5 scénarios d’utilisation de l’automatisation pour **Splunk SOAR**

splunk>
turn data into doing™

Le centre des opérations de sécurité (SOC) est constamment débordé. Les analystes se noient dans les alertes de sécurité et ont bien trop de menaces à investiguer et à résoudre. Le travail des opérations de sécurité regorge de ces types de tâches monotones, routinières et répétitives, en particulier pour l'analyste de niveau 1.

Pour aggraver les choses, les professionnels de la cybersécurité sont une denrée rare, ce qui rend d'autant plus difficile la prise en charge des milliers d'alertes qui arrivent quotidiennement. Une fois combinés, tous ces facteurs entraînent un ralentissement considérable de la détection et de la prise en charge des menaces, ce qui est loin d'être idéal pour l'entreprise ou pour la sécurité des utilisateurs et des actifs.

La bonne nouvelle ? Votre équipe de sécurité débordée peut reprendre le contrôle avec Splunk SOAR. Vous pouvez éliminer les tâches fastidieuses des analystes, rationaliser vos opérations de sécurité et détecter, trier et prendre en charge les alertes plus rapidement que jamais.

Une solution d'orchestration, d'automatisation et de réponse de sécurité (SOAR) peut assumer les tâches les plus banales ou répétitives. Tout processus impliquant la détection, investigation, le confinement (et même des éléments logistiques, comme la communication interfonctionnelle via des tickets) peut être orchestré sur l'ensemble des outils informatiques et de sécurité que vous possédez, et automatisé sans aucune interaction humaine.

Dans cet e-book, nous vous présentons cinq scénarios d'utilisation courants du SOAR, les étapes à suivre dans chacun d'eux, et comment automatiser ces étapes à l'aide d'un playbook prédéfini de Splunk SOAR.

Sommaire

1. Enrichissement des alertes

Lorsqu'il s'agit d'investiguer les alertes de sécurité, la première tâche de l'analyste consiste à examiner les indicateurs de compromission (IOC) tels que l'adresse IP, l'URL, le nom d'utilisateur, le domaine, le hash et tout autre critère pertinent. Cela permet de déterminer la gravité de l'alerte. De nombreux analystes vont ensuite s'immerger dans les données pour obtenir davantage de contexte, ou basculer entre différentes plateformes d'informations sur les menaces pour recueillir plus d'informations.

Un outil SOAR peut facilement combiner les informations de plusieurs outils du SOC, enrichir les données d'alerte et les présenter dans une interface unique. En automatisant le processus de collecte et d'enrichissement des données à partir de diverses sources, l'analyste peut voir de précieux détails liés à l'alerte dès qu'elle fait surface. L'orchestration et l'automatisation aident les analystes à investiguer et à répondre aux alertes de sécurité beaucoup plus rapidement, et enrichissent également les données qu'ils collectent en compilant des informations provenant de diverses sources en un seul endroit.

Le playbook Enrichissement des indicateurs de Recorded Future enrichit les événements importés qui contiennent des hashes de fichiers, des adresses IP, des noms de domaine ou des URL. La mise en contexte de ces informations à l'aide d'informations pertinentes sur les menaces et d'IOC permet d'accélérer les investigations. Recorded Future est une plateforme d'informations de sécurité qui fournit un contexte supplémentaire aux analystes pour leur permettre de répondre plus rapidement aux menaces.

Ce playbook fournit plusieurs actions :

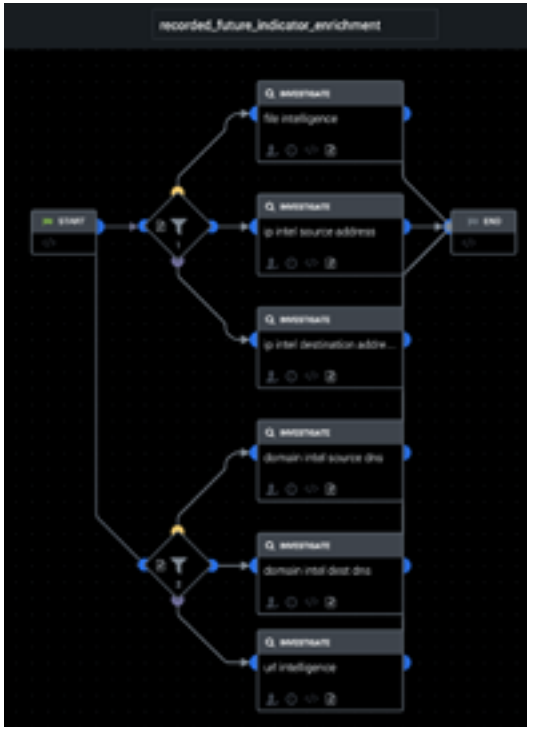
1. **Informations sur les domaines :** obtenez des informations sur les menaces concernant un domaine ;
2. **Informations sur les fichiers :** obtenez des informations sur les menaces concernant un fichier identifié par son hash ;
3. **Informations sur les IP :** obtenez des informations sur les menaces concernant une adresse IP ;
4. **Informations sur les URL :** obtenez des informations sur les menaces concernant une URL.

