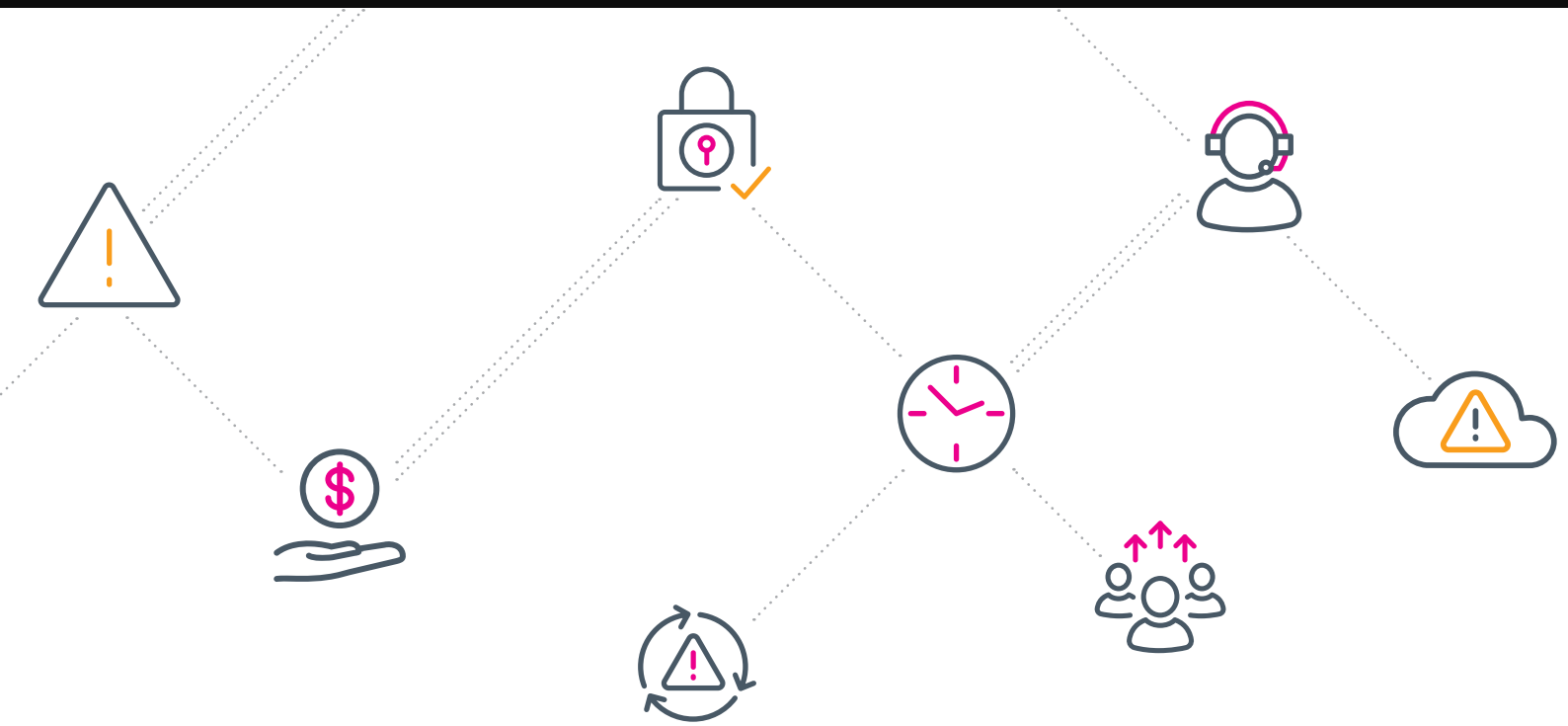
Guide d'achat des solutions SOAR

Acheter une solution d'orchestration, d'automatisation et de réponse de sécurité : qui, quoi, où, quand, pourquoi.

splunk> turn data into doing™

Sommaire



1. Introduction

Investir dans une plateforme d'orchestration, d'automatisation et de réponse de sécurité (SOAR) est une décision sage et hautement stratégique. En effet, il est légitime de penser que le choix de la plateforme sur laquelle va reposer votre centre des opérations de sécurité (SOC) est plus crucial que celui de n'importe quel produit de sécurité spécifique. La plateforme SOAR que vous allez choisir va devenir un élément central de votre infrastructure de sécurité et jouera concrètement le rôle de système d'exploitation pour vos investissements de sécurité.

Ce guide vise à établir les critères essentiels à prendre en compte au cours de l'évaluation des plateformes SOAR.

Orchestration, automatisation et réponse de sécurité : une définition

Si l'automatisation est populaire depuis des années dans d'autres segments logiciels, notamment pour les ventes, le marketing, les RH et les opérations IT, les équipes de sécurité commencent seulement à voir les avantages de l'automatisation et de l'orchestration. Cette prise de conscience suscite un vif intérêt pour l'acquisition de plateformes SOAR. Par conséquent, de nombreux fournisseurs de solutions de sécurité se tournent vers la catégorie SOAR pour capter cette attention nouvelle, en exploitant leurs offres originaires de segments adjacents. Cette tendance produit un effet indésirable : à mesure que l'engouement pour le segment SOAR s'intensifie, un nombre croissant de fournisseurs aux perspectives diverses brouillent les définitions de ce marché et compliquent la comparaison des offres.

Pour apporter de la clarté, nous proposons les définitions suivantes :

Orchestration de sécurité
L'orchestration de sécurité est la coordination, par des machines, d'une série d'actions de sécurité interdépendantes sur une infrastructure complexe.

Automatisation de la sécurité
L'automatisation de la sécurité est l'exécution, par des machines, d'actions de sécurité.

Réponse de sécurité
La réponse de sécurité est la coordination, articulée par une politique, d'activités conduites par des humains et des machines dans le cadre de la prise en charge d'événements, de scénarios et d'incidents.

Nous allons utiliser ces définitions tout au long de ce guide pour examiner les capacités, les attributs et les considérations qui s'imbriquent pour former une plateforme SOAR de pointe.

Identification des scénarios de sécurité

Les équipes identifient généralement des scénarios de sécurité à mettre en œuvre avec la plateforme SOAR. Les scénarios d'utilisation sont modélisés d'après les workflows manuels existants et correspondent généralement aux difficultés opérationnelles prioritaires. Les workflows contiennent habituellement de nombreuses tâches manuelles et nécessitent d'utiliser plusieurs produits.

Outre ces difficultés connues, il est important d'étudier tous les scénarios d'utilisation potentiels avant de commencer votre évaluation. Cet effort doit impliquer des parties prenantes clés de votre équipe des opérations de sécurité. Il est essentiel d'identifier des scénarios d'utilisation complets, même s'ils ne sont pas mis en œuvre dans l'immédiat, pour avoir l'assurance que la plateforme choisie aujourd'hui répondra à vos besoins de demain.

Nous présentons ci-dessous une sélection de scénarios de sécurité dans différentes catégories : investigation, enrichissement, isolation et remédiation.

