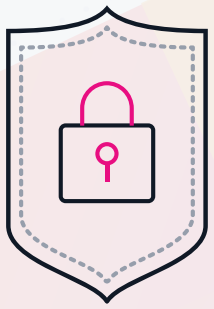
Le Guide essentiel sur la **sécurité**

Bien démarrer avec Splunk pour la sécurité et relever les défis du quotidien



Quel est votre plan de cybersécurité ?

Vous contentez-vous de « prévoir le pire en espérant le meilleur » ?

Sommaire

Comment faire alors pour défendre au mieux votre entreprise et traquer ces nouveaux adversaires ?

En fin de compte, il s’agit d’adopter une approche holistique de votre système de défense à l’échelle de toute l’entreprise.

Introduction

Quel est votre plan de cybersécurité ? Vous contentez-vous de « prévoir le pire en espérant le meilleur » ? Les technologies numériques affectent tous les aspects de nos vies et de nouvelles menaces apparaissent chaque jour. Dans un tel contexte, votre entreprise doit impérativement être précise, informée et préparée à défendre ses actifs et à traquer ses adversaires.

Les failles de grande envergure, les attaques globales par ransomware et l’épidémie d’extraction illégale de cryptomonnaies sont autant d’excellentes raisons pour votre entreprise de collecter, exploiter et comprendre les bonnes données. Vous devez également mettre en œuvre les processus et procédures adaptés, bien souvent tout en implémentant de nouvelles technologies, méthodes et exigences, et en prenant en compte la vélocité et la diversité croissantes des données machine.

Comment faire alors pour défendre au mieux votre entreprise et traquer ces nouveaux adversaires ? En fin de compte, il s’agit d’adopter une approche holistique de votre système de défense à l’échelle de toute l’entreprise. C’est pour cela que, chez Splunk, nous pensons que chaque entreprise a besoin d’un centre névralgique de sécurité, qui sera mis en place à l’aide d’un parcours de sécurité en six étapes que nous allons décrire.

Voyons dans le détail ce qu’il en est.

Splunk dans le centre d'opérations de sécurité (SOC)

Les entreprises axées sur les données exploitent le modèle « investigation, supervision, analyse et action » (IMAA) pour renforcer leur sécurité en optimisant leurs ressources humaines, leurs processus et leur technologie. Cela consiste à utiliser toutes les données de la pile technologique de sécurité, afin de vous aider à investiguer et détecter rapidement les menaces pour agir sans délai de façon manuelle, semi-automatique ou entièrement automatisée. Lorsqu'une équipe de sécurité investit dans son infrastructure de sécurité, elle renforce son écosystème de sécurité et ses compétences, ce qui lui permet d'étendre ses pratiques de sécurité à de nouveaux domaines et de traiter proactivement les menaces.

La plateforme Data-to-Everything Splunk et le portefeuille de sécurité de Splunk regroupent plusieurs domaines de cybersécurité ainsi que des domaines extérieurs, afin de favoriser la collaboration et la mise en œuvre des bonnes pratiques dans les interactions avec vos données. Les équipes de sécurité peuvent utiliser les solutions Splunk pour produire des analyses statistiques, visuelles, comportementales et exploratoires qui vont ensuite informer des décisions et des actions. Ensuite, la plateforme offre un workflow moderne permettant aussi bien de collecter des données, d'invoquer des actions que de prendre en charge les cybermenaces et les défis de sécurité.

Figure 1 : Splunk Enterprise Security comprend un framework commun pour interagir avec les données et invoquer des actions. Le cadre Adaptive Operations permet aux équipes de sécurité d'apporter rapidement et en toute confiance des modifications à l'environnement. Splunk Enterprise Security peut également automatiser la réponse et permettre ainsi à l'infrastructure de réagir à l'attaque en recourant à un éventail d'actions appropriées à chaque domaine.

Ça vous plaît ?

Parfait. Et vous vous demandez sans doute : comment faire pour concrétiser tout cela dans le monde réel ?

Pour vous permettre de prendre un bon départ, nous avons rédigé ce guide rapide qui présente les principaux scénarios de sécurité rencontrés par les entreprises et montre comment la plateforme axée sur l'analyse de Splunk peut vous aider à relever ces défis. Ce guide est divisé en trois sections :

1. **Comprendre les fondamentaux.** Vous trouverez ici une introduction au parcours de sécurité et une présentation rapide des différents scénarios de sécurité, associés aux solutions Splunk pertinentes.

2. **Entreprendre votre parcours de sécurité axée sur l'analyse.** Nous allons ensuite aborder les six étapes du parcours de sécurité axée sur l'analyse en détaillant ce que vous devriez pouvoir faire à chacune d'elle.

3. **Résoudre les problèmes de sécurité courants avec Splunk.** Nous allons enfin aborder des exemples de prise en charge de défis de sécurité courants associés aux scénarios suivants :

   - Investigation et analyse des incidents
   - Supervision de sécurité
   - Détection des menaces avancées
   - Automatisation du SOC
   - Réponse aux incidents et conformité
   - Détection et analyse des fraudes
   - Menaces internes

Prêt à mettre en place une unité de sécurité performante ? C'est bien ce qu'il nous semblait.

Comprendre les fondamentaux

Les cybercriminels ne s'arrêtent jamais, ce qui signifie que vous devez être constamment à l'affût de nouveaux scénarios et informations de sécurité afin de maintenir des niveaux de protection élevés dans votre environnement.

Nous sommes là pour vous aider.

Parcours Splunk de sécurité axée sur l'analyse

Tous ceux à qui on a un jour demandé « Sommes-nous en sécurité ? » savent que la cybersécurité est un parcours, et non une destination. Si l'expédition n'a pas de destination finale, et s'il y aura toujours des difficultés en chemin, vous pouvez prendre des mesures pour faciliter votre voyage.

En premier lieu, vous devez comprendre votre environnement et trouver par quel domaine commencer. Posez-vous les questions suivantes : Qu'est-ce que j'essaie de protéger ? Quelles sont mes données stratégiques ? Comment puis-je répondre aux menaces ?

Le parcours de sécurité axée sur l'analyse en six étapes, illustré par la Figure 2, va vous aider à répondre à ces questions et à mettre sur pied une unité de sécurité hautement performante qui vous permette de comprendre les lacunes dans vos défenses, de voir le prochain défi et de prendre des mesures pour le relever sans trembler.

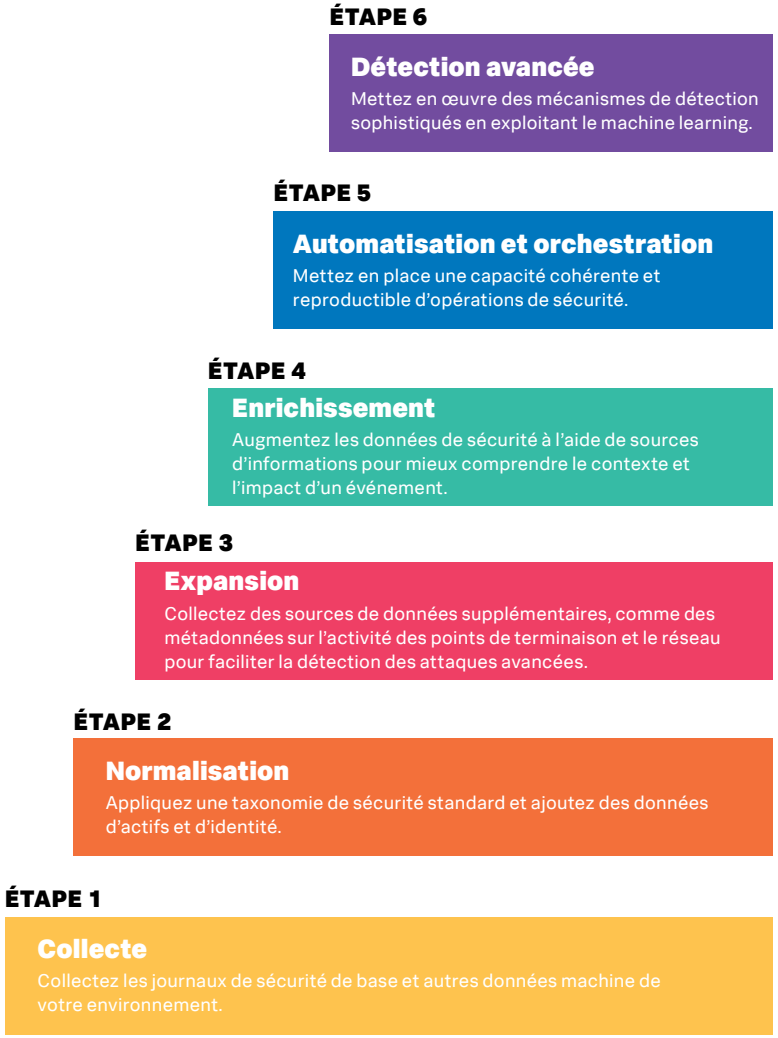
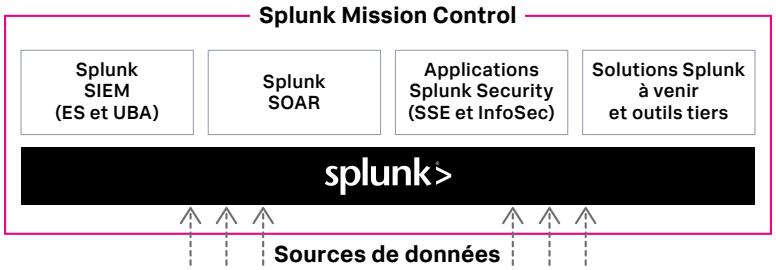