Cessez de travailler plus, travaillez mieux. Splunk SOAR automatise les tâches répétitives telles que l'enrichissement des alertes afin de fournir aux analystes de sécurité tout ce qu'ils doivent savoir sur l'alerte avant de commencer à investiguer. Utilisez ce playbook prédéfini dans Splunk SOAR et collectez rapidement des analyses pour tout type d'investigation.

Obtenez le playbook

L'équipe de sécurité de Norlys applique un principe clair : si quelque chose est pénible, on l'automatise. Le résultat : l'équipe utilise chaque jour 20 playbooks différents pour économiser du temps et de l'argent.

> **« Splunk SOAR nous fait gagner 35 heures par semaine, soit environ cinq heures par jour. Nous pouvons enfin nous concentrer sur les tâches importantes. »**
>
> – M. Tibor Földesi, Analyste de sécurité, Norlys



2. Investigation et prise en charge de l'hameçonnage

Le Rapport d'investigation sur les violations de données 2021 de Verizon[1] nous apprend que l'hameçonnage est toujours l'une des principales causes de violations au cours des deux dernières années. Les attaques par hameçonnage restent l'une des menaces les plus répandues pour les entreprises aujourd'hui.

Une investigation classique sur un cas d'hameçonnage par e-mail commence par l'analyse des données initiales et la recherche d'artefacts. Ces artefacts incluent notamment les pièces jointes de l'e-mail, les liens d'hameçonnage déguisés en URL légitimes, les en-têtes d'e-mail, l'adresse e-mail de l'expéditeur et même l'intégralité du contenu de l'e-mail. Une fois l'e-mail identifié comme malveillant, l'analyste de sécurité doit procéder à son confinement et empêcher les membres de l'entreprise d'être victimes de l'attaque. Habituellement, l'analyste de sécurité peut supprimer l'e-mail de la boîte de réception de l'utilisateur, dans la mesure du possible avant que l'utilisateur n'ait la possibilité de l'ouvrir. Maintenant, imaginez réaliser *toutes* ces étapes manuellement, pour chaque alerte d'hameçonnage reçue.

90
minutes
par alerte d'hameçonnage

Avant SOAR

60
secondes
par alerte d'hameçonnage

Après SOAR

L'ajout d'un outil SOAR vous aidera à gagner du temps et à vous concentrer sur les tâches critiques.

Un client de Splunk SOAR[2] relate qu'il faut en moyenne 90 minutes à son équipe pour investiguer et contenir une seule alerte d'hameçonnage. En plus de cela, son SOC reçoit jusqu'à 300 e-mails d'hameçonnage par jour. Non seulement les analystes de sécurité sont submergés par un déluge d'alertes d'hameçonnage à analyser et traiter, mais traiter chacune d'elle prend trop de temps pour empêcher à coup sûr la menace potentielle de provoquer des dommages irréversibles.

Dans ce scénario d'utilisation, nous allons mettre en lumière le playbook Investigation et réponse à l'hameçonnage, qui analyse les e-mails d'hameçonnage entrants et les confine automatiquement. Le playbook regroupe un total de 15 actions. Lorsque Splunk SOAR reçoit une alerte d'e-mail d'hameçonnage d'une source tierce (par exemple, en récupérant les e-mails directement à partir du serveur de messagerie), il lance automatiquement le playbook et commence à analyser les artefacts suivants :

1. **Réputation des fichiers :** interroge VirusTotal pour obtenir des informations sur la réputation des fichiers ;
2. **Réputation de l'URL :** soumet un seul lien de site web au verdict WildFire ;
3. **Réputation du domaine :** évalue le risque d'un domaine donné ;
4. **Réputation de l'IP :** interroge VirusTotal pour obtenir des informations sur l'IP ;
5. **Géolocalisation de l'adresse IP :** interroge MaxMind pour obtenir des informations sur la localisation de l'adresse IP ;
6. **Identification whois du domaine :** exécute une recherche whois sur le domaine donné ;
7. **Identification whois de l'IP :** exécute une recherche whois sur l'IP donnée.