Tri des alertes
L'objectif du tri des alertes est de valider et hiérarchiser les alertes entrantes. Les scénarios d'utilisation dédiés au tri des alertes entrantes impliquent d'enrichir les événements par du contexte supplémentaire. Ils peuvent aussi inclure une logique permettant d'éliminer les faux-positifs ayant un haut niveau de confiance.

Réponse aux incidents
Les scénarios de réponse aux incidents varient considérablement selon le type d'incident. Par exemple, la réponse à une tentative d'hameçonnage est très différente de la prise en charge d'une attaque par ransomware réussie.

Recherche des indicateurs de compromission (IOC)
En automatisant la recherche des IOC, les équipes peuvent exploiter toute la richesse de la Threat Intelligence qu'elles reçoivent, sans être limitées par le manque de disponibilité des ressources. Elles peuvent également mettre en place un système de score qui facilitera le choix des sources d'informations à utiliser.

Gestion des vulnérabilités
L'automatisation du cycle d'identification, de classification, de remédiation et de prise en charge des vulnérabilités n'apporte pas seulement un gain d'efficacité, mais offre aussi des résultats plus cohérents en assurant l'exécution identique et systématique du processus.

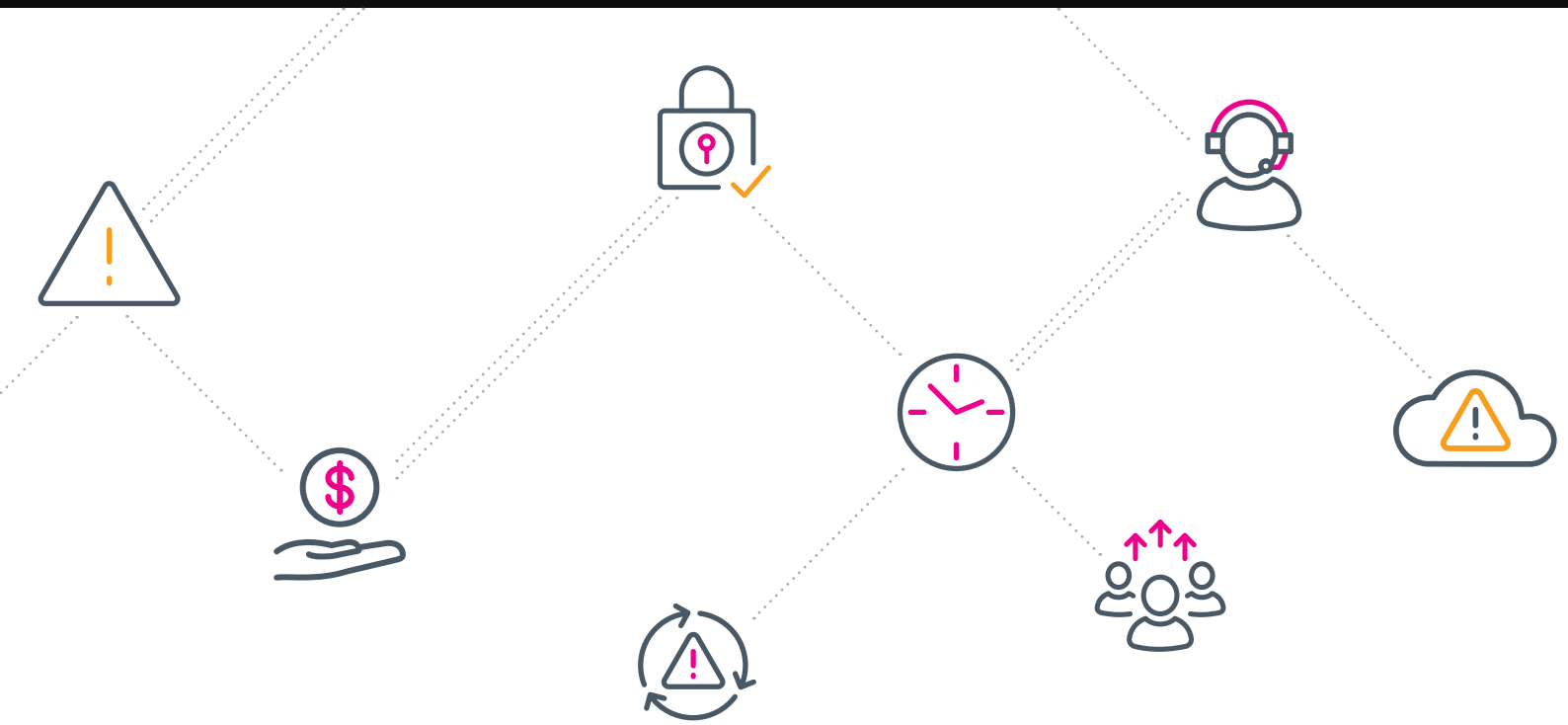
Contrôle des accès au réseau (NAC)
Les plateformes SOAR peuvent renforcer les stratégies de contrôle dynamique des accès. Il est notamment possible d'intégrer un système de détection qui ne faisait jusque-là pas partie de la logique décisionnelle du NAC.

Gestion des utilisateurs
Veiller à ce que les utilisateurs soient activés et désactivés de façon fiable, rapide et systématique peut éliminer les risques d'exploitation malveillante d'un compte d'utilisateur par un agresseur potentiel.

Tests de pénétration
On peut automatiser des activités telles que la découverte des actifs, leur classification et la hiérarchisation des cibles pour accroître la productivité des équipes en charge des tests de pénétration.

Partage des informations
Les organisations qui mettent en place des initiatives de partage des informations ont tout intérêt à utiliser des procédures assistées par l'automatisation. L'automatisation peut aussi rendre les analystes plus productifs et fournir à une communauté des informations urgentes plus rapidement qu'un processus manuel.

Autres cas d'usage
Les autres cas d'usage candidats à l'automatisation sont issus de scénarios bien connus dans lesquels les équipes des opérations de sécurité peuvent codifier les critères à appliquer pour prendre automatiquement des décisions et des mesures appropriées.



2. Critères d’évaluation

Nous suggérons de répartir les critères d’évaluation des solutions SOAR dans au moins trois catégories : fonctionnalités fondamentales, attributs de la plateforme et facteurs commerciaux. Les fonctionnalités fondamentales sont généralement de nature fonctionnelle et s’identifient facilement dans une plateforme. Les attributs de la plateforme sont plus subtils, comme les caractéristiques d’architecture, et ils influenceront la sélection de la plateforme. Les facteurs commerciaux complètent l’offre et incluent les services à valeur ajoutée proposés par un fournisseur pour enrichir sa technologie de base, comme la formation et l’assistance.

Fonctionnalités fondamentales

Les fonctionnalités fondamentales doivent être envisagées comme les composants de base d'une plateforme SOAR. Nous allons donc passer en revue chaque fonctionnalité ou composant, en suggérant des pistes pour leur évaluation et leur sélection.