Figure 2 : Le parcours Splunk de sécurité axé sur l'analyse

Splunk Security Suite

Partiriez-vous en randonnée sans une bonne carte, un sac à dos plein de provisions et un équipement adapté ? Bien sûr que non. Tout comme la réussite d'un voyage nécessite le bon équipement, réussir son parcours de sécurité impose d'avoir la bonne technologie.



La suite Splunk Security Suite aide les équipes de sécurité à naviguer dans des eaux inconnues et à identifier, investiguer et prendre en charge rapidement les menaces, dans des environnements commerciaux dynamiques et numériques. Les solutions Splunk peuvent être utilisées par un analyste de niveau 1 pour effectuer des recherches de base sur une période donnée, un mot-clé, une adresse IP ou un nom de machine. Les mêmes produits permettent aux analystes avancés de niveaux 2 et 3 d'effectuer des corrélations sophistiquées, d'élaborer des modèles analytiques ou de réaliser des investigations scientifiques poussées.

Splunk Security Suite	
Splunk Enterprise	Est une plateforme flexible qui prend en charge un grand éventail de scénarios de sécurité, en vous permettant de superviser et d'analyser rapidement les données machine de n'importe quelle source afin de fournir des informations exploitables et créer des fondations axées sur l'analyse en vue de renforcer votre sécurité globale. Disponible dans le cloud.
Splunk Enterprise Security	Solution de gestion des événements et des informations de sécurité (SIEM) fournissant des informations sur les données machine générées par des technologies de sécurité, et notamment des informations concernant les réseaux, les terminaux et les accès, mais aussi les logiciels malveillants, les vulnérabilités et les identités. Disponible dans le cloud.
Splunk User Behavior Analytics	Solution fondée sur le machine learning qui vous fournit les réponses dont les entreprises ont besoin pour détecter les menaces inconnues et les comportements anormaux des utilisateurs, points de terminaison et applications.
Splunk SOAR	Plateforme d'orchestration, d'automatisation et de réponse de sécurité (SOAR) qui s'intègre à vos technologies de sécurité existantes pour former une couche de « tissu conjonctif » qui les rend plus intelligentes, plus rapides et plus robustes.
Applications	Des applications développées par Splunk, nos partenaires et la communauté pour renforcer et élargir la puissance de la plateforme Splunk. L'application Splunk pour la conformité aux normes de l'industrie des cartes de paiement (PCI) en est un exemple. Disponible dans le cloud.
Splunk Security Essentials	Découvrez de nouveaux scénarios d'utilisation et déployez des détections de sécurité, aussi bien dans Splunk Security Essentials que dans Splunk Enterprise et Splunk Cloud et dans les offres SIEM et SOAR de Splunk. Aujourd'hui, c'est une application pleinement prise en charge avec une licence Splunk Cloud : commencez sans attendre à renforcer votre position de sécurité et accélérez la rentabilisation de votre investissement dans Splunk.
Mises à jour de contenu Splunk Enterprise Security	Destinées aux clients de Splunk Enterprise Security (ES), ces mises à jour fournissent des guides d'analyse de sécurité appelés « Scénarios analytiques » qui expliquent comment exploiter tout le potentiel de Splunk ES pour investiguer et agir face aux nouvelles menaces détectées dans l'environnement, quelles recherches mettre en œuvre et quels résultats vous pouvez attendre.

Scénarios de sécurité

Vous trouverez ensuite les scénarios de sécurité que nous avons répartis sur ce parcours. Lancez-vous. Choisissez votre aventure, votre défi de sécurité. L'objectif de ce manuel est de vous montrer comment la plateforme axée sur l'analyse de Splunk peut vous aider à relever vos défis de sécurité et à progresser dans votre parcours :

Appliquer les solutions Splunk aux scénarios de sécurité

Scénario d'utilisation	Solution Splunk
Investigation et analyse des incidents	Splunk Enterprise, Splunk Enterprise Security, Splunk SOAR
Supervision de sécurité	Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security, Splunk SOAR
Détection des menaces avancées	Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security, Splunk User Behavior Analytics
Automatisation du SOC	Splunk Enterprise, Splunk Enterprise Security, Splunk SOAR
Réponse aux incidents	Splunk Enterprise, Splunk Enterprise Security, Splunk SOAR
Conformité	Splunk Enterprise, Splunk Security Essentials App, PCI, Splunk Enterprise Security
Analyse et détection des fraudes	Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security
Détection des menaces internes	Splunk Enterprise, Splunk Security Essentials App, Splunk User Behavior Analytics

Définition des scénarios de sécurité

Enfin, nous proposons une petite présentation des scénarios d'utilisation afin que nous soyons tous sur la même longueur d'onde.

Investigation et analyse des incidents

Les incidents de sécurité ne préviennent pas, et ils peuvent passer inaperçus assez longtemps pour représenter une grave menace pour une entreprise. En général, lorsque les équipes de sécurité prennent connaissance d'un problème, il y a de fortes chances que le mal soit déjà fait. Splunk fournit aux équipes de sécurité une « source unique de vérité » pour toutes les données machine horodatées d'un environnement informatique. Elles ont ainsi les moyens de mener des investigations plus performantes et plus rapides, réduisant ainsi le risque que la menace reste indécelable pendant une période prolongée.

Supervision de sécurité

La supervision de sécurité vous permet d'analyser un flux continu d'instantanés en quasi-temps réel afin de détecter les menaces et les autres problèmes de sécurité potentiels. Les sources de données de supervision sont le réseau et les systèmes des points de terminaison, ainsi que les dispositifs cloud, les systèmes des datacenters et les applications. La plateforme Data-to-Everything Splunk permet aux équipes de sécurité de détecter et de hiérarchiser les menaces détectées dans les flux de données de ces sources.

Détection des menaces avancées

Une menace persistante avancée (MPA) est un ensemble de processus de piratage informatiques furtifs et continus, souvent orchestrés par une ou plusieurs personnes ciblant une entité spécifique. Les MPA visent habituellement des entreprises privées ou des états pour des motifs commerciaux ou politiques. Splunk Enterprise permet aux entreprises d'analyser et de corréler les données afin de détecter les menaces avancées. Splunk Enterprise Security et Splunk User Behavior Analytics enrichissent les capacités existantes pour appliquer la méthodologie de la kill chain, en utilisant l'analyse statistique, la détection des anomalies et des techniques de machine learning pour détecter les menaces inconnues et avancées.

Automatisation du SOC

Les équipes d'opérations de sécurité adoptent les solutions Splunk pour orchestrer et automatiser l'enrichissement des données et les actions de réponse, ainsi que pour gérer les incidents. Elles utilisent les solutions Splunk d'automatisation du SOC pour faire évoluer leurs opérations, accélérer la réponse et désamorcer les menaces et autres problèmes de sécurité. Les solutions Splunk aident également les équipes à opérationnaliser les pratiques de sécurité axée sur l'analyse et leur donnent les moyens de collaborer avec tous leurs partenaires dans l'entreprise.