Ensuite, le playbook va collecter des informations sur le fichier joint et l'URL de l'e-mail et lancer deux actions :

8. **Détonation du fichier :** exécute le fichier dans le sandbox Threat Grid et récupère l'analyse ;
9. **Détonation de l'URL :** charge l'URL dans le sandbox Threat Grid et récupère l'analyse.

1 2021 Data Breach Investigations Report
2 Case study: Automating Phishing Investigations at Rackspace

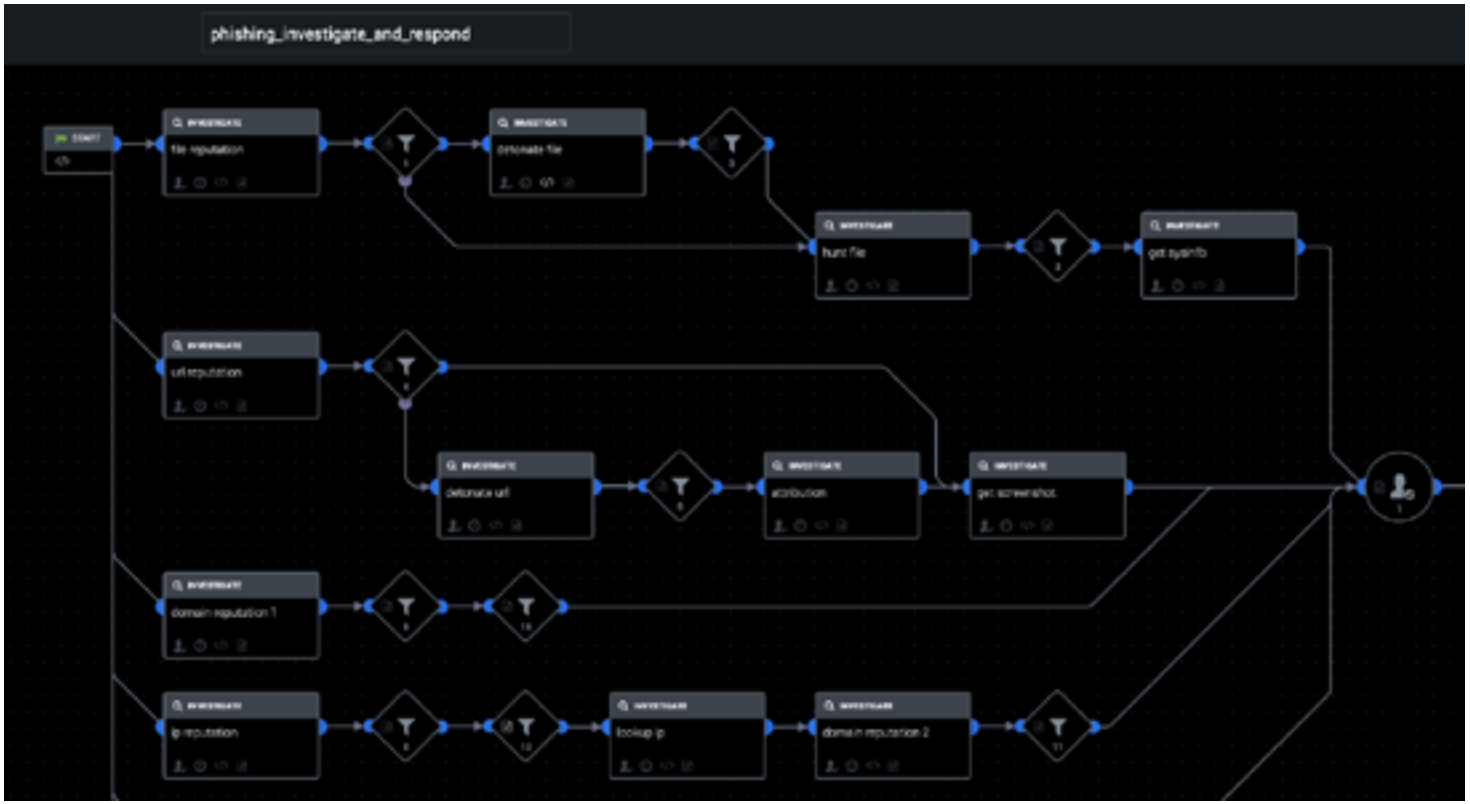
Si, pendant la phase d'investigation, le fichier, l'URL, l'adresse IP ou le domaine semble suspect de quelque manière que ce soit, le playbook utilise des paramètres prédéterminés pour prendre la décision de contenir la menace en supprimant l'e-mail de la boîte de réception de l'utilisateur.