Orchestrateur

L'orchestrateur doit diriger et superviser toutes les activités liées à un scénario de sécurité donné, du début à la fin. Dans toutes les situations, il est crucial que l'orchestrateur produise des résultats d'une fiabilité prévisible et qu'il assure une utilisation optimale de toutes les ressources disponibles.

Assimilation des données

L'automatisation et l'orchestration de la sécurité commence par l'assimilation des données. Un orchestrateur doit être capable d'assimiler des données de sécurité provenant de n'importe quelle source, quel que soit le format. Il doit être capable de recevoir des données poussées vers la plateforme autant que de sonder des sources de données et d'importer des données dans la plateforme. Si les données injectées ne sont pas structurées, l'orchestrateur doit permettre à l'utilisateur de fournir un gestionnaire de données pour les interpréter et les rendre exploitables par la plateforme SOAR. L'orchestrateur doit également pouvoir assimiler des données de sources multiples et avoir la possibilité de maintenir les données séparées de façon logique.

Prise de décision

Les utilisateurs doivent pouvoir sélectionner les procédures d'automatisation qui sont appliquées à une source de données. Par exemple, une procédure en cas d'hameçonnage par e-mail peut être appliquée à une source de messagerie électronique, tandis qu'une source d'alertes SIEM sera traitée à l'aide d'une procédure d'investigation. L'étape de prise de décision est étroitement liée aux fonctions de gestion des alertes, décrites plus loin.

Exécution des tâches

Il incombe généralement à l'orchestrateur de distribuer les tâches d'automatisation de sa file au moment opportun et optimal ; les tâches sont alors transmises au moteur d'automatisation pour être exécutées.

Supervision humaine

Un orchestrateur doit efficacement équilibrer automatisation machine et supervision humaine obligatoire. L'intervention d'un analyste est requise dans trois scénarios courants : quand il faut l'autorisation du propriétaire d'un actif pour exécuter une action de sécurité sur une cible, quand il faut veiller à ce que sécurité et continuité des activités soient correctement équilibrées, et quand il faut enrichir une logique décisionnelle codifiée (en cas d'erreur, par exemple).

Gestion des données

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. L'orchestrateur doit aussi pouvoir mettre en cache des données pertinentes en cas de besoin, pour éviter de mobiliser d'autres ressources.

Tolérance aux interruptions de service

Une plateforme SOAR interagit régulièrement avec de nombreux produits et services différents pour exécuter les procédures d'automatisation. Un orchestrateur doit prévoir que la disponibilité de ces produits et services n'est pas toujours garantie. L'accès aux services externes peut être interrompu ou coupé. Dans ces situations, l'orchestrateur doit se comporter de façon prévisible, se rétablir et reprendre ses opérations de façon digne, en suivant sa configuration.

Moteur d'automatisation

Le moteur d'automatisation est au cœur de la plupart des plateformes SOAR : il reçoit les actions (ou tâches) de l'orchestrateur et les exécute de façon fiable. Comme les tâches d'automatisation s'exécutent de façon indépendante et sans interaction humaine dans la plupart des cas, des qualités telles que l'évolutivité et l'extensibilité de la plateforme sont des facteurs de poids.

Évolutivité

Il est impératif de comprendre comment le moteur d'automatisation va évoluer à la fois verticalement et horizontalement. Il faut prévoir qu'un utilisateur va automatiser de nouveaux scénarios d'utilisation au fil du temps. Chaque nouveau cas d'usage vient augmenter la charge de calcul du moteur

d'automatisation. 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 augmenter les performances et protéger le retour sur investissement de l'automatisation.

Ouvert et évolutif
Le paysage de la sécurité évolue rapidement et le moteur d'automatisation doit pouvoir prendre en charge de nouvelles fonctionnalités sans refonte majeure. Le moteur d'automatisation doit pouvoir s'adapter aux capacités spécifiques de son environnement.

Gestion des alertes

Juste après l'assimilation des données abordée plus haut, la plateforme SOAR doit intégrer une fonction de gestion des alertes qui va les mettre en file d'attente et les hiérarchiser pour aider les analystes à les trier plus efficacement. L'investigation des alertes peut être accomplie au moyen d'actions manuelles ou automatisées pour atteindre le plus haut niveau possible de productivité et de précision. L'interface d'une fonction de gestion des alertes doit être conçue de façon à ce que tous les aspects d'une alerte de sécurité puissent être rapidement assimilés en vue d'une action efficace. L'interface doit également mettre en évidence les bonnes informations au bon moment afin d'éviter aux analystes d'avoir à effectuer de longues recherches ou à naviguer entre différents contextes.

Détails des alertes
Les attributs techniques d'une alerte de sécurité doivent être organisés de façon à permettre à l'analyste de les assimiler rapidement afin de comprendre le scénario de sécurité. Cela consiste notamment à proposer une vue organisée de données telles que : adresses IP, noms de domaine, hachage de fichiers, noms d'utilisateurs, adresses e-mail et autres champs de données utiles. L'utilisation d'un format standard comme Common Event Format (CEF) ou équivalent offre également des avantages considérables pour l'échange des données.

Émission d'actions
Lorsqu'il étudie une alerte, l'analyste de sécurité doit pouvoir initier manuellement des actions en utilisant les données de l'alerte en question. Il peut s'agir d'actions d'investigation, d'isolation et de correction, ou d'actions génériques. L'interface doit permettre à l'utilisateur d'accomplir une action en sélectionnant les données à exploiter. Ce comportement est parfois désigné sous le nom d'exécution contextuelle d'actions et il permet de faire pivoter l'analyse autour d'informations récemment découvertes.

Outre l'exécution manuelle d'actions, l'analyste doit aussi pouvoir initier un ensemble de mesures face à une alerte. Cet ensemble d'actions est généralement appelé procédure.

Résultats de l'action
Lorsque des mesures manuelles ou automatisées sont prises face à une alerte, les résultats ne doivent pas seulement être visibles et intelligibles pour l'analyste : ils doivent aussi être interprétables par la plateforme SOAR qui peut éventuellement les exploiter pour prendre une décision automatisée. Les résultats des actions doivent être disponibles sous une forme résumée (en tableau, par exemple) et sous une forme plus complète (JSON).

Journal d'activité
La plateforme doit 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 et si l'action a bien été menée à terme.

État, gravité et sensibilité des alertes
Chaque alerte gérée par la plateforme doit inclure des indicateurs d'état (nouveau, ouvert, fermé), de gravité et de sensibilité (on pense notamment aux désignations du protocole Traffic Light ou TLP). Chaque indicateur doit être modifiable au sein de l'interface de gestion des alertes et à partir d'une procédure.

Collaboration autour des alertes
L'interface doit prévoir un espace de collaboration pour les analystes afin de leur permettre de laisser des commentaires et d'échanger des informations diverses sur une alerte. Idéalement, ces échanges collaboratifs doivent être capturés et présentés avec les autres données d'alerte.

