Votre organisation est-elle suffisamment mature pour SOAR ?

19 février 2021 - ID G00 719029 - 16Lecture min. publiée

Par Pete Shoard

Les outils d'orchestration, d'automatisation et de réponse de la sécurité permettent aux organisations qui ont un niveau de préparation approprié dans leurs processus d'opérations de sécurité d'augmenter l'efficacité et la cohérence. Les responsables de la sécurité et de la gestion des risques doivent se préparer de manière adéquate pour garantir la valeur de ces outils.

Aperçu

Principales conclusions

- Les équipes de sécurité qui ne disposent pas de processus d'opérations de sécurité bien développés et de compétences de développement interne gaspillent de précieux budgets de sécurité en essayant de déployer et d'intégrer un outil SOAR.
- Malgré des capacités prêtes à l'emploi, les playbooks, les scénarios et les intégrations SOAR ne peuvent pas être utilisés efficacement sans personnalisation.
- La compatibilité avec les investissements existants est essentielle pour qu'une organisation tire pleinement parti de la suite de fonctionnalités qu'un outil SOAR peut fournir.
- Contrairement à une ligne de production robotisée, SOAR ne remplace pas les rôles principaux. Au contraire, il augmente les processus établis pour les rendre plus efficaces.

Recommandations

Les responsables de la sécurité et de la gestion des risques qui envisagent d'acheter des solutions SOAR pour leurs opérations de sécurité doivent :

- Ciblez les processus internes inefficaces mais efficaces au sein des opérations de sécurité actuelles pour évaluer si l'automatisation de ces processus fournira un avantage défini d'un outil SOAR.
- Impliquez des équipes extérieures à la sécurité, telles que les opérations d'infrastructure et de réseau, dans la décision d'acquérir et de mettre en œuvre un outil SOAR, en examinant tous les processus potentiellement éligibles et la compatibilité avec les investissements technologiques existants afin d'identifier les bons candidats pour l'automatisation.
- Engagez des équipes de développement internes ou identifiez les compétences de programmation requises au sein de l'organisation pour garantir que le produit SOAR peut être pleinement exploité.

introduction

Appelés SOAR, les outils destinés à accroître l'efficience et l'efficacité des opérations de sécurité sont sur le marché depuis plusieurs années. Au cours de cette période, nous avons assisté à une évolution rapide des capacités et des offres des fournisseurs (voir Guide du marché des solutions d'orchestration, d'automatisation et de réponse de sécurité). Le principal argument de vente de ces outils est leur capacité à réagir automatiquement à un incident ou à un problème sans aucune forme d'analyse humaine . En réalité, cependant , la mise en œuvre réussie de telles fonctions est loin d'être simple.

La plupart des commentaires des acheteurs indiquent que le succès réside généralement dans l'augmentation des processus existants, rarement dans la gestion des processus de bout en bout. La portée et la simplicité d'une telle fonctionnalité sont souvent largement exagérées dans le marketing produit ; pour la plupart des cas d'utilisation, une réponse de sécurité automatisée entièrement et non interactive est un mythe . Des implémentations approfondies sont possibles mais peuvent être très difficiles, avec des dépendances critiques à l'intégration. Cette recherche aide les responsables de la sécurité et de la gestion des risques à identifier la pertinence et la préparation efficace de leur service pour la mise en œuvre des technologies SOAR de manière judicieuse et réaliste.