Protégez votre organisation contre les risques de violation en exploitant la puissance de Splunk SOAR, et optimisez vos investigations pour répondre aux alertes d'hameçonnage en un temps record.

« L'hameçonnage représente 36 % des violations, contre 25 % l'an dernier. »

– Rapport d'investigation sur les violations de données 2021, Verizon

Obtenez le playbook

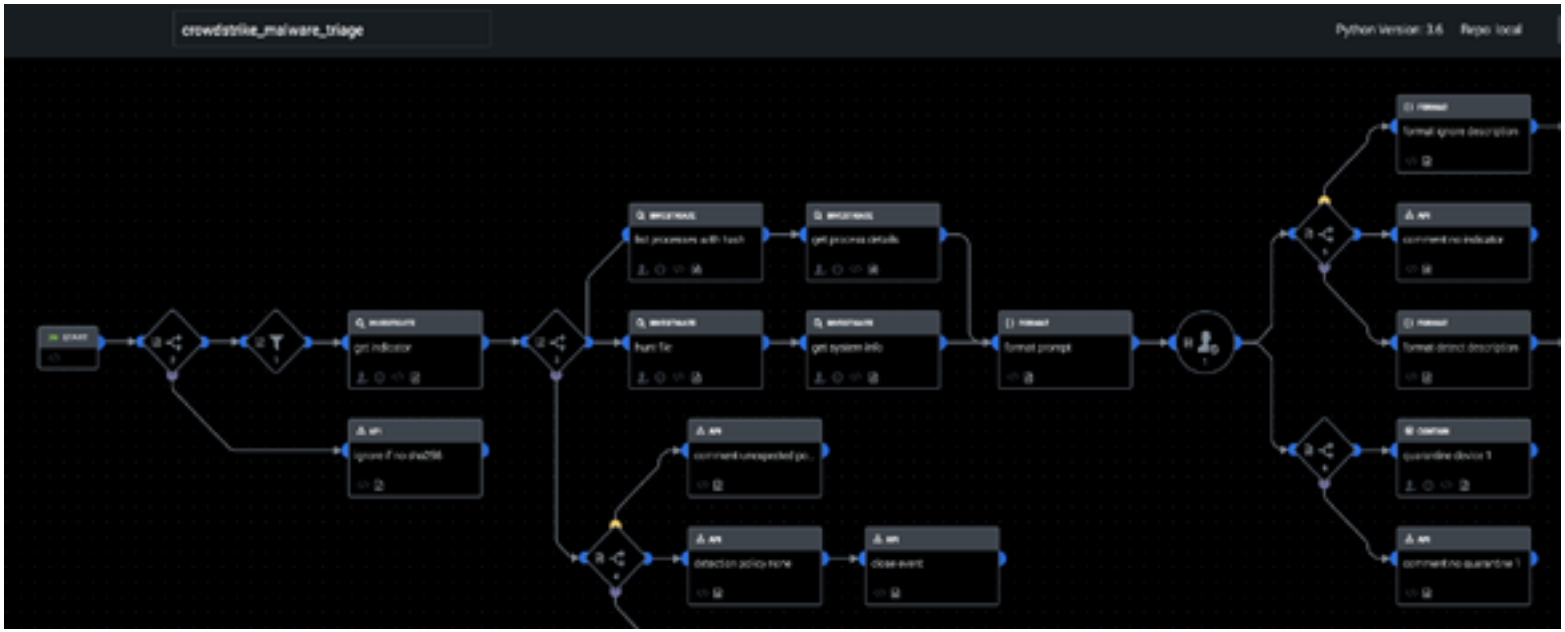


3. Tri des logiciels malveillants aux points de terminaison

Les outils de détection et de réponse aux points de terminaison sont parfaits pour superviser et collecter des données d'activité à partir des terminaux d'un réseau. À l'heure où le monde adopte progressivement des méthodes de travail à distance plus flexibles (et passe à une infrastructure hébergée dans le cloud), la visibilité des points de terminaison reste une priorité pour toutes les équipes de sécurité.