Gestion des investigations

Une fois les alertes ou les événements confirmés et escaladés, un composant de gestion des investigations doit ouvrir un cycle élargi et interfonctionnel allant de la création à la résolution. Ce composant doit inclure

des attributs supplémentaires propres au concept d'investigation afin de distinguer celle-ci de l'alerte. Plusieurs alertes peuvent avoir été confirmées, agrégées et escaladées au sein d'une même investigation. La gestion des alertes est généralement technique, tandis que la gestion des investigations intègre couramment des étapes techniques et non techniques. Enfin, le volume d'investigations est souvent plus faible que celui des alertes : de nombreuses organisations reçoivent des centaines ou des milliers d'alertes par jour, tandis que les investigations se comptent plutôt en unités.

Organisation des données d'investigation
Toutes les données relatives à une investigation doivent être agrégées par le composant de gestion des investigations. L'affichage des informations en un seul et même endroit permet aux utilisateurs de les assimiler efficacement sans avoir à changer de contexte.

Ajout de données à une investigation
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. L'ajout automatisé d'informations à une investigation doit aussi être réalisables à partir d'une procédure.

Lien entre investigations et alertes
Au cours d'une investigation, il arrive couramment que l'on identifie des données méritant une investigation ou un scénario imposant d'initier sans attendre une mesure d'isolement. Par conséquent, si un analyste conclut qu'il faut prendre une mesure, l'interface de gestion des investigations doit orienter l'analyste vers l'interface de gestion de l'alerte en question de façon parfaitement fluide. À partir de l'interface de gestion des alertes, d'autres actions peuvent être accomplies, et les modifications apportées aux données concernées doivent être répercutées dans l'interface de gestion des investigations.

Correspondance avec les processus existants
De nombreuses organisations ont mis au point des procédures opérationnelles standards (SOP) pour la réponse aux incidents, les urgences, les catastrophes et autres situations critiques. 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. Des informations de contexte supplémentaires peuvent être incorporées à la description de la tâche. Comme dans les applications de gestion de tâches, une tâche terminée par son propriétaire doit être signalée comme fermée. L'interface doit fournir une indication de la progression et de l'état de l'investigation.

Audit des activités
L'ajout ou la modification d'informations ainsi que les changements d'état sont des détails importants pour une investigation. Chaque modification de l'investigation doit être consignée dans une trace d'audit exportable.

On pense notamment aux changements suivants :

- ajout de données ;
- modification de données ;
- modification d'une étape ou d'une tâche ;
- ajout de fichiers ou de notes ;
- modification de fichiers ou de notes ;
- finalisation d'une tâche ;
- autre activité ou modification de l'investigation.

Gestion des procédures

La gestion des procédures facilite la maintenance des SOP. Idéalement, ce composant doit assurer le contrôle des versions et permettre de gérer la syndication des SOP sous la forme de procédures à l'échelle d'une organisation et, potentiellement, d'une communauté.

Organisation des procédures
La gestion des procédures doit permettre l'organisation et le groupement adéquats des procédures. Les utilisateurs doivent pouvoir définir leurs propres groupements selon ce qui fonctionne le mieux dans leur organisation. On peut, par exemple, choisir d'organiser et de grouper les procédures par thème, sensibilité, segment organisationnel ou type d'actif.

Modification groupée des procédures
Les rouages de chaque procédure seront certainement uniques. Les procédures présentent

toutefois, au niveau administratif, un certain nombre d'aspects communs.

Un système de gestion des procédures doit permettre l'édition groupée de certains attributs :

- sources de données à assimiler ;
- activation/désactivation de l'exécution automatique pour activer/désactiver un fonctionnement en mode de sûreté ;
- activation/désactivation de la journalisation avancée ;
- groupement catégorique des procédures.

Contrôle des versions et distribution
Nous recommandons vivement d'intégrer un système de contrôle de version (VCS) tel que Git pour faciliter la gestion des procédures à grande échelle. Au niveau du déploiement, l'exploitation d'un VCS permet la distribution systématique des procédures sur plusieurs systèmes. Cela est particulièrement utile pour synchroniser les procédures entre un système de développement et un système de production, ou entre plusieurs systèmes de production répartis sur des sites différents. Sur le plan du développement, le VCS est indispensable pour suivre les révisions et pouvoir au besoin annuler des modifications. Un avantage collatéral de cette approche est que les développeurs peuvent éditer les procédures dans l'outil de leur choix puis synchroniser facilement les versions modifiées avec la plateforme.

Éditeur d'automatisation

L'éditeur d'automatisation est l'outil qui permet à un analyste ou à un responsable de codifier des processus sous la forme de procédures d'automatisation. Le prédécesseur de l'éditeur visuel d'automatisation est l'éditeur de code source. Utiliser exclusivement un éditeur de code source rendait l'élaboration des procédures fastidieuse, difficile et accessible uniquement à un groupe restreint de programmeurs. L'éditeur visuel d'automatisation permet à tous les experts en sécurité qui ne maîtrisent pas nécessairement la rédaction du code source des procédures, à mettre sur pied des procédures complètes et sophistiquées. L'éditeur visuel doit respecter les normes BPMN de modélisation et de notation des processus métier, un ensemble de conventions graphiques pour la spécification des processus. Le système BPMN comprend des symboles intuitifs pour les utilisateurs professionnels tout en donnant aux utilisateurs techniques la possibilité de représenter des processus extrêmement complexes.

Éléments de l'interface utilisateur
L'interface utilisateur doit proposer un espace de dessin sur lequel on peut assembler des procédures visuellement. Cette partie de l'interface doit présenter un espace permettant de spécifier une action (telle que block_ip ou file_reputation). Une fois l'action sélectionnée, elle devra vraisemblablement être configurée à l'aide de paramètres. L'interface doit permettre de saisir manuellement ces paramètres ou de les sélectionner dans une liste. Les données d'alerte et/ou de résultat d'action doivent également être utilisables comme paramètres.

L'interface doit comprendre un espace de test et de débogage de sorte que la transition entre mode d'édition et mode de test soit transparente. Enfin, une vue du code source de la procédure automatisée doit être accessible si l'utilisateur souhaite le consulter.

Représentation du code en blocs
L'utilisation de blocs pour représenter des étapes articulées dans la plateforme d'automatisation permet aux utilisateurs de rédiger des procédures exhaustives et complexes sans toucher au code source sous-jacent. Les blocs doivent pouvoir être reliés de plusieurs façons (un vers un, un vers plusieurs, plusieurs vers un) de manière à dicter un ordre d'exécution. Visuellement, l'utilisateur doit pouvoir élaborer une procédure incluant l'exécution d'actions, des appels API, des déclarations conditionnelles (si-alors) et des embranchements reliant une procédure à une autre.

Intervention des humains dans le processus de décision
La prise en charge de l'automatisation supervisée est une exigence courante. Elle permet de faire intervenir un être humain dans la séquence d'automatisation pour qu'il approuve, vérifie ou enrichisse l'exécution de la procédure. L'éditeur d'automatisation doit prendre en charge cette étape de supervision humaine en proposant d'insérer des points d'approbation adjacents à une ou plusieurs actions de sécurité dans une procédure. L'auteur de la procédure doit pouvoir préciser quelles personnes sont insérées

dans la boucle d'automatisation, ainsi que le type de notification ou l'approbation voulue. L'éditeur de procédure et la plateforme sous-jacente prévoiront également la création d'une logique de gestion des erreurs provoquant l'intervention d'un être humain dans la boucle, par exemple lorsqu'un service de réputation n'est pas disponible pour appuyer la prise de décision.