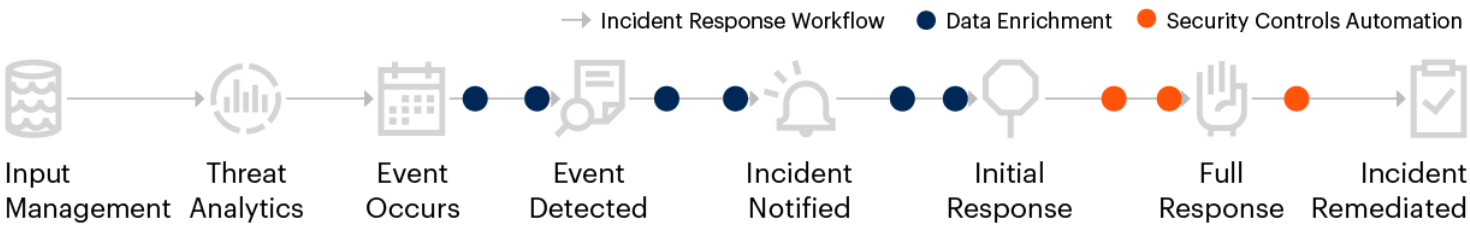
Les outils SOAR sont souvent considérés à tort comme une solution miracle qui, une fois implémentée, connectera des fonctions d'alerte à des ensembles d' outils tels que des pare-feu, un système de détection et de prévention des intrusions (IDPS) et la détection et la réponse des points de terminaison (EDR). Au lieu de cela, les responsables de la sécurité et de la gestion des risques doivent considérer la fonction des technologies SOAR comme permettant deux fonctions : la collecte d'entrées à partir des fonctions d'opérations de sécurité, telles que les alertes, et l'automatisation partielle des processus, tels que l' analyse et le tri des incidents . Les capacités SOAR doivent principalement être conçues pour aider à définir, hiérarchiser et piloter des activités de réponse aux incidents normalisées selon un flux de travail prédéfini.

SOAR est régulièrement utilisé pour automatiser des tâches dans un processus de réponse aux incidents typique (voir Figure 1) :

- Le traitement automatisé des informations de sécurité pour prendre en charge un flux de travail de réponse aux incidents (le traitement automatisé des données de sécurité peut inclure des alertes d'informations de sécurité et de gestion des événements [SIEM] et/ou des renseignements sur les menaces)
- Le workflow d'orchestration pour les éléments impliquant la collecte et l'enrichissement des données, et la collecte des approbations de changement et d'autres marqueurs basés sur l'audit
- La mise en œuvre ou la prise en charge supplémentaire d'une procédure ou d'une action pour déployer des modifications aux contrôles de sécurité

Figure 1 : SOAR dans un flux de travail d'incident typique

SOAR in a Typical Incident Workflow



Source: Gartner
719029_C

Gartner

La maturité de l'organisation et des processus est un facteur clé de la réussite de la mise en œuvre des technologies SOAR. Les principales considérations pour une organisation cherchant à acheter une technologie SOAR sont les suivantes :

- Ai-je des processus de sécurité de confiance que je souhaite rendre plus efficaces ou automatiser ?
- Mes technologies de sécurité et mes abonnements existants s'intégreront-ils bien avec un ensemble d'outils tiers via l'API ?
- La technologie SOAR choisie s'aligne-t-elle sur la feuille de route et l'évolution des opérations de sécurité et de l'architecture informatique de l'entreprise ?

Les solutions sur le marché SOAR sont encore à l' état adolescent (voir Hype Cycle for Security Operations, 2020). On s'attend donc à ce que les organisations qui disposent de processus existants solides et d'un environnement de centre d'opérations de sécurité (SOC) bien structuré réussissent le mieux à mettre en œuvre et à tirer parti des produits SOAR.

Les responsables de la sécurité sont confrontés à une capacité réduite à appliquer les politiques en raison de l'augmentation prononcée de la complexité apportée par la transformation numérique accélérée. De plus en plus de plates-formes SaaS, d'appareils et de systèmes industriels appartenant aux utilisateurs non contrôlés et de plates-formes Internet des objets (IoT) réduisent la visibilité ; tous sont à grande échelle, très dynamiques et en dehors des formes traditionnelles de contrôles axés sur la sécurité. Cette complexité crée également un déficit de compétences au sein des organisations ; beaucoup tentent d'utiliser des technologies plus autonomes et intelligentes pour tenter de combler cet écart. La réduction de la complexité des opérations de sécurité est un objectif clé pour de nombreuses organisations. L'automatisation totale ou partielle des processus est complexe en soi, et il existe de nombreux obstacles à sa réussite.