Bien que les outils de détection et de réponse des points de terminaison (EDR) ou les plateformes de protection des terminaux (EPP) puissent faciliter la supervision des activités suspectes présentes sur les terminaux des systèmes de votre organisation, ces outils peuvent générer une surabondance d'alertes, dont certaines peuvent être de faux positifs, tandis que d'autres signalent des menaces réelles. Heureusement, un outil SOAR peut orchestrer des décisions et des actions pour examiner, trier et traiter rapidement ce volume élevé d'alertes, en plus de filtrer les faux positifs, de déterminer le niveau de risque et de répondre en conséquence.

C'est d'ailleurs précisément ce que fait le playbook Tri des logiciels malveillants de Crowdstrike. Il enrichit l'alerte détectée par Crowdstrike et fournit un contexte supplémentaire pour en déterminer le degré de gravité. Une fois toutes les informations collectées, il invite l'analyste à l'examiner. Selon le choix de l'analyste, le fichier en question peut être ajouté à la liste des indicateurs personnalisés dans Crowdstrike avec la politique de détection « détecter » ou « aucun », et le point de terminaison peut éventuellement être mis en quarantaine et isolé du réseau par l'analyste. Autre avantage de ce playbook : il va retrouver les alertes passées similaires et catégoriser le hash du fichier, afin que les futures alertes puissent provoquer la même action de réponse sans déranger l'analyste.



Ce playbook fournit plusieurs actions :

1. **Obtention de l'indicateur :** obtient un IOC en fournissant un type et une valeur ;
2. **Obtention des détails du processus :** récupère les détails d'un processus en cours d'exécution ou exécuté précédemment, en fonction d'un ID de processus ;
3. **Obtention d'informations sur le système :** obtient les détails d'un dispositif sur la base de son ID ;
4. **Recherche de fichier :** recherche un fichier sur le réseau à l'aide de requêtes ciblant le hash ;
5. **Énumération des processus :** liste les processus qui ont récemment utilisé l'IOC sur un appareil particulier ;
6. **Mise en quarantaine du dispositif :** bloque le dispositif ;
7. **Téléchargement d'indicateur :** télécharge un ou plusieurs indicateurs que vous souhaitez que CrowdStrike examine.

« L'automatisation avec Splunk SOAR nous permet de traiter les alertes d'e-mail infecté en 40 secondes environ contre 30 minutes auparavant, voire plus. »

– M. Adam Fletcher, RSSI, Blackstone

Selon les recherches du Ponemon Institute, une entreprise peut recevoir en moyenne 17 000 alertes de logiciels malveillants par jour[3]. Lorsque vous recevez une telle abondance d'alertes, il est souvent difficile de hiérarchiser celles qui doivent être traitées immédiatement. Blackstone, une grande société d'investissement, a utilisé Splunk SOAR pour trier et traiter les alertes entrantes en moins d'une minute. Lire l'étude de cas.

Utilisez ce playbook prédéfini dans Splunk SOAR pour trier les alertes et identifier celles qui sont susceptibles d'avoir les conséquences les plus lourdes.