Échange des informations sur les résultats des actions
L'interface de l'éditeur d'automatisation doit mettre à disposition les nouvelles informations résultant des actions précédentes sous la forme d'entrées ou de paramètres utilisables dans les actions et les blocs de décision en aval. Les résultats des actions précédentes doivent être accessibles visuellement et sélectionnables à l'aide d'un menu déroulant au moment de renseigner les paramètres des actions suivantes.

Accès au code source de la procédure
Au fil de l'élaboration de la procédure dans l'éditeur visuel, le code source résultant doit être généré en temps réel et accessible à l'auteur. Certains utilisateurs préfèrent rédiger tout ou partie de la procédure de façon traditionnelle, en code source. L'interface doit pouvoir remplacer momentanément l'éditeur visuel par un éditeur de source. Le basculement entre les deux modes d'édition doit être fluide et simple.

Construction visuelle et non visuelle de la procédure en parallèle
Lorsque l'on travaille sur le code source d'une procédure, l'éditeur d'automatisation doit permettre d'éditer la procédure au niveau du code sans perdre la possibilité de la modifier en mode visuel. Il arrive que l'auteur souhaite apporter des modifications au code source de certains blocs (actions, décisions) pour intégrer des personnalisations hors du champ de l'éditeur visuel. Une fois ces modifications faites, l'utilisateur doit conserver la possibilité d'éditer visuellement la procédure.

Intégration des tests et du débogage, et journalisation de l'exécution
La norme veut que les environnements de développement intégrés (IDE) proposent des fonctions d'exécution et de débogage. Dans le cas d'une plateforme d'automatisation, l'utilisateur doit pouvoir lancer la procédure sur une alerte de sécurité et observer son activité et ses résultats. Le log et les codes d'erreur doivent être affichés dans une fenêtre de débogage visible en même temps que l'éditeur visuel ou l'éditeur de code source si l'auteur le souhaite. L'objectif est de donner à l'auteur la possibilité de modifier, tester et déboguer rapidement des procédures dans une seule et même interface.

Mode de sûreté
L'éditeur d'automatisation doit aussi proposer un mode de sûreté pour les nouvelles procédures à tester en pré-production. Ce mode simule l'exécution de cibles d'automatisation sans réaliser aucune modification. Une fois que l'auteur ou un autre utilisateur de la plateforme est suffisamment confiant dans la logique de la procédure, ce mode de sûreté peut être désactivé et la procédure peut commencer à fonctionner normalement.

Framework d'application

Le framework d'application fournit une interface extensible pour de nouvelles intégrations qui vont connecter la plateforme à des outils ponctuels parmi les milliers que compte le marché actuel de la sécurité.

Écosystème ouvert
Une plateforme SOAR peut perdre de sa valeur au fil du temps sans intégration aux nouvelles offres du marché. Pour garantir la possibilité d'intégrer de nouvelles applications, la plateforme doit adopter un écosystème ouvert permettant à quiconque de développer des intégrations. Les utilisateurs conservent ainsi leur autonomie et leur indépendance vis-à-vis des fournisseurs. Les technologies peuvent aller et venir sans que cela n'affecte les procédures automatisées. Les nouvelles technologies doivent être rapidement intégrées dans la plateforme sans qu'il ne faille modifier le cœur de celle-ci. Enfin, les utilisateurs doivent pouvoir se munir de plateformes supplémentaires sans dépendre des développements du fournisseur de SOAR.

Métriques et rapports

Les métriques et les rapports sont essentiels pour toutes les plateformes d'automatisation et les plateformes SOAR ne font pas exception. L'automatisation est une promesse de gain de productivité et de qualité. Les métriques sont indispensables pour comprendre l'efficacité de la

plateforme d'automatisation et identifier où apporter des améliorations pour accroître le retour sur investissement.

Tableaux de bord flexibles
Les métriques sont propres aux organisations et aux personnes. Pour cette raison, les utilisateurs doivent pouvoir organiser leurs métriques de façon pertinente pour leur organisation. La plateforme SOAR doit donner la possibilité de personnaliser finement la présentation des métriques. Il faut ainsi pouvoir configurer l'ordre dans lequel les informations apparaissent sur le tableau de bord, préciser quelles métriques sont affichées et sur quelles fenêtres temporelles.

Suivi des performances
Le déploiement de l'automatisation a pour but d'augmenter l'efficacité des opérations. Il est donc essentiel de connaître le gain quantitatif de performance et les économies de ressources obtenus par l'automatisation, et de pouvoir consulter ces informations sur un tableau de bord.

Quelques exemples de métriques de performance clés qui doivent être disponibles sur la plateforme :

- temps moyen de résolution (MTTR) ;
- temps moyen de séjour (MDT), quel est le délai entre une compromission (par un acteur menaçant) et la mise en place d'une réponse appropriée ;
- nombre d'heures de travail d'analystes économisées grâce à l'exécution automatisée ;
- nombre d'équivalents temps-plein (FTE) économisés grâce à l'exécution automatisée ;
- temps moyen économisé par exécution de procédures ;
- coûts économisés (coût du FTE x FTE économisés).

Rapports d'efficacité de la sécurité
Le déploiement de l'automatisation sert également à améliorer l'efficacité et la position de sécurité de l'entreprise. Une vision claire du nombre total d'alertes de sécurité prises en charge et du rythme auquel elles sont gérées est impérative pour comprendre les avantages de l'automatisation en termes d'efficacité.

Quelques exemples de métriques d'efficacité de la sécurité, indispensables sur la plateforme :

- MTTR et MDT (présentés plus haut) ;
- nombre total d'alertes ouvertes ;
- alertes ouvertes par jour (ou par heure, semaine ou mois) ;
- alertes fermées par jour (ou par heure, semaine ou mois) ;
- performance vis-à-vis des accords de niveau de service (SLA).

Intégration d'applications et performance des procédures
Savoir quelles sont les procédures les plus souvent invoquées peut apporter un éclairage sur les domaines de l'automatisation qui mériteraient des investissements supplémentaires. Idéalement, la conception de la procédure doit viser la fermeture automatique des faux positifs et des vrais positifs à haut niveau de confiance. Dans les cas où l'automatisation n'assure pas intégralement le tri des alertes, il peut être nécessaire de réviser les procédures.

Pour identifier les lacunes de l'automatisation ainsi que l'efficacité de l'intégration des outils, les métriques ci-dessous doivent être fournies par la plateforme d'automatisation :

- alertes fermées par l'automatisation (par heure, jour, semaine, mois ou autre intervalle) ;
- intégrations d'applications les plus actives ;
- actions les plus actives (manuelles et automatisées) ;
- procédures automatisées les plus actives ;
- temps d'exécution des procédures ;
- temps d'exécution des actions ;
- charge de travail humaine.