La plupart des produits SOAR ont des avantages fondamentaux et certaines fonctionnalités marginales. Cet avantage de base se classe généralement dans l'une des trois catégories principales :

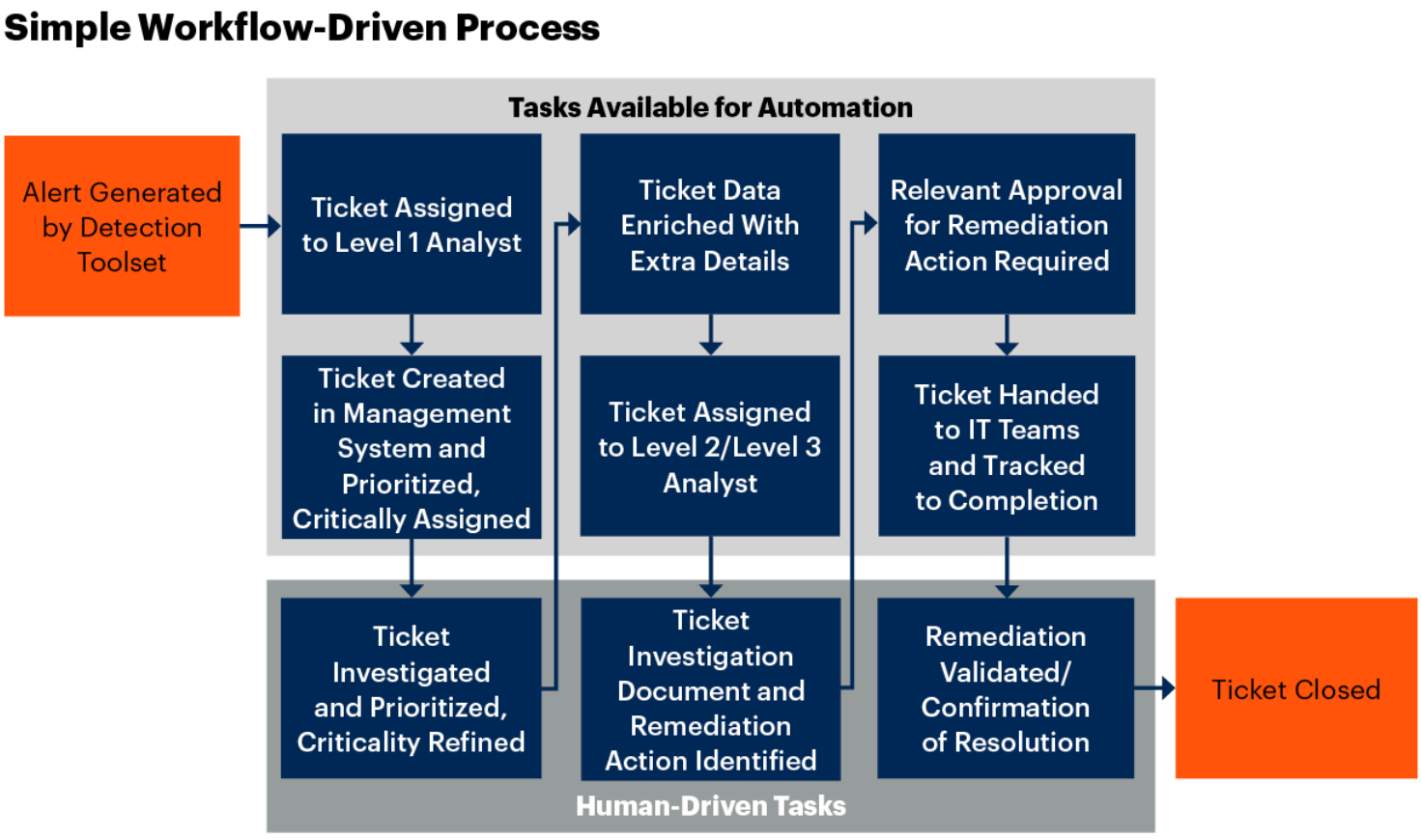
- **Flux de travail de réponse aux incidents** — De nombreux produits sur le marché visent à faciliter le processus de gestion d'un incident de sécurité, à faciliter l'autorisation de modification ou à catégoriser et attribuer correctement les tickets aux bonnes zones. Ils garantissent également que le problème est résolu dans des délais prédéfinis et avec un niveau de détail cohérent.