Réponse aux incidents

La réponse aux incidents (IR) implique la supervision et la détection des événements de sécurité sur les systèmes IT, puis l'exécution de plans de réponse à ces événements. Les équipes d'IR sont parfois appelées « blue teams ». Les « blue teams » défendent l'infrastructure d'une entreprise lorsque des menaces sont détectées, tandis que les « red teams » tentent de découvrir les faiblesses dans la configuration actuelle de ces mêmes systèmes. Splunk propose différentes fonctionnalités d'IR dans son portefeuille de sécurité, selon l'offre choisie. Chacune fournit des mécanismes pour mener des investigations sur les événements détectés. Les solutions Splunk peuvent également comprendre des outils pour guider les collaborateurs chargés de la réponse aux incidents dans des procédures normalisées.

Conformité

Tous les environnements ou presque sont caractérisés par des exigences réglementaires prenant une forme ou une autre : RGPD, HIPAA, PCI, SOC et même les directives généralistes qui ne sont pas considérées comme de véritables critères de conformité, comme les 20 contrôles de sécurité critiques du CIS. Il existe de nombreuses manières de relever les défis de conformité avec les solutions Splunk. On peut par exemple créer des règles de corrélation et des rapports pour identifier les menaces pesant sur des données sensibles ou des collaborateurs clés, ainsi que pour automatiser la démonstration de la conformité.

Analyse et détection des fraudes

Les données machine jouent un rôle central et sont au cœur de la détection des activités frauduleuses à l'ère du numérique. Splunk peut assimiler de nouvelles données afin que les équipes de lutte contre la fraude soient armées pour mieux détecter et investiguer les anomalies. De cette manière, les entreprises sont en capacité de réduire leurs pertes financières, protéger leur réputation et préserver leur efficacité.

Détection des menaces internes

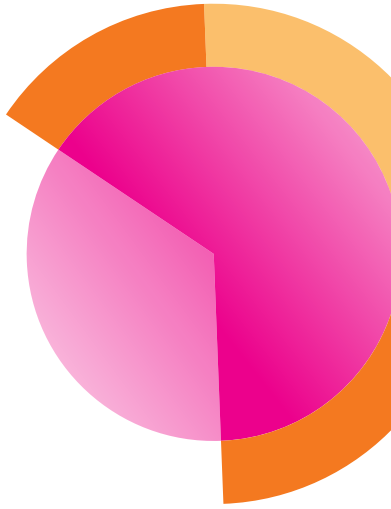
Les menaces internes proviennent de collaborateurs, sous-traitants ou partenaires actuels ou passés ayant accès au réseau de l'entreprise et qui, intentionnellement ou accidentellement, exfiltrent, détournent ou détruisent des données sensibles. Ils disposent souvent d'un accès légitime aux réseaux et ont l'autorisation de télécharger du contenu sensible en échappant facilement aux produits de sécurité traditionnels. Les solutions Splunk donnent aux équipes de sécurité la possibilité de détecter et de hiérarchiser les menaces posées par les adversaires internes et les collaborateurs compromis, menaces qui seraient autrement passées inaperçues.

Entreprendre votre parcours de sécurité axée sur l'analyse

Pour être efficace, un programme de cybersécurité doit évoluer continuellement. Malheureusement, peu d'entreprises savent exactement où elles en sont et comment faire mieux. Savoir où vous vous situez dans votre parcours vous aidera à gérer votre temps et vos ressources plus efficacement. Avec une meilleure connaissance des prochaines étapes, vous planifierez mieux la réussite des phases ultérieures.

Voici le découpage des six étapes du parcours de sécurité axée sur l'analyse qui exploite les données pour garder une longueur d'avance sur les attaques. À chaque étape, nous allons examiner les aspects suivants :

- l'applicabilité des scénarios d'utilisation ;
- les sources de données ;
- les étapes importantes ;
- les défis.



Étape 1 : **Collecte**

Collectez les journaux de sécurité de base et autres données machine de votre environnement.

Applicabilité des scénarios de sécurité

Investigation et analyse des incidents

Supervision de sécurité

Détection des menaces avancées

Automatisation du SOC

Réponse aux incidents

Conformité

Analyse et détection des fraudes

Menaces internes

Description

L'étape 1 se concentre sur l'obtention des matières premières nécessaires pour commencer à mieux comprendre l'environnement que vous devez défendre.

Sources de données
La bonne pratique de l'étape 1 consiste à collecter les données machine générées par les quatre composants fondamentaux de votre infrastructure de sécurité :

1. **Réseau.** Toute équipe de sécurité doit absolument avoir une visibilité sur le trafic réseau. À ce premier stade, la priorité consiste à identifier le trafic qui entre et qui sort de votre réseau. Il est crucial de voir aussi bien le trafic autorisé que les tentatives de communication qui ont été bloquées.

   Sources utilisées :
   - Logs de trafic des pare-feux de machines de fournisseurs comme :
     - Palo Alto Networks ;
     - Cisco ;
     - Checkpoint ;
     - Fortinet.

2. **Point de terminaison (par hôte).** Les logs des points de terminaison complètent la visibilité sur le réseau et donnent des informations sur les activités malveillantes : exécution de malware, activité non autorisée d'un utilisateur interne, présence d'un agresseur sur le réseau, etc. Il est important de capturer ces données sur les serveurs, les postes de travail et tous les systèmes d'exploitation.

   Sources utilisées :
   - logs d'événements Windows ;
   - logs des systèmes Linux ;
   - logs Auditd Linux ;
   - logs des systèmes MacOS.

3. **Authentification.** Les logs d'authentification peuvent vous indiquer quand et depuis où les utilisateurs accèdent aux systèmes et aux applications. Comme la plupart des attaques qui aboutissent implique notamment l'utilisation d'identifiants valides, ces données sont essentielles pour faire la différence entre une connexion légitime et une appropriation de compte.

   Sources utilisées :
   - Windows Active Directory ;
   - authentification locale ;
   - gestion des identités et des accès (IAM) cloud ;
   - logs auditd Linux ;
   - logs des systèmes MacOS.

4. **Activité web.** De nombreuses attaques commencent par la visite d'un site web malveillant ou se terminent par l'exfiltration de données précieuses vers un site contrôlé par le malfaiteur. Il est indispensable de pouvoir savoir qui accède à quels sites et quand pour mener des investigations.

Sources utilisées :
- Filtres de trafic de pare-feux de nouvelle génération (NGFW) ou logs de Proxy de fournisseurs comme :
  - Palo Alto Networks ;
  - Cisco ;
  - Checkpoint ;
  - Fortinet ;
  - Bluecoat ;
  - Websense.

Étapes importantes

Après avoir bien intégré les données de ces quatre catégories, vous devriez avoir franchi plusieurs étapes importantes :

- les journaux d'activité critiques se trouvent dans un autre système où ils ne pourront pas facilement être manipulés par un intrus ;
- les quatre catégories de données sont disponibles pour effectuer des investigations de base.

Défis

Recueillir les différentes sources de données peut être pénible, tout comme il peut être fastidieux de vérifier que les données sont correctement importées. Cette tâche est souvent mal exécutée : les informations capturées sont alors insuffisantes, ce qui entraîne des pertes de temps et empêche de réaliser des investigations complètes.

Étape 2 : **Normalisation**

Appliquez une taxonomie de sécurité standard et ajoutez des données d'actifs et d'identité.

Applicabilité des scénarios de sécurité

Investigation et analyse des incidents

Supervision de sécurité

Détection des menaces avancées

Automatisation du SOC

Réponse aux incidents

Conformité

Analyse et détection des fraudes

Menaces internes

Description

À l'étape 2, vous veillez à ce que vos données soient conformes à une taxonomie de sécurité standard. Cela signifie que les champs représentant des valeurs communes (adresse IP source, port, nom d'utilisateur, etc.) ont désormais les mêmes noms, quelle que soit la machine qui a créé l'événement. Cet investissement stratégique dans la normalisation des données vous permet :

- d'intégrer une plus grande sélection de mécanismes de détection, provenant de différents fournisseurs et de la communauté ;
- de commencer à mettre en œuvre un centre des opérations de sécurité (SOC) pour superviser les systèmes et les utilisateurs de votre réseau ;
- de commencer à faire évoluer les capacités de votre équipe de sécurité.

Même si vous ne prévoyez pas de mettre sur pied un SOC formel, ces données normalisées vont :

- faciliter la corrélation entre différentes sources ;
- normaliser les investigations ;
- améliorer l'efficacité des analystes.