Si l'automatisation a pour but de combler le manque de ressources humaines, il reste des cas où l'activité quotidienne d'une plateforme SOAR nécessite une implication humaine. Il s'agit notamment d'opérations de tri manuel et autres actions propres à une alerte, ainsi que des cas où une demande d'approbation humaine a été insérée dans une procédure dans une optique d'« automatisation supervisée ».

Comprendre la charge de travail humaine peut aussi permettre d'identifier les domaines nécessitant un approfondissement ou un ajustement de l'automatisation. La plateforme d'automatisation doit fournir les exemples de métriques en vue d'évaluer la charge de travail humaine impliquée dans le processus d'automatisation :

- alertes affectées à une personne ;
- alertes fermées par une personne ;
- temps moyen d'approbation ;
- nombre d'approbations en attente ;
- approbations requises (par heure, jour, semaine, mois ou autre intervalle).

Attributs de la plateforme

Comme mentionné plus haut, les attributs de la plateforme vont être de nature plus qualitative. Par conséquent, ces critères sont plus souvent évalués en observant la plateforme et en interagissant avec elle.

Options de déploiement

Une plateforme SOAR doit prendre en charge les déploiements locaux, dans le cloud ou hybrides. Si certains professionnels de la sécurité préfèrent les déploiements locaux, d'autres préfèrent les déploiements dans le cloud. Déployez SOAR de manière à répondre au mieux aux besoins de votre entreprise, à rationaliser les opérations de sécurité et à faciliter votre transformation numérique.

L'appui d'une communauté

Une plateforme SOAR doit impérativement entretenir des liens avec la communauté des opérations de sécurité pour être performante à long terme. Les produits, services et plateformes sont bien trop nombreux pour qu'une entreprise développe à elle seule toutes les intégrations que cela demande. Le paysage de la sécurité évolue constamment et il faut donc qu'une communauté de professionnels travaille ensemble et partagent des procédures, des bonnes pratiques et des stratégies pour faire face aux dernières menaces. Une plateforme SOAR doit donc appuyer un modèle communautaire robuste et faciliter le partage des intégrations d'applications et des procédures.

Une communauté vaste et active

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.

Pour faciliter l'échange des idées, il est impératif de connecter les utilisateurs au sein de la communauté. Pour ce faire, on fournit généralement un outil de communication comme Slack qui permet aussi bien les discussions en groupe que les messages directs. Les outils de messagerie sont efficaces pour obtenir une aide technique, des pistes de conception, des réponses à des questions et échanger des idées de cas d'usage de l'automatisation. D'autres outils de communication permettent également de diffuser de nouvelles idées, comme les pages Github où les utilisateurs publient leur travail, ou un dépôt communautaire central hébergeant des présentations, des procédures et des intégrations d'application.

Collaboration

La collaboration améliore considérablement la substance d'une plateforme en multipliant les fonctionnalités, en élargissant la couverture des intégrations et en proposant des procédures automatisées pour une gamme croissante de scénarios.

Collaboration au sein de la communauté

Du point de vue du contenu, les contributions des utilisateurs et du fournisseur doivent être accessibles dans un dépôt centralisé et à disposition de tous les utilisateurs de la communauté. Il s'agit autant des contributions techniques telles que les procédures et les intégrations d'application, que les contributions non techniques comme les présentations, les revues techniques, les blogs et autres formes de documentation. Le dépôt d'informations doit être en croissance constante et proportionnelle à la taille de la communauté.

Collaboration au sein de la plateforme

Le puzzle de la collaboration n'est pas complet si la plateforme ne rassemble pas les différentes pièces. Il incombe à la plateforme SOAR de permettre aux utilisateurs d'exploiter les avantages

de la collaboration au sein de différents cercles de confiance. La plateforme doit prendre en charge les formes les plus sensibles de collaboration : les communications au sein de l'équipe de sécurité de l'organisation. Elles vont se faire à l'aide d'une fonction de conversation intégrée et d'ajout de notes et de données aux alertes et investigations.

Compétences cognitives

Une plateforme SOAR doit exploiter les connaissances des humains et des observations précédentes pour orienter les futures décisions. Les connaissances humaines doivent être codifiées dans le système sous forme de procédures pour permettre l'automatisation. La plateforme peut aussi tirer parti des observations antérieures en suivant les statistiques d'exécution, les caractéristiques des données ingérées et les résultats des actions. Ces informations peuvent être utilisées pour recommander des actions, des procédures ou un ensemble d'actions dans une séquence pouvant devenir une procédure. Il est donc important de connaître les compétences cognitives actuelles de la plateforme SOAR ainsi que la stratégie et la feuille de route des prochaines versions de la plateforme dans ce domaine.

Automatisation progressive

L'intégration de l'automatisation dans les opérations de sécurité augmente généralement au fil du temps. Bien souvent, les équipes adoptent l'automatisation en implémentant un scénario d'utilisation à la fois, afin d'établir une relation de confiance avec la plateforme. Pour favoriser cette confiance dans l'automatisation, la plateforme SOAR doit proposer un ensemble de fonctionnalités permettant une interaction humaine sélective avec les procédures automatisées.

Les interventions humaines dans un workflow doivent se baser sur les actifs (outil de sécurité ou technologie spécifique) ou les actions. La première méthode (par actif) doit permettre d'informer l'administrateur d'un actif à chaque fois qu'une action est exécutée sur l'actif en question. La seconde (par action) doit se faire en insérant des demandes d'intervention humaine à n'importe quel point d'une procédure automatisée. Cette demande donnera à son destinataire la possibilité de poursuivre, suspendre ou abandonner l'exécution. Avec ce type de supervision, les utilisateurs apprennent à faire confiance aux étapes d'automatisation programmées.

Sécurité

L'un des aspects les plus importants d'une plateforme d'automatisation et d'orchestration de la sécurité est sa propre sécurité. Dans la mesure où une plateforme SOAR détient des identifiants d'authentification et autres informations hautement sensibles, elle doit être renforcée, chiffrer les informations sensibles et fournir un système robuste de contrôle des accès basé sur le rôle.

Les bonnes pratiques de sécurité essentielles à rechercher dans une plateforme SOAR sont les suivantes :

- chiffrement des identifiants de sécurité ;
- pas de stockage des identifiants dans la mémoire ;
- prise en charge des systèmes de gestion de l'authentification ;
- prise en charge de l'authentification multi-facteurs.

Évolutivité

Il est impératif de comprendre comment la plateforme SOAR va évoluer à la fois verticalement et horizontalement. Les nouveaux scénarios d'utilisation ajoutés au fil du temps vont accroître la charge de calcul qui pèse sur la plateforme. Celle-ci doit donc 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).

Une plateforme ouverte et extensible

La sécurité évolue constamment comme en témoigne la multitude de produits spécifiques disponibles aujourd'hui. Une plateforme SOAR doit être conçue dans une optique d'ouverture et d'extensibilité. Elle doit aisément accueillir de nouveaux scénarios de sécurité, produits, actions et procédures.