- **Enrichissement des données** — Après l'identification d'un incident ou pendant la collecte et le traitement des données, les solutions SOAR peuvent aider à intégrer des renseignements externes sur les menaces, effectuer des recherches contextuelles internes ou exécuter des processus pour recueillir des données supplémentaires sur les problèmes.

- **Automatisation des contrôles de sécurité** — La réponse automatisée fournit une résolution « sans analyste » aux problèmes courants en appliquant une forme de réponse utilisant la technologie au sein du parc informatique d'une organisation. Certains peuvent verrouiller un utilisateur et d'autres peuvent appliquer des modifications aux passerelles de messagerie. La fonctionnalité d'automatisation des contrôles de sécurité est la plus percutante, mais aussi la plus complexe et est rarement mise en œuvre pour un ou deux cas d'utilisation triviaux .

Les playbooks prêts à l'emploi et fournis qui traitent ces trois principaux types de scénarios ne sont pas conçus pour fonctionner spécifiquement pour votre organisation. Ils ne prendront pas en compte vos processus internes spécifiques, vos exigences d'intégration technologique ou vos besoins critiques pour l'entreprise. Les responsables de la sécurité et de la gestion des risques doivent examiner ces technologies avec l'espoir qu'ils devront personnaliser les fonctionnalités prêtes à l'emploi ainsi qu'ajuster et reconfigurer en permanence à mesure que les technologies et les processus subordonnés évoluent. La fonctionnalité regroupée avec le produit est précieuse dans la mesure où elle facilitera l'alignement avec les processus internes (voir Figure 2). Il aide également à analyser les écarts pour identifier les domaines dans lesquels les dirigeants aimeraient qu'un SOAR les aide, ainsi que ce qu'ils pourraient avoir à développer à partir de zéro.

Figure 2 : Exemple d'un processus simple axé sur le flux de travail et avantage potentiel de l'automatisation



Source: Gartner
719029_C

Les plates-formes SOAR sont capables de supprimer le besoin de tâches banales et répétables actuellement effectuées par le personnel existant. Cependant, ces tâches doivent être accompagnées d'une documentation à l'appui cohérente, ce qui permet de les adapter à l'automatisation. Une telle approche réduira presque certainement la charge de travail du personnel, mais ne créera généralement qu'un espace permettant à ce personnel d'augmenter ses rôles et d'exécuter un ensemble plus large de fonctions d'opérations de sécurité. Contrairement à une ligne de production robotisée, l'automatisation de ce type ne remplace pas les rôles principaux, mais plutôt un moteur d'efficacité tâche par tâche.

L'automatisation de n'importe quelle partie d'un processus de sécurité est un défi, indépendamment de l'utilisation de technologies telles que SOAR. Mais, avec le volume considérable de tâches requises pour exécuter les fonctions de sécurité, l'automatisation est le seul moyen réaliste pour les organisations de répondre au volume de travail requis. L'automatisation des tâches répétitives et prévisibles crée un espace pour se concentrer sur des fonctions plus critiques. Les organisations qui ne sont pas sur la voie de l'automatisation se retrouveront bientôt dans l'incapacité d'obtenir une valeur efficace de leurs investissements de sécurité existants et des investissements qu'elles n'ont pas encore réalisés.

Une analyse

Examinez les processus des opérations de sécurité interne pour identifier les avantages

SOAR à lui seul ne remplace pas les analystes de sécurité. Le mot clé dans SOAR est l'orchestration, qui est le composant clé qui doit être construit avant que l'automatisation et la réponse puissent être exploitées. L'orchestration, par définition, consiste à arranger ou à manipuler, en particulier au moyen d'une planification ou de manœuvres intelligentes ou approfondies.