Sources de données

À l'étape 2, vous devez recueillir des informations de référence sur :

- les actifs IT (systèmes, réseaux, appareils, applications) ;
- les identités des utilisateurs, provenant d'Active Directory, de LDAP et autres systèmes IAM/SSO.

Étapes importantes

Les étapes importantes de l'étape 2 :

- les données sont correctement mappées selon le Common Information Model (CIM) ;
- les performances de recherche sont considérablement améliorées par l'utilisation de modèles de données accélérés associés au CIM ;
- les informations sur les actifs et les utilisateurs sont corrélées aux événements de votre plateforme de logs de sécurité.

Défis

Bien que vous disposiez des données de détection de base interrogeables, vous ne possédez pas encore les informations ni l'éclairage nécessaires pour des détections de sécurité plus approfondies et une visibilité accrue sur les points de terminaison.

Étape 3 : **Expansion**

Collectez des sources de données haute-fidélité supplémentaires, comme des métadonnées sur l'activité des points de terminaison et le réseau pour faciliter la détection des attaques avancées.

Applicabilité des scénarios de sécurité

Investigation et analyse des incidents

Supervision de sécurité

Détection des menaces avancées

Automatisation du SOC

Réponse aux incidents

Conformité

Analyse et détection des fraudes

Menaces internes

Description

Les données DNS (système de noms de domaine) et les données de points de terminaison vont vous donner accès à un riche ensemble de capacités de détection, donnant aux chasseurs de menaces les moyens de découvrir et de traquer les adversaires présents sur le réseau.

Sources de données

Les sources de données incluent à ce stade :

1. **Réseau.** La plupart des chasseurs de menaces et des analystes en Threat Intelligence vous diront que s'ils ne devaient choisir qu'une seule source de données pour leurs analyses, ce seraient les données DNS.

   Sources utilisées :

   - données de transfert spécifiques aux protocoles provenant de sources comme Splunk Stream ou Bro ;
   - données sur les requêtes DNS provenant de logs de débogage ou de sources de données de transfert ;
   - activité DHCP.

2. **Points de terminaison.** Des données d'activité riches sur les points de terminaison, qui capturent la création de processus, les modifications de fichiers, les modifications de registre et les connexions réseau, entre autres, offrent un historique incroyablement clair des événements critiques se produisant sur un point de terminaison.

   Sources utilisées :

   - sysmon ;
   - Osquery ;
   - Carbon Black Defense.

Étapes importantes

En recueillant des sources de données haute-fidélité, vous aurez :

- établi les fondements nécessaires pour des détections avancées ;
- acquis la possibilité de reconnaître certains indicateurs courants de compromission.

Défis

Les données que vous collectez sur le réseau et les points de terminaison sont riches en informations, mais elles manquent de contexte et peuvent contenir des indicateurs de compromission connus des autres organisations mais qui passent inaperçus dans votre environnement.

Étape 4 : **Enrichissement**

Augmentez les données de sécurité à l'aide de sources d'informations pour mieux comprendre le contexte et l'impact d'un événement.

Applicabilité des scénarios de sécurité

Investigation et analyse des incidents

Supervision de sécurité

Détection des menaces avancées

Automatisation du SOC

Réponse aux incidents

Conformité

Analyse et détection des fraudes

Menaces internes

Description

En plus de collecter des données machine vitales, les équipes de sécurité hautement performantes enrichissent leurs données avec d'autres informations issues de sources internes et externes. Des connaissances contextuelles et exploratoires, provenant des flux de Threat Intelligence, de sources d'informations open source (OSINT) et d'informations internes, permettent à votre personnel de sécurité d'extraire une plus grande valeur des données collectées pour détecter les événements et les incidents de sécurité plus tôt.

Sources de données

Ses sources de données sont nombreuses :

- listes locales d'IP/URL bloquées ;
- fils open source d'informations sur les menaces ;
- fils commerciaux d'informations sur les menaces ;

Étapes importantes

En enrichissant les données avec des informations sur le contexte, le personnel de sécurité est en mesure de :

- comprendre l'urgence d'une alerte en fonction de la nature critique de l'actif concerné ;
- enrichir rapidement les alertes en les rapprochant de flux de Threat Intelligence, en les croisant avec d'autres systèmes et en procédant à la collecte de contexte supplémentaire.

Défis

Vous disposez d'importantes capacités de détection, mais votre équipe fonctionne de manière ad hoc ou ne prend pas en compte le contexte de ce qu'elle voit en le corrélant à des informations venant de l'extérieur. De plus, les requêtes ne sont pas suivies, les performances ne sont pas mesurées, la collaboration est ponctuelle et les enseignements ne sont ni conservés ni réutilisables pour référence future.

Étape 5 : **Automatisation et orchestration**

Mettez en place une capacité cohérente et reproductible d'opérations de sécurité.

Applicabilité des scénarios de sécurité

Investigation et analyse des incidents

Supervision de sécurité

Détection des menaces avancées

Automatisation du SOC

Réponse aux incidents

Conformité

Analyse et détection des fraudes

Menaces internes

Description

En exploitant une solution d'orchestration, d'automatisation et de réponse de sécurité (SOAR), les entreprises disposent de plusieurs moyens puissants pour réduire leurs risques. La mise en place de l'automatisation et de l'orchestration offre plusieurs grands avantages, dont la possibilité de renforcer vos défenses en intégrant vos outils de sécurité et sources de Threat Intelligence actuels, l'accélération de la réponse aux événements de sécurité, la simplification du processus d'investigation et la réduction des dommages provoqués par les menaces. Les organisations matures trient et hiérarchisent les alertes entrantes de façon automatique et en continu, permettant ainsi à leurs ressources humaines de se concentrer sur les problèmes critiques qui nécessitent leur attention. Elles bénéficient également d'une régularité et d'une répétabilité accrues grâce à l'exécution de procédures d'automatisation normalisées, par opposition à la mise en œuvre manuelle d'un plan de réponse.

Sources de données

Les sources de données de cette étape comprennent les événements haute-fidélité générés par des plateformes de données comme Splunk Enterprise. Les recherches de corrélation, les événements notables et autres événements haute-fidélité sont importés par un système d'automatisation et d'orchestration pour servir de base à des actions.

Étapes importantes

Les étapes importantes de l'étape 5 vous donnent de nouvelles capacités :

- suivre les incidents ;
- mesurer régulièrement l'efficacité des analystes ;
- agir selon des procédures prescrites ;
- automatiser des actions de réponse simples et les combiner pour produire des orchestrations plus sophistiquées.

Défis

Les équipes de sécurité travaillent dur sur la ligne de front : elles identifient, analysent et réduisent les menaces dans toute la mesure du possible. Pourtant, en dépit de leurs efforts, la liste des incidents de sécurité non traités s'allonge, car les investigations et les menaces connues prennent l'essentiel de leur temps. (La réalité est simple : il n'y a pas assez de professionnels qualifiés pour analyser le volume d'incidents que la plupart des entreprises reçoivent.)

Étape 6 : **Détection avancée**

Mettez en œuvre des mécanismes de détection sophistiqués en exploitant le machine learning.

Applicabilité des scénarios de sécurité

Investigation et analyse des incidents

Supervision de sécurité

Détection des menaces avancées

Automatisation du SOC

Réponse aux incidents

Conformité

Analyse et détection des fraudes

Menaces internes

Description

En mettant le machine learning, la science des données et les statistiques avancées au service de l'analyse des utilisateurs, des points de terminaison et des applications de votre environnement, vous vous donnez des armes pour détecter les adversaires, les menaces inconnues et les menaces internes, même lorsqu'ils ne laissent que de minces traces de leur activité.

Sources de données

Pourchasser les adversaires requiert de procéder à une collecte plus granulaire des données de vos points de terminaison. Des données d'activité riches sur les points de terminaison, qui capturent la création de processus, les modifications de fichiers, les modifications de registre et les connexions réseau, offrent un historique incroyablement clair des événements critiques se produisant sur un point de terminaison.

Quelques exemples de sources de données :

- Microsoft Sysmon ;
- Osquery ;
- Carbon Black Defense.

Étapes importantes

À l'étape 6, vous employez :

- les techniques les plus sophistiquées actuellement pour identifier les menaces inconnues ;
- de nouveaux mécanismes de détection lorsqu'ils deviennent disponibles, en exploitant l'expertise de votre équipe et les organisations de recherche externes.