Framework d'intégration ouvert

L'effet immédiat d'un framework d'intégration ouvert est que les technologies peuvent entrer et sortir de la plateforme sans nuire aux opérations automatisées.

Les utilisateurs doivent avoir la possibilité de prendre en charge des intégrations supplémentaires sans dépendre du fournisseur de la plateforme SOAR. Et cela implique de leur donner les moyens de développer leurs propres intégrations s'ils

le souhaitent. Cela s'applique notamment aux applications développées en interne, aux API personnalisées ou fournies en accès précoce par un fournisseur, ou aux projets d'extension des fonctionnalités de la plateforme d'automatisation. Ce framework ouvert doit respecter un standard et un modèle de programmation commun. Il s'accompagnera d'une documentation abondante et de nombreux exemples.

Aucune restriction d'interface

Certaines technologies présentent des interfaces à l'aide d'API REST, SSH, syslog, API personnalisées ou autre protocole ou méthode. Un cadre d'intégration extensible ne doit imposer aucune restriction sur les types d'interface. En cas de connectivité entre la plateforme d'automatisation et le produit ou l'application spécifique, la méthode de l'interface ne doit pas affecter l'intégration de l'application et toute méthode doit pouvoir être utilisée.

Mobilité

Les plateformes d'orchestration, d'automatisation et de réponse de sécurité sont conçues pour accélérer les temps de réponse, en d'autres termes, pour réduire les temps d'attente (MDT) et le temps moyen de résolution (MTTR). Pour obtenir une réponse rapide, les analystes de la sécurité doivent être joignables lorsqu'un cas ou un problème de sécurité nécessite une intervention humaine. Mais les analystes ne sont pas toujours assis à leur bureau avec leur ordinateur portable ouvert, prêts à répondre à des messages à tout moment. C'est pourquoi il est important qu'une plateforme SOAR offre l'accès, l'interactivité et le contrôle de la plateforme à partir de l'appareil mobile de l'analyste. De cette façon, les analystes peuvent lancer des playbooks lorsqu'ils sont en déplacement, examiner les artefacts de sécurité et les événements de triage sans ouvrir un ordinateur portable, répondre aux requêtes de leur mobile et être toujours joignables, qu'ils soient assis à leur bureau ou non.

Simplicité d'utilisation

Bien que les logiciels d'entreprise ne soient jamais simples, il est possible de réduire les frictions au déploiement et à l'utilisation d'une plateforme SOAR.

Installation et configuration

Le format compact d'une appliance virtuelle facilite le déploiement car la plupart des entreprises utilisent déjà la virtualisation avec d'autres infrastructures.

Initiation

Une plateforme SOAR peut aplanir considérablement la courbe d'apprentissage initiale en proposant un processus d'initiation qui va aider l'utilisateur à configurer les paramètres système, à connecter une source de données et à activer ses premières procédures.

Réduire le délai d'automatisation

Une plateforme SOAR doit permettre aux utilisateurs de commencer rapidement à créer des automatisations. Pour cela, elle doit fournir un ensemble conséquent de procédures automatisées prêtes à l'emploi. Elle accélérera également ce processus en donnant les moyens de rédiger, tester et déployer rapidement des procédures automatisées.

Un IDE graphique aidera les non-programmeurs à élaborer et modifier des procédures. Dans cette optique, une plateforme SOAR doit proposer un outil permettant de créer ou modifier visuellement des procédures d'automatisation. L'élaboration graphique des procédures réduit le temps de développement et améliore la qualité en évitant les erreurs de code et en appliquant un standard qui favorisera la cohérence des procédures.

Facteurs commerciaux

Quelles que soient les performances de la technologie proposée par une entreprise, d'autres facteurs, extérieurs à ce qu'on associe traditionnellement au produit, viennent influencer le processus de décision d'achat. Les caractéristiques de l'entreprise qui propose le produit sont le premier facteur de poids. Tout aussi important, l'ensemble de services proposés, qui viennent compléter la technologie de base pour former le produit global dont l'acquéreur fera, à terme, l'expérience.

Qualités de l'entreprise

Lorsque l'on prend une décision d'achat, le profil, la qualité et le potentiel de l'entreprise sont des facteurs de poids. En effet, un grand nombre de jeunes entreprises proposant de nouvelles solutions sur des marchés émergents ne survivront pas. Vous devez choisir une entreprise qui possède la robustesse nécessaire pour tenir ses engagements.

Histoire de l'entreprise

L'entreprise que vous choisirez doit avoir une riche expérience dans le développement de solutions

de sécurité. Si le segment de l'orchestration, l'automatisation et la réponse de sécurité est relativement nouveau sur le marché, ses origines remontent à plusieurs décennies. Il est essentiel de comprendre comment l'entreprise a été formée et pourquoi elle a décidé de s'engager dans le segment SOAR.

Capacité d'exécution

Recherchez une entreprise dotée de l'expertise d'une équipe de professionnels chevronnés. La capacité d'une entreprise à tenir ses engagements à l'avenir dépend très largement du parcours professionnel de ses membres.

Base de clients

La qualité et le profil de la base de clients d'une entreprise est un excellent miroir. Les clients de premier plan soumettent un fournisseur potentiel à de nombreuses vérifications avant de prendre une décision d'achat.

Prix et récompenses

Passez en revue les prix et récompenses obtenus par l'entreprise. Ces distinctions sont le signe que l'industrie confirme la fiabilité du fournisseur et de ses produits. Soyez attentifs au fait que la qualité des prix est aussi variable que celle des sociétés.