> **Tout comme un chef d'orchestre doit diriger l'orchestre pour livrer de la musique, l'équipe des opérations de sécurité doit planifier, organiser et décider comment elle souhaite réagir aux différents types d'événements de sécurité pour obtenir les résultats souhaités.**

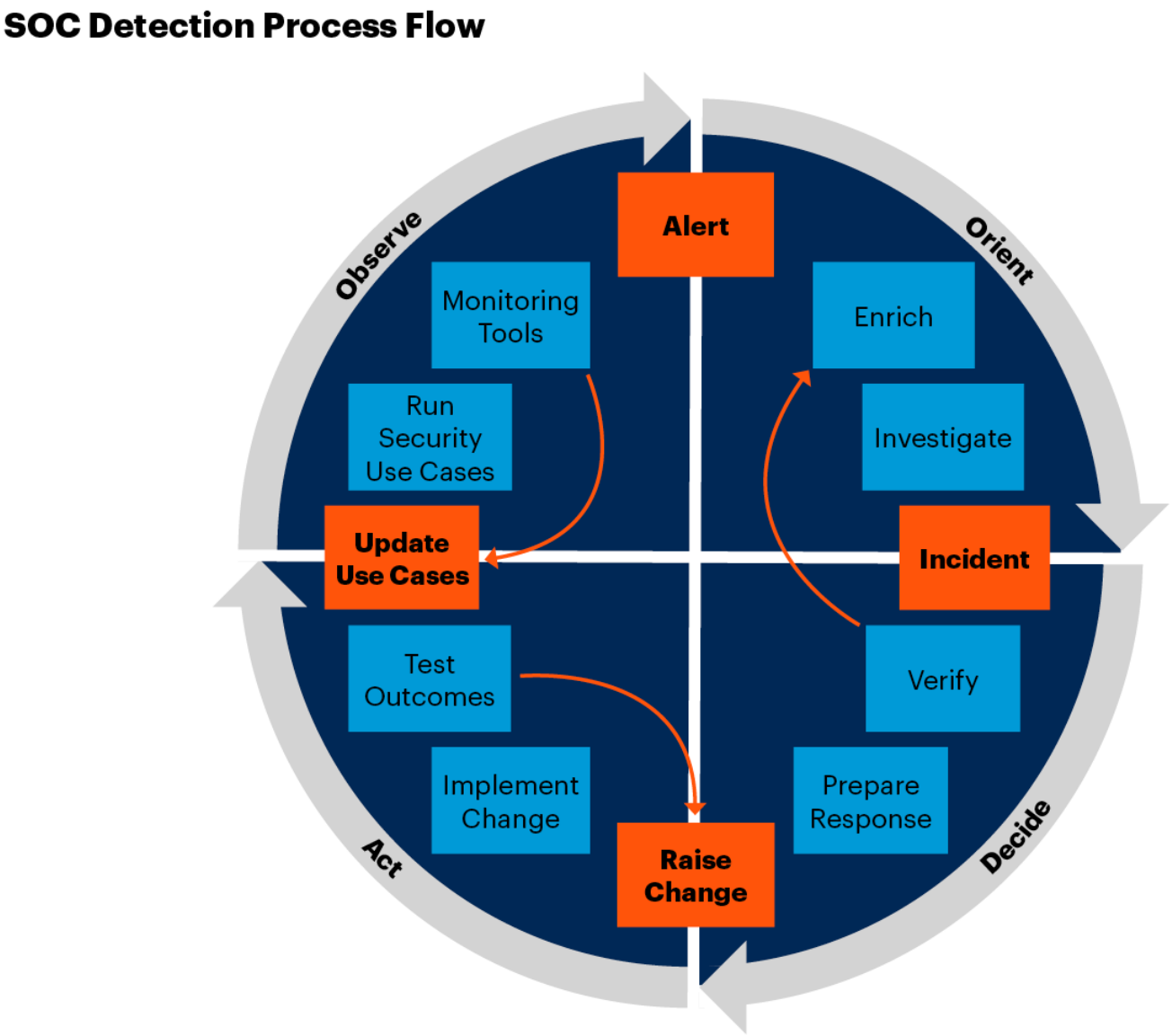
Les équipes d'opérations de sécurité qui souhaitent intégrer une plate-forme SOAR dans leur environnement doivent disposer de processus internes bien définis pour commencer le voyage. La construction de ces processus internes nécessite des compétences du personnel interne qui ne peuvent pas être achetées sur une plate-forme. E type d'événement haque ou processus orchestrées ou améliorés nécessite une analyse humaine pour déterminer les mesures correctives qui font le plus de sens pour la tolérance au risque de l'entreprise ou l'équipe pour intensifier l'événement. Souvent appelée playbooks, l'orchestration en plusieurs étapes doit répondre aux critères initiaux pour lancer le processus d'un événement ou d'un scénario spécifique .