Défis

À ce stade, vous devrez constamment améliorer votre organisation de sécurité et acquérir de nouvelles capacités. Votre équipe devra certainement effectuer de nouvelles recherches. Mais en suivant ce parcours jusqu'au bout et en développant vos capacités jusqu'à leur maturité, vous avez l'assurance d'être à la hauteur. Vous subirez toujours des attaques, mais vous vous serez doté des meilleures armes pour détecter et prévenir de nombreuses menaces courantes ou plus rares qui pèsent sur les entreprises modernes.

Relevez les défis de sécurité courants avec la Splunk Security Operations Suite

Le parcours de sécurité est semé d'embûches. Imaginez que vous ayez un manuel des difficultés que vous pourriez rencontrer, de sorte qu'en cas de problème, vous ayez sous la main les outils pour gérer la situation et rester opérationnel.

Ne vous en faites pas. Nous avons pensé à tout.

Nous présentons ici quelques exemples pour vous aider à relever 16 défis de sécurité courants (vous en trouverez d'autres encore dans l'application Splunk Security Essentials ou la démo en ligne de Splunk Security). Chaque exemple détaille le défi et fournit des informations sur les sources de données, les scénarios d'utilisation, les solutions Splunk, les difficultés de programmation, la mise en œuvre, le volume d'alertes, les faux-positifs connus et la meilleure approche de réponse.

Ces exemples sont les suivants :

- Investigation et analyse des incidents
  - Détectez les déplacements latéraux avec WMI
  - Identifiez les tentatives répétées d'accès non autorisé
- Supervision de sécurité
  - Détectez les buckets S3 publics dans AWS
  - Localisez des infections multiples sur un hôte
- Détection des menaces avancées
  - Détectez les connexions à un nouveau domaine
  - Retrouvez les e-mails provenant de domaines ressemblants
- Automatisation du SOC
  - Automatisez l'investigation des malware
  - Automatisez l'investigation des cas d'hameçonnage
- Réponse aux incidents
  - Détectez les alertes DLP d'exfiltration de données par utilisateur
  - Effectuez une détection basique des DNS dynamiques
- Conformité
  - Détectez la création d'un nouveau compte d'administration local
  - Retrouvez les utilisateurs connectés à un système protégé normalement hors d'accès
- Analyse et détection des fraudes
  - Détectez les comptes utilisateurs compromis
  - Identifiez les prestataires de santé anormaux
- Détection des menaces internes
  - Détectez les envois massifs de données sur le web
  - Détectez les connexions réussies au compte d'un ancien employé

Investigation et analyse des incidents

Détectez les déplacements latéraux avec WMI

ÉTAPE 3

Tactiques MITRE ATT&CK

Déplacement latéral **Exécution**

Techniques MITRE ATT&CK

Services distants **Instrumentation de la gestion Windows**

Sources de données

Sécurité Windows **Détection des points de terminaison et réponse**

Défi de sécurité
La WMI, ou instrumentation de la gestion de Windows, est devenue très populaire chez les pirates car elle peut réaliser des opérations de reconnaissance sur les systèmes, détecter les antivirus et les machines virtuelles, exécuter du code, se déplacer latéralement, conduire des activités persistantes et voler des données.

Scénario d'utilisation
Détection des menaces avancées

Catégorie
Déplacement latéral

Solutions Splunk requises
Simple Search Assistant

Difficulté du SPL
Basique

Méthode de mise en œuvre
Ce scénario d'utilisation nécessite l'installation de sysmon sur les points de terminaison que vous souhaitez superviser, et celle de l'extension sysmon sur vos forwarders et vos search heads.

Volume d'alertes
Bas

Faux positifs connus
Aucun faux positif connu

Prise en charge
Lorsque cette recherche se déclenche, vous devez lancer votre processus de réponse aux incidents et investiguer les actions menées par le processus.

Aide à la détection des déplacements latéraux avec WMI
Pour détecter les déplacements latéraux avec WMI, commençons par charger nos données sysmon EDR. Tout autre log des lancements de processus incluant la ligne de commande complète conviendra également. Nous recherchons les lancements de ligne de commande WMI (EventCode 1 indique un lancement de processus) puis nous appliquons un filtre pour détecter les chaînes de ligne de commande incluant nos champs suspects.

```
index=* sourcetype=XmlWinEventLog:Microsoft-Windows-sysmon/
Operational EventCode=1 Image=*wmic* CommandLine=*node*
CommandLine="*process call create*"
| table _time host Image CommandLine
```


Identifiez les tentatives répétées d'accès non autorisé

ÉTAPE 1

Tactiques MITRE ATT&CK

Accès des identifiants

Techniques MITRE ATT&CK

Force brute

Sources de données

Authentification Sécurité Windows

Défi de sécurité
La plupart des échecs de connexion sont dus à des erreurs de mot de passe. Toutefois, des échecs répétés de connexion à des systèmes sensibles dont l'accès n'est normalement pas autorisé peuvent être le signe d'une activité malveillante. Dans la plupart des organisations, il est rare qu'un utilisateur reçoive un message d'accès non autorisé, en-dehors des scénarios à faible risque comme les logs de proxy. Quand cela concerne des activités à plus haut risque, comme les connexions système, l'accès aux partages de fichiers, etc., ou quand cela se reproduit constamment pour un même utilisateur, il y a généralement matière à investigation.

Scénario d'utilisation
Menaces internes

Catégorie
Menaces internes

Solutions Splunk requises
Simple Search Assistant

Difficulté du SPL
Intermédiaire

Méthode de mise en œuvre
Vérifiez que vous assimilez les données du forwarder universel et que l'extension technologique Splunk est installée, et tout fonctionnera automatiquement.

Volume d'alertes
Bas

Faux positifs connus
Le scénario le plus probable, quand cette détection est un faux-positif, est un problème de configuration des accès de l'utilisateur. Par exemple, un groupe AD a été modifié la veille, et l'utilisateur a été accidentellement retiré du groupe de sécurité « dev_system_access ». En-dehors de ce cas, il n'existe pas de cas-type produisant un faux-positif.

Prise en charge
Lorsque cette alerte se déclenche :

1. déterminez si l'utilisateur a précédemment eu accès aux ressources désirées ;
2. recherchez les changements de poste récents ;
3. recherchez les modifications récentes des groupes AD.

Dans la plupart des entreprises, l'étape d'escalade suivante consisterait à contacter le responsable de la ressource et/ou le superviseur de l'utilisateur afin de déterminer si ce comportement est normal ou non. Recherchez les signes d'intention malveillante et les compromissions de compte potentielles.