Obtenez le playbook
Découvrez-le en action

3 Ponemon Institute – The Cost of Malware Containment

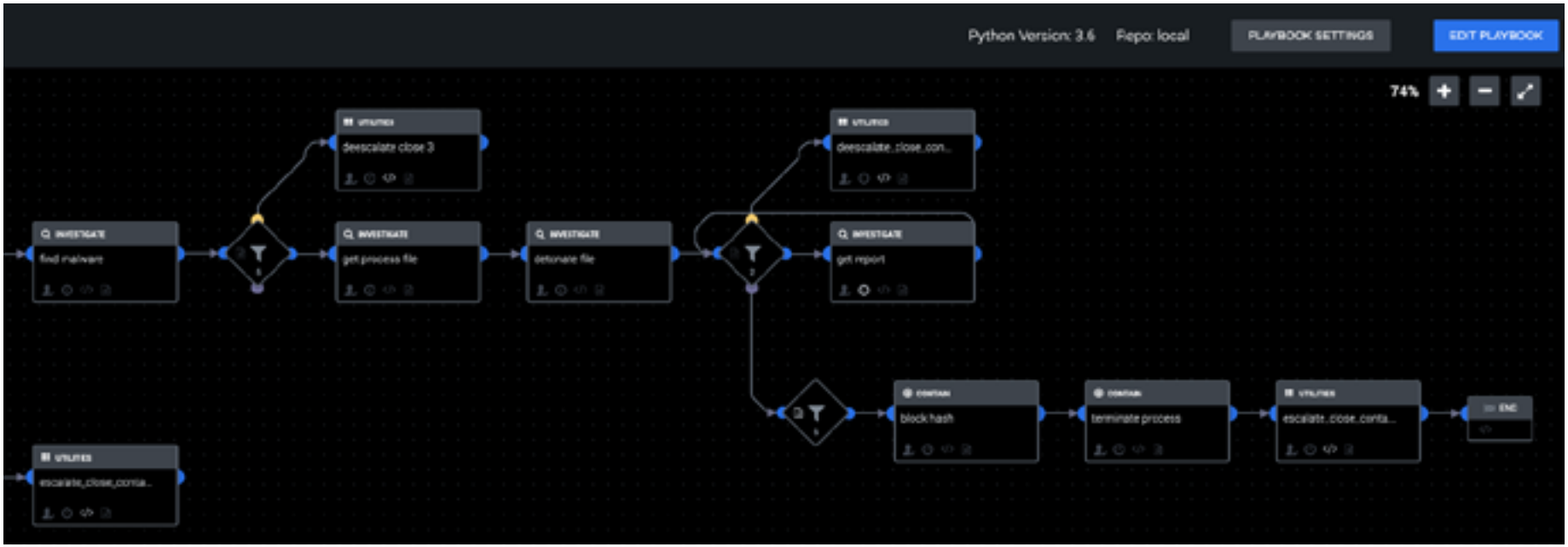
4. Commande et contrôle : investigation et confinement

Une attaque par commande et contrôle (C&C ou C2) se produit lorsqu'un adversaire infecte un ordinateur et a la capacité de lui envoyer des commandes. Il accède à la machine en exploitant les vulnérabilités d'une application logicielle ou au moyen d'un e-mail d'hameçonnage contenant une URL malveillante ou une pièce jointe qui, une fois ouverte, exécute un code malveillant.

Une fois que l'adversaire a établi une connexion entre son serveur et la machine infectée, il est alors en mesure de la contrôler en envoyant des commandes depuis le serveur. Le malfaiteur peut ensuite effectuer un certain nombre d'opérations pour prendre le contrôle d'autres machines sur le réseau, exfiltrer des données sensibles ou même arrêter les systèmes.

Splunk SOAR peut vous aider à investiguer et à contenir des scénarios de commande et de contrôle en quelques minutes, au lieu de plusieurs heures.

Dès qu'une alerte d'attaque par commande et contrôle apparaît, Splunk SOAR lance le playbook Investiguer et confiner C2. Ce playbook est conçu pour effectuer les étapes d'investigation et de confinement potentiel nécessaires pour répondre de façon adéquate à un scénario d'attaque par commande et contrôle. Il va extraire les informations de fichier et de connexion d'une machine virtuelle compromise, enrichir les informations, puis prendre des mesures de confinement en fonction de l'importance des informations. On appelle informations importantes, par exemple, les fichiers ayant un score de menace supérieurs à 50 et les adresses IP ayant le statut de réputation « MALVEILLANT », entre autres attributs.



Ce playbook fournit plusieurs actions :

1. **Blocage du hash :** ajoute un hash à la liste noire Carbon Black ;
2. **Blocage de l'adresse IP :** bloque une adresse IP ;
3. **Recherche de logiciels malveillants :** exécute le plugin de volatilité malfind pour trouver le code/dll injecté dans la mémoire en mode utilisateur ;
4. **Géolocalisation de l'adresse IP :** interroge MaxMind pour obtenir des informations sur la localisation de l'adresse IP ;
5. **Obtention du fichier de processus :** extrait le fichier de processus du dump mémoire ;
6. **Obtention du rapport :** obtient plus de détails sur une balise AutoFocus ;
7. **Recherche d'adresse IP :** recherche une adresse IP et récupère une liste de balises associées ;
8. **Liste des VM :** dresse la liste des VM enregistrées ;
9. **Envoi d'e-mail :** envoie un e-mail ;
10. **Instantané des VM :** prend un instantané de la ou des VM ;
11. **Fin de processus :** tue les processus en cours d'exécution sur une machine ;
12. **Identification whois de l'IP :** exécute une recherche whois sur l'IP donnée.