Les plates-formes SOAR peuvent être configurées pour accélérer les processus répétitifs dans les opérations de sécurité (comme le montrent les flèches orange définissant les processus de bouclage dans la figure 3). Par conséquent, les plates-formes peuvent prendre en charge des processus tels que la chasse aux menaces ou les enquêtes sur les incidents, devenant ainsi un « plan de contrôle » pour les équipes

d'enquête SOC. Dans certains cas, ils peuvent également aider à répondre à un incident. Les opérations de sécurité utilisent souvent la boucle observer, orienter, décider et agir (OODA) lors de la définition des processus. Les outils SOAR doivent être utilisés de la même manière pour enrichir ce cadre :

- **Observez** les événements et identifiez ce qui se passe.
- **Orientez** l'observation et ajoutez un contexte pour identifier ce que l'observation signifie.
- **Décider** des actions de réponse appropriées en fonction de la tolérance au risque et de la capacité de l'entreprise.
- **Agir** sur la décision et appliquer ce qui a été appris aux processus d'observation, et répéter.

Figure 3 : Flux de processus de détection SOC en relation avec OODA



Source: Gartner
719029_C

Gartner

Les technologies SOAR peuvent aider une équipe d'opérations de sécurité à identifier des itinéraires plus rapides vers des décisions et des actions de réponse, mais le chemin qu'elles empruntent et la façon dont le risque commercial est évalué sont les compétences qui nécessitent une interaction humaine. Ceci

s'applique également aux actions de réponse. Un playbook bien défini dans un produit SOAR peut créer une vitesse de décision plus efficace. Cependant, la décision de réagir à un événement doit être élaborée et acceptée par l'équipe des opérations de sécurité interne et l'ensemble de l'organisation. Ces décisions sur la manière de réagir sont déterminées par le contexte de l'événement dans l'environnement, la tolérance au risque de l'entreprise et la capacité des équipes en dehors des opérations de sécurité à réagir si nécessaire.

Par conséquent, nous ne pouvons appliquer SOAR qu'aux événements et scénarios auxquels nous nous attendons et auxquels nous savons déjà comment réagir. De nombreux fournisseurs proposent un nombre croissant de playbooks prédéfinis pour des cas d'utilisation spécifiques et des cas d'utilisation créés par leur communauté d'utilisateurs ; ceux-ci peuvent être « glissés et déposés » dans le scénario de réponse, ou les fournisseurs ont des services pour aider à créer des playbooks dans leurs outils. Ceux-ci peuvent être utiles pour aider à surmonter le défi de créer initialement un ensemble de base d'actions d'orchestration et de réponse, mais ils ne constituent pas une solution à long terme et nécessitent une personnalisation et une maintenance régulière.

Il est important de ne pas gaspiller d'argent et d'efforts sur des produits SOAR avant d'avoir parfaitement compris et préparé vos processus internes (voir SOAR : Assessing Readiness Through Use-Case Analysis) . Les responsables de la sécurité et de la gestion des risques ont tendance à se souvenir de l'important investissement en temps et en ressources nécessaires pour déterminer exactement comment l'équipe des opérations de sécurité doit fonctionner. Cette maturité des processus opérationnels préparera bien mieux les équipes d'opérations de sécurité à tirer parti de la technologie SOAR. Même pour une petite équipe d'exploitation, la création de quelques playbooks peut être un catalyseur majeur pour l'adoption et la recherche d'efficacité dans une plate-forme SOAR.

> **L'automatisation des processus interrompus ou incomplets ne rend pas votre organisation de sécurité plus efficace ; cela casse simplement les choses plus rapidement.**

Des ensembles de compétences spécifiques seront nécessaires aux membres de l'équipe interne pour coder et scripter afin de tirer parti d'une plate-forme SOAR et de la maintenir tout au long de sa durée de vie. Ces compétences sont nécessaires car, bien qu'il puisse y avoir des points communs dans la façon de répondre à certains types d'événements de sécurité, aucune organisation n'est construite exactement comme l'autre. Cela signifie que pour créer des actions automatisées ou des playbooks pour orchestrer des événements, les équipes d'opérations de sécurité devront personnaliser et maintenir chacun de ces cas d'utilisation dans la plate-forme SOAR.