Services annexes

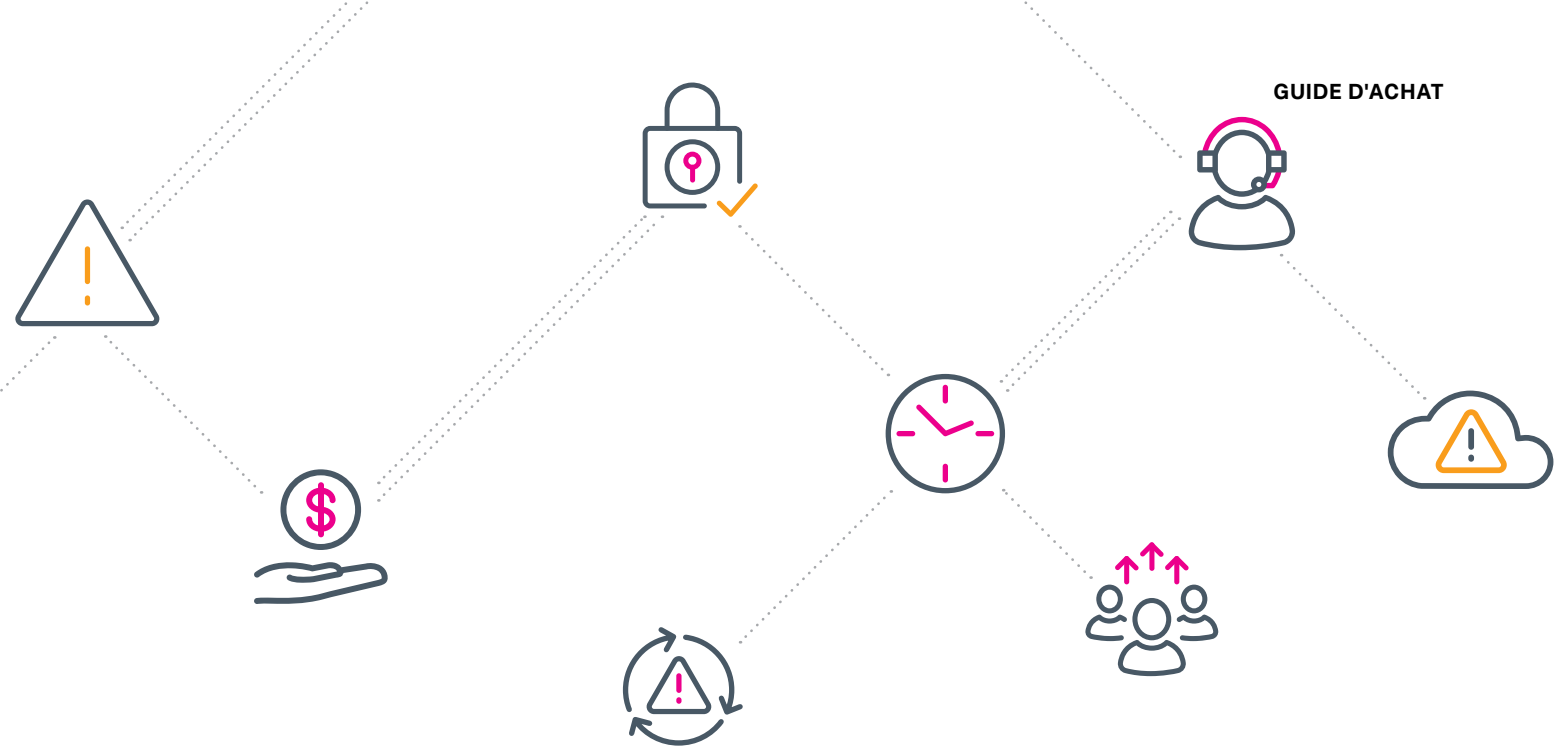
Les services auxiliaires proposés par une entreprise autour de sa technologie peuvent influencer considérablement l'expérience de déploiement d'une entreprise et, en fin de compte, le succès du projet.

Services professionnels

Le niveau de maturité des opérations de sécurité varie considérablement d'une organisation à l'autre. Il faut donc déterminer si l'entreprise fournit des services professionnels qui vont améliorer les chances de réussite du déploiement. Il est également important que des experts soient disponibles pour assister à l'élaboration de processus (s'ils n'existent pas encore) et à la conversion des workflows en procédures d'automatisation.

Service après-vente

De nombreuses start-ups offrent d'excellentes technologies et un support pré-vente de qualité, mais échouent à l'étape du service après-vente. Examinez la gamme des options d'assistance pour savoir si l'entreprise qui vous intéresse propose le soutien dont vous aurez besoin.



3. Conclusion

Ce guide présente de nombreux critères à prendre en compte au cours de l'évaluation des plateformes SOAR. Des composants de base aux facteurs commerciaux en passant par les attributs de la plateforme, il est important d'établir vos critères d'évaluation dans le détail avant de commencer le processus d'évaluation et de choisir une plateforme.

Pour en savoir plus sur Splunk SOAR, la plateforme d'automatisation et d'orchestration de la sécurité, **téléchargez gratuitement** Splunk SOAR Community Edition ou **adressez-vous à notre service commercial** pour plus d'informations.

2020-Splunk-SEC-SOAR-Buyers-Guide-A4-105-French-WP

Liste d'évaluation

Utilisez cette liste pratique pour évaluer les différentes plateformes d'automatisation, d'orchestration et de réponse de sécurité.

Nom de la plateforme : _____

Capacités fondamentales

- ☐ **Orchestrateur**
  - ☐ Assimilation des données
  - ☐ Prise de décision
  - ☐ Exécution des tâches
  - ☐ Supervision humaine
  - ☐ Gestion des données
  - ☐ Tolérance aux interruptions
- ☐ **Moteur d'automatisation**
  - ☐ Évolutivité
  - ☐ Extensibilité
- ☐ **Gestion des alertes**
  - ☐ Détails des alertes
  - ☐ Initiation d'actions
  - ☐ Résultats des actions
  - ☐ Journal d'activité
  - ☐ État, gravité et sensibilité des alertes
  - ☐ Collaboration autour des alertes
- ☐ **Gestion des investigations**
  - ☐ Organisation des données d'investigation
  - ☐ Ajout de données à une investigation
  - ☐ Lien entre investigations et alertes
  - ☐ Correspondance avec les processus existants
  - ☐ Audit des activités
- ☐ **Gestion des procédures**
  - ☐ Organisation des procédures
  - ☐ Modification groupée des procédures
  - ☐ Contrôle des versions et distribution
- ☐ **Éditeur d'automatisation**
  - ☐ Éléments de l'interface utilisateur
  - ☐ Représentation du code en blocs
  - ☐ Intervention des humains dans le processus de décision
  - ☐ Échange des informations sur les résultats des actions
  - ☐ Accès au code source de la procédure
  - ☐ Construction visuelle et non visuelle de la procédure en parallèle
  - ☐ Intégration des tests et du débogage, et journalisation de l'exécution
  - ☐ Mode sécurisé
- ☐ **Framework d'applications**
  - ☐ Écosystème ouvert
- ☐ **Métriques et rapports**
  - ☐ Tableaux de bord flexibles
  - ☐ Rapports de performance
  - ☐ Rapports d'efficacité de la sécurité
  - ☐ Intégration d'applications et performance des procédures Playbook Performance
  - ☐ Charge de travail humaine
- ☐ **Options de déploiement**
  - ☐ Local
  - ☐ Cloud
  - ☐ Hybride

Attributs de la plateforme

- ☐ **Appui de la communauté**
  - ☐ Communauté vaste et active
- ☐ **Collaboration**
  - ☐ Collaboration au sein de la communauté
  - ☐ Collaboration au sein de la plateforme
- ☐ **Capacités cognitives**
  - ☐ Automatisation progressive
- ☐ **Sécurité**
  - ☐ Évolutivité
  - ☐ Ouverture et extensibilité
  - ☐ Framework d'intégration ouvert
  - ☐ Aucune restriction d'interface
  - ☐ Simplicité d'utilisation
  - ☐ Installation et configuration
  - ☐ Initiation
  - ☐ Réduction du délai d'automatisation

Facteurs commerciaux

- ☐ Qualités de l'entreprise
- ☐ Historique de l'entreprise
- ☐ Capacité d'exécution
- ☐ Base de clients
- ☐ Prix et récompenses
- ☐ Services auxiliaires
- ☐ Services professionnels
- ☐ Service après-vente