Aide à l'identification des tentatives répétées d'accès non autorisé
Pour découvrir les tentatives répétées d'accès non autorisé à l'aide de données en direct, nous utilisons une recherche simple avec le langage de recherche ci-dessous. Ici, nous analysons les logs de sécurité Windows et nous recherchons spécifiquement le code d'état 0xC000015B, qui indique que l'utilisateur n'a pas reçu le type de connexion demandé. Nous cherchons les utilisateurs qui présentent de nombreux exemplaires de ce code chaque jour, signe potentiel d'une tentative d'accès à des ressources sensibles. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=* source=win*security user=* EventCode=*
action=failure Logon_Type=* Failure Reason Logon Type
Status=0xC000015B
```

Supervision de sécurité

Détectez les buckets S3 publics dans AWS

ÉTAPE 3

Sources de données

Suivi d'audit AWS

Défi de sécurité
Nous connaissons tous ce scénario. Les utilisateurs hébergent des fichiers dans un bucket AWS S3 pour les transférer rapidement mais oublient de les supprimer, ou utilisent des buckets S3 pour sauvegarder des données sensibles et se trompent dans la gestion des droits d'accès. Comme les buckets S3 mal configurés et publics exposent inutilement des données sensibles à un risque d'exploitation et sont une cause de faille courante, il est essentiel de détecter les buckets S3 existants et les nouveaux buckets définis comme « publics ».

Scénario d'utilisation
Supervision de sécurité
Détection des menaces avancées

Catégorie
Exfiltration de données, SaaS

Solutions Splunk requises
Splunk Security Essentials
Extension Splunk pour Amazon Web Services
Splunk Simple Search Assistant

Difficulté du SPL
Intermédiaire

Méthode de mise en œuvre
La recherche des buckets S3 publics est facilitée par des données normalisées et calquées sur le modèle de données unifié CIM (Common Information Model). L'extension Splunk pour Amazon Web Services apporte une visibilité sur les différents composants du service AWS, et notamment sur les événements du service CloudTrail et des buckets S3. En imaginant que vous utilisez l'extension AWS pour Splunk pour assimiler ces logs, cette recherche devrait fonctionner automatiquement et sans problème. Pendant l'implémentation, veillez à respecter la bonne pratique consistant à spécifier l'index de vos données.

Volume d'alertes
Très bas

Faux positifs connus
Cette recherche peut produire deux types d'alertes non désirées. Cela survient lorsque quelqu'un :

1. crée intentionnellement un bucket public ; dans ce cas, vous souhaiterez peut-être mettre sur liste blanche les employés du marketing qui font cela régulièrement, ou créer une politique pour la création d'un bucket public afin de pouvoir exclure les buckets publics délibérés des recherches ;
2. crée un bucket public temporairement avant de le passer en mode privé.

Prise en charge
Lorsque cette recherche se déclenche, vous devez lancer votre processus de réponse aux incidents et investiguer les actions menées par le processus.

Aide à la détection des déplacements latéraux avec WMI
Pour détecter les déplacements latéraux avec WMI, commençons par charger nos données sysmon EDR. Tout autre log des lancements de processus incluant la ligne de commande complète conviendra également. Nous recherchons les lancements de ligne de commande WMI (EventCode 1 indique un lancement de processus) puis nous appliquons un filtre pour détecter les chaînes de ligne de commande incluant nos champs suspects.

Prise en charge
Quand une alerte de bucket S3 public se déclenche, il faut se poser trois questions :

1. Le bucket S3 est-il toujours public ?
2. Les fichiers sont-ils publics ?
3. Que contient le bucket ?

La première question trouve facilement une réponse : il suffit de rechercher le nom du bucket et « PutBucketACL » dans les logs. Vous verrez toutes les modifications ACL qui sont survenues. La deuxième et la troisième questions sont plus délicates, et nécessitent que la journalisation des accès au serveur soit activée sur le bucket S3 (ce qui n'est pas le cas par défaut ni très pratique, donc ne comptez pas dessus).

Si vous administrez un environnement AWS d'entreprise, analysez en priorité les buckets S3 ouverts. Vous pourriez même souhaiter automatiser la correction à l'aide de fonctions AWS.

Aide à la détection des buckets S3 publics dans AWS
Pour rechercher les buckets S3 publics à l'aide de données en direct, nous utilisons une recherche simple avec le langage de recherche ci-dessous. La recherche en direct s'applique aux fichiers de log d'AWS CloudTrail, filtre les événements PutBucketAcl qui se sont produits lorsque les permissions du bucket ont été modifiées, et extrait ceux qui incluent AllUsers. La capture d'écran indique les résultats d'une recherche sur des données de démonstration.

```
index=* sourcetype=aws:cloudtrail AllUsers
eventName=PutBucketAcl
| spath output=userIdentityArn
path=userIdentity.arn
| spath output=bucketName
path="requestParameters.bucketName"
| spath output=aclControlList path="requestParameters.
AccessControlPolicy.AccessControlList"
| spath input=aclControlList output=grantee path=Grant{}
| mvexpand grantee
| spath input=grantee
| search "Grantee.URI"=*AllUsers
| table _time, Permission, Grantee.URI, bucketName,
userIdentityArn | sort - _time
```

Localisez des infections multiples sur un hôte

ÉTAPE 1

Tactiques MITRE ATT&CK

Accès initial | Exécution

Techniques MITRE ATT&CK

Compromission Drive-by | Hameçonnage par pièce jointe | Hameçonnage par lien | Exécution utilisateur

Sources de données

Antivirus | Anti-malware

Défi de sécurité
Les virus sont chose courante, mais une infection par plusieurs virus simultanément est plus inquiétants. Une telle activité peut être le signe d'un kit d'exploitation en train d'essayer plusieurs techniques pour optimiser ses chances de réussite, mais il peut également s'agir de virus sans lien les uns avec les autres. Les produits traditionnels anti-malware détectent efficacement les logiciels malveillants connus, mais échouent souvent face à des types de malware nouveaux ou modifiés. Comme les variantes de ces logiciels peuvent aménager une voie d'accès aux systèmes internes, permettre une présence malveillante persistante ou exfiltrer des données, vous devez immédiatement faire de l'inspection des hôtes infectés une priorité pour identifier tout ce qui aurait pu échapper à la détection.

Scénario d'utilisation
Supervision de sécurité

Catégorie
Point de terminaison compromis

Solutions Splunk requises
Splunk Security Essentials
Extension Common Information Model Splunk
Splunk Simple Search Assistant

Difficulté du SPL
Basique

Méthode de mise en œuvre
Détecter les hôtes qui présentent de multiples infections nécessite de recueillir les logs d'une solution antivirus. En ayant intégré les logs Symantec, par exemple, cette recherche devrait très bien fonctionner. Si vous êtes équipé d'un autre produit antivirus, vous pouvez facilement adapter les critères de recherche aux noms de champ et sourcetypes de votre produit, en particulier si vous utilisez une extension Splunk qui les mappe sur le Common Information Model (faites une recherche dans Splunkbase).

Volume d'alertes
Bas

Faux positifs connus
Aucun faux positif connu.

Prise en charge
Lorsqu'un hôte est touché par de multiples infections, votre plan de réponse doit être le même que dans tout autre incident impliquant un malware, mais l'urgence sera plus grande.

Aide à la localisation des infections multiples sur un hôte
Pour localiser les hôtes qui affichent des infections multiples sur une courte période à l'aide de données en direct, notre exemple utilise une recherche simple avec le langage de recherche ci-dessous. Nous commençons par importer notre groupe de données de base, Symantec Endpoint Protection Risks, sur les dernières 24 heures. S'il existe plusieurs façons de grouper les événements (et stats est sans doute la plus rapide), nous utilisons transaction car c'est la plus simple. Elle permet de grouper tous les événements en fonction du Computer_Name. On peut appliquer un dernier filtre pour isoler les cas où un minimum de trois événements ont duré au moins quelques minutes. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=* sourcetype=symantec:* earliest=-24h
| transaction maxpause=1h Computer_Name
| where eventcount >=3 AND duration>240
```

Détection des menaces avancées

Détectez les connexions à un nouveau domaine

ÉTAPE 2

Tactiques MITRE ATT&CK

Exfiltration **Commande et contrôle**

Techniques MITRE ATT&CK

Exfiltration sur un canal de commande et contrôle

Exfiltration sur un protocole alternatif

Protocole standard de la couche d'application

Sources de données

Proxy web **NGFW**

Défi de sécurité
Dans la plupart des entreprises, les domaines visités par les utilisateurs un jour donné sont extrêmement semblables à ceux qu'ils ont visité la veille. Mais que faire du petit pourcentage de domaines qui ont été consultés à partir de votre réseau aujourd'hui sans jamais l'avoir été auparavant ? Il y a nécessairement une part de trafic légitime à destination de quelques sites jusqu'ici inconnus sur le réseau, mais cette part sera très réduite par rapport à l'ensemble des domaines visités. Le reste de ces domaines inédits représente une menace potentielle.

Être informé de l'accès des utilisateurs à de nouveaux domaines est utile à de nombreux égards, mais c'est surtout essentiel pour détecter les cas où votre système se connecte à un domaine contrôlé par un adversaire et qui est utilisé comme centre de communications de commande et contrôle, ou qui exploite un serveur d'exfiltration de données ou de distribution de malware. Si vous pensez qu'un hôte est infecté, il peut être très intéressant de vérifier s'il a récemment contacté de nouveaux domaines.

Scénario d'utilisation
Détection des menaces avancées

Catégorie
Commande et contrôle, exfiltration de données

Solutions Splunk requises
Splunk Enterprise
Splunk Security Essentials
Splunk URL Toolbox
Splunk Simple Search Assistant

Difficulté du SPL
Intermédiaire

Méthode de mise en œuvre
Cette méthode de détection des anomalies détecte la première et la dernière heure d'un groupe de valeurs arbitraire (par exemple la première connexion par combinaison utilisateur + serveur, la première visualisation par combinaison dépôt de code + utilisateur, ou le premier ID d'événement Windows indiquant l'utilisation d'une clé USB par système). Dans le cadre d'une utilisation normale, vous regardez si la dernière valeur se situe dans les 24 dernières heures et vous générez une alerte si c'est le cas. C'est une fonctionnalité majeure de nombreux outils de science des données de sécurité disponibles sur le marché (mais pas de Splunk UBA), que vous pouvez facilement obtenir avec Splunk Enterprise.