Au-delà de la simple maintenance des playbooks et des réponses, beaucoup de travail est nécessaire pour maintenir les connexions API qui sont utilisées pour connecter divers outils de sécurité à une plate-forme SOAR (par exemple, SIEM, EDR, Cloud Access Security Broker [CASB] et Secure Web passerelle [SWG]). SOAR est également un élément clé des plates-formes de détection et de réponse étendues (XDR) visant à fournir des capacités d'orchestration à un écosystème d'outils de sécurité complémentaires (voir Innovation Insight pour la détection et la réponse étendues). Compte tenu à la fois des processus internes et des

exigences de plate-forme pour des ensembles de compétences spécifiques, les dirigeants SRM doivent reconnaître et être prêts à relever les défis afin de tirer efficacement parti de SOAR.

Impliquer l'ensemble de l'organisation de sécurité lors de la définition des exigences pour SOAR

Les exigences d'automatisation et d'orchestration vont bien au-delà des simples processus qui gèrent les alertes à partir d'ensembles d'outils de sécurité. Les entreprises doivent aller au-delà de la simple connexion d'une nouvelle technologie à un SIEM et s'engager à la place avec la communauté de sécurité au sens large, de ceux qui écrivent et appliquent la politique de sécurité à ceux qui exécutent les fonctions de gestion des correctifs. Si vous vous concentrez sur l'automatisation des tâches ou la réduction des frais généraux de personnel et généralement la réduction des coûts d'exploitation, vous devez réaliser des économies de temps égales ou supérieures à celles qui seraient consacrées à la dotation en personnel. Par exemple, si un outil SOAR vous coûterait 100 000 $ et les heures de travail du personnel 200 $, vous devrez alors trouver des tâches équivalant à environ 500 heures ou environ 12,5 semaines de travail pour justifier la valeur de cet investissement. Pour mieux quantifier votre investissement, posez des questions telles que :

- Dans quelle mesure l'efficacité des tâches/processus s'améliorera-t-elle ?
- Quelle taille d'équipe est nécessaire pour être efficace ?
- Quelles métriques seront importantes une fois que j'aurai implémenté SOAR ?

SOAR est une solution de framework trop polyvalente qui a des cas d'utilisation intégrés. Bien que les idées concernant l'investigation, la prévention ou la résolution des problèmes de sécurité au sein de votre organisation soient relativement génériques, l'environnement dans lequel ces outils sont censés fonctionner vous est très spécifique. Ils ne peuvent pas prendre en compte les nuances de l'informatique de votre entreprise, vos processus internes, vos exigences de conformité ou vos besoins culturels et géographiques directement hors de la boîte. L'investissement que vous faites dans SOAR n'est pas simplement le prix associé à la technologie. C'est aussi le temps du personnel pour configurer et maintenir cette configuration ainsi que le coût des compétences requises et des connaissances en sécurité pour le faire efficacement. Certains éléments de processus nécessitent une décision commerciale qu'un outil SOAR ne peut pas appliquer (voirConseils pour sélectionner les bons outils pour votre centre d'opérations de sécurité). De nombreuses tâches secondaires peuvent être automatisées et ne relèvent pas nécessairement du domaine de responsabilité des équipes de sécurité, mais utilisent et bénéficient des données collectées par les outils de sécurité. Les clients Gartner avec des processus d'opérations de sécurité matures pris en charge par SOAR ont commencé à intégrer des processus SOAR en dehors des opérations de sécurité. Les exemples incluent l'intégration et la désintégration des ressources humaines, les rapports et l'audit de gestion des identités et des accès, et les opérations informatiques à l'appui du dépannage.

Les capacités S OAR existent déjà dans de nombreux ensembles d'outils

Lorsqu'elles examinent l'automatisation, les organisations doivent déterminer si les besoins d'automatisation sont déjà satisfaits, en partie par des fonctionnalités déjà existantes dans d'autres outils déployés dans les organisations.