Utilisez ce playbook prédéfini dans Splunk SOAR pour investiguer et contenir un scénario de commande et de contrôle.

Obtenez le playbook

« Ce qui m'a le plus impressionné dans l'attaque SolarWinds, c'est le savoir-faire parfait des malfaiteurs. Non seulement ils ont effectué une attaque sans faille, mais ils se sont assurés de cacher leurs traces en utilisant des adresses IP, des VPS et des domaines qui étaient géographiquement corrects ou imitaient précisément la victime qu'ils attaquaient. »

– Ryan Kovar, éminent Stratège en sécurité chez Splunk

5. Threat Intelligence

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

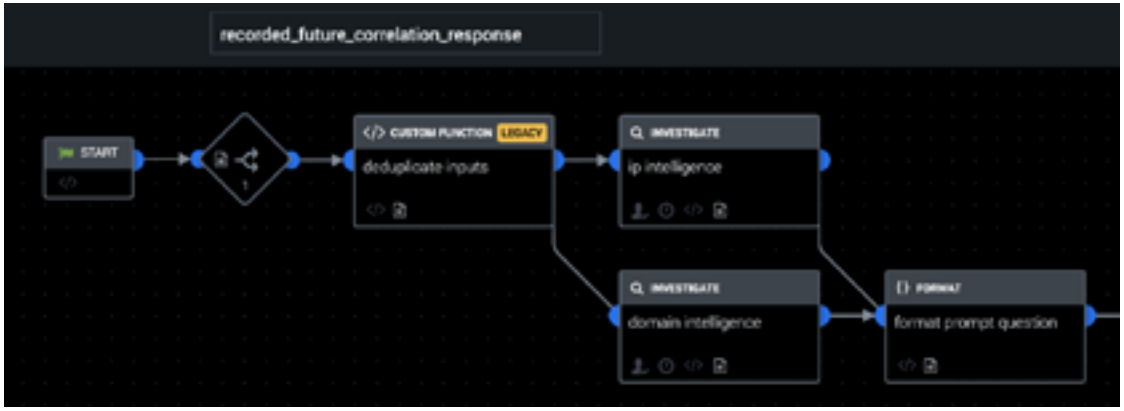
De nombreuses équipes de sécurité utilisent aujourd'hui des plateformes d'informations sur les menaces pour fournir à leurs analystes un contexte et des éléments d'information pertinents pour les aider à comprendre la menace plus rapidement. Mais bien souvent, ils doivent naviguer parmi une multitude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

Dans ce scénario d'utilisation, vous verrez comment le playbook Corrélation de Recorded Future est employé pour rassembler davantage de contexte sur les indicateurs de réseau pertinents, en réponse à une recherche de corrélation Splunk. Une fois muni de suffisamment de contexte, le playbook bloque automatiquement l'accès, sur approbation d'un analyste. En comparant les données de supervision du trafic aux flux de menaces groupés de Recorded Future, Splunk identifie les connexions réseau à haut risque et les transmet à Splunk SOAR. Splunk SOAR interroge Recorded Future pour savoir pourquoi les indicateurs de réseau figurent sur la liste des menaces puis présente une décision à l'analyste quant au blocage de l'adresse IP et des noms de domaine. Dans cet exemple, la supervision du trafic de couche 4 par Cisco WSA est utilisée comme source de données de supervision du réseau, et Cisco Firepower NGFW et Cisco Umbrella peuvent être utilisés pour appliquer des actions de blocage au périmètre et utiliser des décharges DNS.

Ce playbook fournit les actions suivantes :

1. **Blocage de l'adresse IP :** bloque un réseau IP ;
2. **Informations sur les domaines :** obtenez des informations sur les menaces concernant un domaine ;
3. **Informations sur les IP :** obtenez des informations sur les menaces concernant une adresse IP.

Obtenez le playbook



Une fois que l'analyste parvient à bloquer l'accès au réseau via le playbook Corrélation de Recorded Future, Splunk SOAR peut déclencher un deuxième playbook pour investiguer, rechercher et bloquer une URL. Non seulement Splunk SOAR peut orchestrer des actions sur une multitude de produits de sécurité, mais il peut également déclencher plusieurs playbooks pour résoudre un seul incident, et c'est là tout son intérêt.