La mise en œuvre de cette recherche est relativement évidente car elle attend des données conformes au modèle CIM. Commencez par assimiler vos données de proxy (ou autres données de visibilité sur la navigation web, comme stream:http ou Bro) et assurez-vous qu'elles contiennent un champ uri. La seule autre étape consiste à vérifier que vous avez bien installé l'application URL Toolbox, qui permet à Splunk de lire les noms de domaine. Pour appliquer cette recherche à un plus grand volume de données (ou augmenter sa fréquence d'exécution), nous recommandons d'exploiter les fonctions d'accélération.

Volume d'alertes
Très élevé

Faux positifs connus

Dans la plupart des entreprises, le pourcentage de nouveaux domaines est faible. Toutefois, s'il fallait envoyer toutes ces alertes aux analystes pour investigation, ils seraient rapidement submergés car la majorité de ces « alertes de nouveau domaine » sont déclenchées par un trafic légitime. Si cette recherche ne génère pas de faux positifs à proprement parler, la valeur des alertes « nouveau domaine » prises isolément est si faible qu'il faut les traiter différemment de la plupart des autres recherches de corrélation. Elles sont essentiellement exploitables en tant que données de contexte ou une fois corrélées à d'autres indicateurs.

Prise en charge

Ces événements de domaine sont généralement surtout utiles comme données de contexte pour un autre événement tel qu'un malware non nettoyé, un nouveau service ou des connexions inhabituelles. La façon la plus simple de procéder consiste à enregistrer les événements dans un index résumé, puis d'inclure cet index dans les données à interroger dans le cadre d'opérations d'investigation. Les clients Enterprise Security le feront facilement avec le framework de gestion des risques. Créer une action Adaptive Response basée sur un indicateur de risque lorsque vous enregistrez la recherche permettra d'ajuster le score de risque des actifs impliqués et de l'afficher dans le workbench d'investigation lorsque vous analyserez un actif. Pour être complet, afin d'analyser l'efficacité d'une alerte donnée, nous recommandons de rechercher les domaines concernés dans une source d'informations open source comme VirusTotal pi ThreatCrowd.

Aide à la détection des connexions à un nouveau domaine

Pour détecter les connexions à un nouveau domaine à l'aide de données en direct, nous utilisons une recherche simple avec le langage de recherche ci-dessous. Nous commençons par importer notre jeu de données proxy en utilisant les champs du modèle de données unifié CIM et en filtrant uniquement les événements qui contiennent une URI.

Nous utilisons ensuite URL Toolbox pour extraire le domaine de l'URL. Enfin, nous excluons les adresses IP de notre recherche à l'aide de la commande de filtrage regex. Cette étape est facultative mais nous avons constaté que le rapport signal-bruit pouvait être très mauvais lorsque l'on inclut les adresses IP, dans la mesure où certaines applications se connectent à de nombreuses IP d'instances éphémères d'AWS dans le cadre de leur fonctionnement normal. Enfin, nous utilisons la commande stats pour calculer la première et la dernière fois que cette combinaison de champs est apparue, et de déterminer si la première apparition de l'événement a eu lieu au cours de la dernière journée (afin de savoir si c'est une nouveauté). La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
tag=web url=*
| eval list="mozilla" | 'ut_parse_extended(url,list)'
| regex ut_domain!="^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$"
| stats earliest(_time) as earliest latest(_time) as
latest by ut_domain, sourcetype
| where earliest >= relative_time(now(), "-1d@d")
```

Retrouvez les e-mails provenant de domaines ressemblants

ÉTAPE 4

Tactiques MITRE ATT&CK

Accès initial

Techniques MITRE ATT&CK

Hameçonnage par lien

Sources de données

E-mail

Défi de sécurité
Les e-mails provenant de domaines ressemblants constituent une tactique courante d'hameçonnage. Certains pirates modifient des lettres faciles à confondre, envoyant par exemple à des employés de splunk.com des e-mails provenant de spiunk.com. Ils peuvent aussi utiliser un sous-domaine crédible (.help.com, .support, etc.). Le problème est qu'une personne est plus susceptible d'ouvrir un e-mail s'il semble avoir été envoyé par une source légitime. Dans le cas des e-mails avec usurpation d'identité, la différence est quasiment imperceptible.

Scénario d'utilisation
Détection des menaces avancées

Catégorie
Compromission des points de terminaison, SaaS

Solutions Splunk requises
Splunk Search Assistant
First Time Seen Assistant
Application URL Toolbox

Difficulté du SPL
Avancée

Méthode de mise en œuvre
La mise en œuvre de cette recherche est généralement assez simple. Si vous avez intégré des données conformes au CIM, elle devrait fonctionner directement. Il vaut toujours mieux préciser l'index et le sourcetype de vos données de messagerie, en particulier si vous avez plusieurs sources de logs d'e-mail, comme une ESA en périmètre et un environnement Exchange central. La recherche devrait fonctionner à merveille si vous avez installé l'application URL Toolbox et que vous avez le bon index, le bon sourcetype, et le champ src_user.

Volume d'alertes
Très bas

Faux positifs connus
Cette recherche parcourt les e-mails entrants pour détecter tous les domaines ressemblant à ceux qui sont habituellement consultés dans votre entreprise, et s'apparente à l'exécution de dnstwist sur un nom de domaine. Face à des e-mails provenant de noms de domaine très similaires mais différents de ceux observés au quotidien, la recherche peut générer des alertes qui sont des faux positifs On pourrait imaginer que l'entreprise plank.com, qui produit des planches en bois pour la construction de bateaux de pirates, envoie des e-mails à leur contact commercial chez splunk.com. Cela crée une distance de Levenshtein de deux (le « a » devient « u » et on ajoute la lettre « s »), ce qui génère une alerte. Pour réduire le nombre de fausses alertes, on peut filtrer les exemples connus de la recherche ou envoyer les résultats dans une détection de Première apparition pour éliminer automatiquement les exemples passés.

Prise en charge

Lorsque cette recherche renvoie des valeurs, initiez votre processus de réponse aux incidents et consignez l'heure de l'événement, l'émetteur, le destinataire, l'objet du message et les éventuelles pièces jointes. Contactez l'émetteur. Si le comportement est légitime, documentez que le domaine est autorisé en précisant qui l'autorise. Dans le cas contraire, les identifiants de l'utilisateur peuvent avoir été exploités par un tiers et une investigation supplémentaire s'impose.

Aide à la recherche des e-mails provenant de domaines ressemblants

Pour localiser les e-mails provenant de domaines ressemblants dans les données en direct, nous allons utiliser le Simple Research Assistant, l'application URL Toolbox et le langage de recherche ci-dessous. Nous commençons par récupérer les logs de messagerie contenant une adresse source, et nous effectuons une agrégation par adresse source. Nous extrayons ensuite le domaine et nous agrégeons par domaine à analyser. Nous filtrons également les domaines que nous possédons et qui nous envoient habituellement du courrier. Grâce à l'application gratuite URL Toolbox, nous extrayons les sous-domaines des domaines de premier niveau. Comme le champ que nous allons passer à l'algorithme de Levenshtein est domain_detected, nous ajoutons chaque sous-domaine au champ multivaleur domain_detected. URL Toolbox reçoit deux champs multivaleur et effectue une vérification croisée pour calculer le score de Levenshtein de chaque combinaison. Nous extrayons le score le plus faible de ce groupe. Enfin, nous appliquons un filtre pour récupérer les scores de Levenshtein inférieurs à trois. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=* sourcetype=cisco:esa* OR
sourcetype=ms:o365:*:messagetrace OR
sourcetype=MSExchange*:MessageTracking OR
tag=email src_user=*
| stats count by src_user
| rex field=src_user "\@(?.*)"
| stats sum(count) as count by domain_detected
| eval domain_detected=mvfilter(domain_detected!=
"mycompany.com" AND domain_detected!="company.com" AND
domain_detected!="mycompanylovestheenvironment.com")
| eval list="mozilla" | 'ut_parse_extended(domain_
detected, list)'
| foreach ut_subdomain_level* [eval orig_domain=domain_
detected, domain_detected=mvappend(domain_detected, '<>'
. "." . ut_tld)]
| fields orig_domain domain_detected ut_domain count
| eval word1=mvappend(domain_detected, ut_domain),
word2 = mvappend("mycompany.com", "company.com",
"mycompanylovestheenvironment.com")
| lookup ut_levenshtein_lookup word1 word2 | eval ut_
levenshtein= min(ut_levenshtein)
| where ut_levenshtein < 3
| fields - domain_detected ut_domain | rename orig_
domain as top_level_domain_in_incoming_email word1 as
domain_names_analyzed word2 as company_domains_used
count as num_occurrences ut_levenshtein as Levenshtein_
Similarity_Score
```