La fonctionnalité dont vous avez besoin existe-t-elle déjà nativement dans l'ensemble de produits et est-elle sous-utilisée ?

SIEM est un excellent exemple où l' intégration avec des fournisseurs de technologies tiers et l'automatisation des flux de travail existent déjà dans une certaine mesure. Une partie de cette automatisation n'existe que sous une forme simple ; d'autres organisations ont réalisé d'importants investissements dans ces domaines et sont déjà probablement plus matures qu'une offre SOAR autonome. Le SIEM est un domaine qui a évolué et continue d'évoluer rapidement, car le volume de données consommées par sa communauté d'utilisateurs peut être écrasant. Des termes tels que « réduction des faux positifs », « réponse automatisée » et « gestion des cas » existaient bien avant la création de SOAR.

Les ensembles d'outils qui gèrent déjà les fonctions de workflow pour la partie informatique de votre entreprise sont également des sources de fonctions d'automatisation qui existent déjà dans les actifs technologiques préachetés . La fonctionnalité peut être innée, ou elle peut être offerte en tant que module supplémentaire achetable. Dans certains cas, il peut être nécessaire de le développer en interne en utilisant les cadres d'API existants du produit ou des fonctions de développement personnalisées spécifiques qui permettent une extension.

Assurez-vous que votre organisation possède les compétences appropriées pour tirer parti efficacement de SOAR

Dans certains cas, la fonctionnalité spécifique dont vous avez besoin d'un ensemble d'outils SOAR ne sera pas disponible en standard. Vous pourrez peut-être tirer parti d'éléments dans les manuels prêts à l'emploi ou dans le cadre de routines et de capacités existantes pour rendre le développement plus efficace. Par conséquent, le fonctionnement n'est pas impossible à réaliser, mais pourrait être nettement plus complexe. Les responsables de la sécurité et de la gestion des risques doivent tenir compte de la disponibilité des compétences en interne pour développer les fonctionnalités requises, ainsi que du temps et des coûts que cela peut ajouter au coût total de possession d'un ensemble d'outils SOAR. La plupart des ensembles d'outils SOAR ont un environnement de développement intégré et une documentation complète pour prendre en charge le développement qui peut être requis ; en fait, c'est un bon indicateur de la fonctionnalité et de la compatibilité de l'outil SOAR si ces spécifications existent. Même si cette documentation est complète et que des intégrations avec les outils actuels existent,

Il est important d'aborder votre projet en sachant que le contenu fourni avec la plupart des produits SOAR n'est pas conçu pour répondre aux cas d'utilisation spécifiques dont votre organisation peut avoir besoin. Souvent, ce contenu consiste en un simple ensemble de workflows ou de playbooks de haut niveau et personnalisables. Ceux-ci sont conçus pour démontrer le concept et soutenir le travail de développement initial afin de garantir que la plate-forme commence à montrer de la valeur dès le début. Dans certains cas, ils fournissent les blocs de construction nécessaires aux équipes opérationnelles et de développement pour intégrer leurs cas d'utilisation spécifiques.

Un long délai est souvent associé à la mise en œuvre et à la configuration d'un ensemble d'outils SOAR. Souvent, cela dépasse trois mois et peut allonger les délais jusqu'à environ, et parfois plus de 12 mois. Le fournisseur ou son partenaire peut proposer des conseils approfondis pour mettre en place et faire fonctionner l'outil. Une considération essentielle à ce stade devrait être le développement et l'ajustement futurs de l'ensemble d'outils. Cela s'applique également à la surcharge continue associée à la maintenance et à la compatibilité des ensembles d'outils de sécurité existants (et potentiels futurs), qui peuvent être introduits pour remplacer l'infrastructure existante à une date ultérieure. Il est nécessaire d'allouer les ressources appropriées avec l'expertise nécessaire pour soutenir les opérations d'un outil SOAR, étendre son utilisation et tirer le meilleur parti de votre investissement.

Preuve

Lors de la préparation de cette recherche, Gartner a utilisé une combinaison d'informations provenant d'interactions avec les clients et de briefings avec les fournisseurs pour cartographier et résoudre les conflits entre les capacités des produits et les défis et attentes des utilisateurs finaux habituels des plates-formes SOAR.