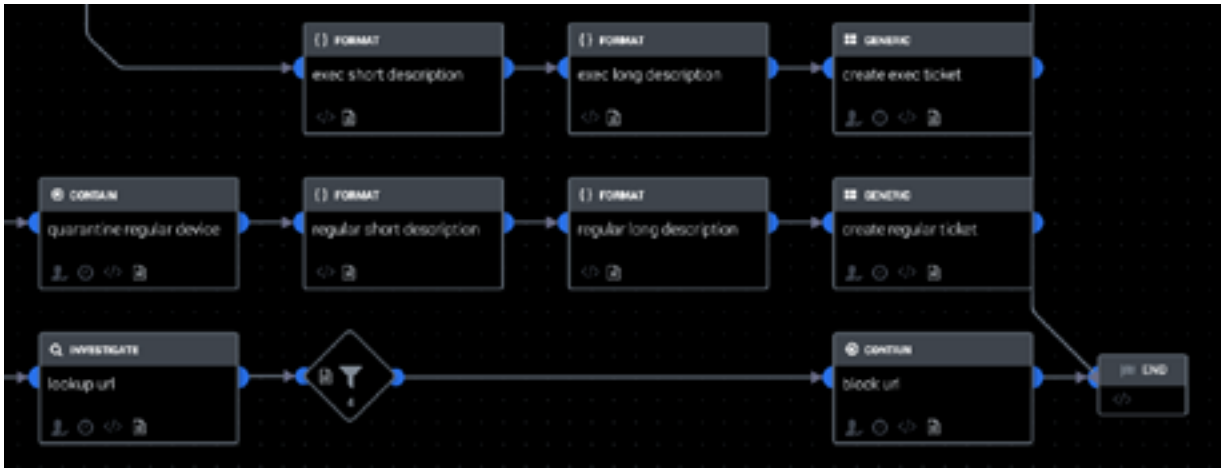
Lorsqu'une URL suspecte est détectée, le playbook Détection et blocage d'URL de Zscaler permet d'identifier les dispositifs internes qui ont accédé à cette URL et trier l'importance de ces dispositifs pour l'organisation. Ensuite, en fonction du degré de malveillance de l'URL et selon que l'appareil concerné appartient ou non à un cadre de l'entreprise, l'URL sera bloquée et un ticket ServiceNow sera créé. Ce playbook est pris en charge via VirusTotal, Zscaler, Microsoft Exchange, ServiceNow, Splunk et Carbon Black.

Ce playbook fournit les actions suivantes :

1. **Blocage d'URL :** bloque une URL ;
2. **Création de ticket :** crée un incident ;
3. **Obtention des attributs utilisateur :** obtient les attributs d'un utilisateur ;
4. **Recherche d'URL :** recherche les catégories liées à une URL ;
5. **Mise en quarantaine du dispositif :** met le point de terminaison en quarantaine ;
6. **Exécution de requête :** obtient des données d'objet en fonction de la requête spécifiée ;
7. **Réputation de l'URL :** demande à VirusTotal des informations sur l'URL.

Les informations sur les menaces peuvent être utilisées pour enrichir un large éventail de scénarios d'utilisation, ce qui en fait une ressource essentielle pour les équipes de sécurité lorsqu'elles investiguent les alertes. Utilisez ces playbooks prédéfinis pour aider votre équipe à gagner du temps dans la recherche d'indicateurs malveillants, et ainsi lui permettre de consacrer plus de temps à la gestion des tâches critiques.

Obtenez le playbook



Décuplez les capacités de vos opérations de sécurité

Maintenant que vous connaissez SOAR et certains scénarios d'utilisation courants, nous espérons que vous pourrez donner à votre équipe de sécurité les moyens de lutter contre les déluges d'alertes et de gagner en efficacité en exploitant la puissance de l'automatisation et de l'orchestration. Rappelez-vous qu'avec SOAR, vous pouvez :

- investiguer les menaces et y répondre plus rapidement ;
- augmenter l'efficacité et la productivité du SOC ;
- éliminer les tâches fastidieuses des analystes afin qu'ils cessent de travailler plus et commencent à travailler mieux ;
- rendre à votre équipe débordée le contrôle sur les opérations de sécurité.

Pensez à essayer notre édition communautaire gratuite et nos playbooks prédéfinis.

En savoir plus

21-19396-Splunk-Five Automation Use Cases For Splunk SOAR-EB-111

splunk> turn data into doing™