Base de clients

Une entreprise est le reflet de la qualité et du profil de sa clientèle. De fait, les grandes entreprises complexes effectuent une évaluation rigoureuse de leurs fournisseurs potentiels dans plusieurs domaines avant de procéder à un achat.

Récompenses et distinctions

Penchez-vous sur les récompenses et autres distinctions que l'entreprise a reçues, car elles prouvent que les performances du fournisseur sont à la hauteur. Mais soyez prudents, car la qualité des distinctions varie également.

Services auxiliaires

Les services auxiliaires qu'une entreprise offre pour sa technologie peuvent grandement influencer le déploiement au sein d'une organisation et le succès d'un projet.

Services professionnels

Les niveaux de maturité des opérations de sécurité peuvent varier considérablement d'une entreprise à l'autre. Il est donc important de déterminer si la société fournit des services professionnels qui augmentent les chances de réussite du déploiement. Il est également crucial de pouvoir compter sur des experts pour faciliter la création de processus (s'il en manque) et la conversion de procédures manuelles en procédures automatisées.

Service après-vente

Beaucoup de startups excellent sur le plan de la technologie et de l'avant-vente, mais se révèlent décevantes en matière de service après-vente. Étudiez les options d'assistance et déterminez si la société fournit le type d'assistance dont vous aurez besoin.

L’offre de Splunk

Grâce à Splunk, votre équipe peut reprendre les commandes.

Spunk SOAR permet à votre équipe de travailler plus intelligemment, de réagir plus rapidement et de renforcer les défenses de sécurité de votre entreprise. Pour vous, c’est la promesse de pouvoir automatiser les tâches répétitives, trier les incidents de sécurité plus rapidement grâce à l’automatisation de la détection, des investigations et de la réponse, maximiser la productivité, l’efficacité et la précision et renforcer vos défenses en connectant et en coordonnant des workflows complexes à l’échelle de votre équipe et de vos outils.

Splunk SOAR prend également en charge une large gamme de fonctions de sécurité, notamment la gestion des événements et des cas, la threat intelligence intégrée, les outils de collaboration et le reporting, ainsi que l’intégration de votre infrastructure de sécurité existante afin que chaque partie participe activement à la stratégie de défense, tout en travaillant de concert.

Toujours plus d’intégrations

Pour accéder à d’autres d’intégrations, Splunkbase propose des milliers d’applications de sécurité tierces à connecter et à intégrer à Splunk SOAR. Grâce à ces intégrations, Splunk SOAR peut ordonner à vos outils de sécurité d’effectuer un large éventail d’actions, par exemple, demander à VirusTotal de vérifier la réputation de fichiers ou à Cisco Firewall de bloquer une adresse IP. Le modèle d’application de Splunk SOAR prend en charge l’intégration avec plus de 350 outils et plus de 2 100 actions différentes, toutes disponibles sur Splunkbase. Ces applications, utilitaires et extensions prêts à l’emploi peuvent aider votre équipe pour la supervision de la sécurité, les pare-feu nouvelle génération, la gestion des menaces avancées et bien plus encore.

Lancez-vous.

Pour en savoir plus sur Splunk SOAR, téléchargez l'édition communautaire gratuite ou contactez le service commercial pour en savoir plus.

22-23828-Splunk-SOAR Buyers Guide-EB-101_FR

splunk> turn data into doing