Automatisation du SOC

Automatisez l'investigation des malware

ÉTAPE 5

Sources de données

Authentification **Sécurité Windows**

Défi de sécurité
Lorsque le même malware apparaît sur plusieurs systèmes, il se peut que vous soyez à l'aube d'un incident majeur (on l'a souvent vu avec les vers, les ransomware et les grandes campagnes d'hameçonnage). Investiguer une alerte de malware et y répondre peut prendre 30 minutes, voire plus, à chaque alerte. En automatisant l'investigation et la réponse, Splunk SOAR confirme si le processus est malveillant et prend immédiatement des mesures pour bloquer le hash sur les points de terminaison infectés.

Scénario d'utilisation
Supervision de sécurité
Détection des menaces avancées
Automatisation du SOC

Catégorie
Compromission de points de terminaison, déplacement latéral

Solutions Splunk requises
Splunk SOAR

Difficulté du SPL
Sans objet

Méthode de mise en œuvre
Importez les événements de malware de vos sources de données dans votre plateforme SOAR. Menez des activités d'investigation, notamment en obtenant des informations sur les IP, les URL et les fichiers concernés pour prendre plus rapidement des décisions. Ces actions de collecte de contexte se prêtent idéalement à l'automatisation. En fonction de vos décisions, réalisez des actions d'isolement et/ou de correction, manuellement ou en suivant des procédures d'automatisation.

Volume d'alertes
Très bas

Faux positifs connus
Sans objet

Prise en charge
La procédure investigue et corrige les infections de malware sur le point de terminaison. En automatisant ces réponses, vous gagnez du temps à deux égards : vous n'avez pas besoin de répondre vous-même, et les actions nécessaires au blocage des points de terminaison infectés sont mises en œuvre plus rapidement. Vous allez commencer à automatiser les activités d'investigation et de détection propres à des cas d'usage précis : masquage de fichiers et de répertoire, créations de fichiers de base de données, exécution d'un fichier aux extensions multiples, processus à une seule lettre sur un point de terminaison, etc.

Aide à l'enrichissement contextuel des alertes

Automatisez l'investigation et la prise en charge de l'hameçonnage

ÉTAPE 5

Sources de données

Suivi d'audit **AWS**

Défi de sécurité
Les e-mails d'hameçonnage peuvent avoir de graves conséquences dans une entreprise s'ils ne sont pas détectés. L'exploration de chaque e-mail peut prendre un temps considérable, car l'analyse doit examiner le corps de l'e-mail et ses pièces jointes, et identifier tous les utilisateurs susceptibles de l'avoir reçu. En automatisant l'investigation, les analystes répondent bien plus rapidement à ces attaques.

Scénario d'utilisation
Supervision de sécurité
Détection des menaces avancées
Automatisation du SOC

Catégorie
Hameçonnage, tactiques adverses, compromission de compte

Solutions Splunk requises
Splunk SOAR

Difficulté du SPL
Sans objet

Méthode de mise en œuvre
Importez les e-mails suspects dans la plateforme SOAR. Menez des activités d'investigation, notamment en obtenant des informations sur les IP, les URL et les fichiers concernés pour prendre plus rapidement des décisions. Ces actions de collecte de contexte se prêtent idéalement à l'automatisation. En fonction de vos décisions, prenez des mesures pour supprimer tous les exemplaires de l'e-mail d'hameçonnage de votre système de messagerie à l'aide d'une procédure d'automatisation.

Volume d'alertes
Très bas

Faux positifs connus
Sans objet

Prise en charge
Mettre en œuvre et automatiser les bonnes investigations lors de l'élaboration d'une procédure peut vous permettre de limiter la part d'intervention humaine nécessaire pour accomplir des actions, car la réponse mise en œuvre par la procédure va contribuer à normaliser l'investigation des cas d'hameçonnage, accélérant ainsi la correction et l'application des mesures.

Automatisez l'investigation des cas d'hameçonnage

Réponse aux incidents

Détectez les nouvelles alertes DLP d'exfiltration de données par utilisateur

ÉTAPE 3

Tactiques MITRE ATT&CK

Exfiltration

Techniques MITRE ATT&CK

Exfiltration

Sources de données

DLP

Défi de sécurité
Quand un utilisateur qui ne génère habituellement pas d'alertes DLP d'exfiltration de données en produit tout à coup, il s'agit d'un événement plus grave qu'une alerte traditionnelle. Dans le cas de règles critiques ou d'utilisateurs hautement privilégiés, investiguez ces événements pour déterminer si des informations industrielles sensibles quittent l'entreprise.

Scénario d'utilisation
Menaces internes

Catégorie
Menaces internes

Solutions Splunk requises
Simple Search Assistant

Difficulté du SPL
Intermédiaire

Méthode de mise en œuvre
La mise en œuvre de cette règle est assez simple : il suffit en effet de pouvoir déterminer quelles alertes DLP représentent vraiment une exfiltration de données. Cette nomenclature ou configuration varie considérablement d'une entreprise à l'autre : vous devrez donc vous coordonner avec votre équipe DLP. En-dehors de cet aspect, si vous avez un champ user et un champ signature, la recherche fonctionnera.

Volume d'alertes
Élevé

Faux positifs connus
Il s'agit d'une recherche strictement comportementale, donc les « faux-positifs » se définissent un peu différemment. À chaque fois qu'elle se déclenche, elle reflètera avec exactitude la première occurrence sur la période de la recherche (ou, avec la fonctionnalité de cache de lookup, la première occurrence sur la période de construction de la lookup). S'il n'y a pas véritablement de « faux-positif » au sens traditionnel du terme, il y a en revanche un mauvais rapport signal-bruit.

Prise en charge
Comme il s'agit d'une alerte comportementale, vous ne devrez généralement pas l'utiliser de façon isolée, sauf si :

- la gravité de l'alerte ou le niveau de priorité de l'utilisateur sont tels qu'il faille impérativement l'examiner de façon isolée, ou
- votre DLP est ajusté si finement que les alertes sont rares.

Pour tous les autres cas, la plupart des alertes ne doivent être envisagées qu'en conjonction avec d'autres alertes, via un mécanisme d'agrégation du risque dans Splunk ES ou les modèles de menace dans Splunk UBA.

Aide à la détection des nouvelles alertes DLP d'exfiltration de données par utilisateur

Cet exemple utilise le Simple Search Assistant. Notre groupe de données est un jeu de données de base d'événements DLP. Dans cette analyse, nous filtrons les alertes d'exfiltration de données. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=* tag=dlp tag=incident
| stats earliest(_time) as earliest latest(_time) as latest
by user, signature
| where earliest >= relative_time(now(), "-1d@d")
```

Effectuez une détection basique des DNS dynamiques

ÉTAPE 1

Tactiques MITRE ATT&CK

Commande et contrôle | OPSEC adverse | Mise en place et maintenance de l'infrastructure

Techniques MITRE ATT&CK

DNS dynamiques | Protocole standard de la couche d'application

Sources de données

Proxy web | NGFW | DNS

Défi de sécurité

Les adversaires recherchent la flexibilité dans leurs mécanismes de commande et contrôle, et les DNS dynamiques peuvent leur offrir. S'il existe des usages légitimes pour les DNS dynamiques (beaucoup de professionnels de l'IT les utilisent pour accéder à des réseaux domestiques), cette pratique peut être très risquée si elle ne fait pas l'objet d'une supervision étroite. Heureusement, avec Splunk et une liste fournie par Malware Domains, la détection des DNS dynamiques dans votre environnement devient facile.

Scénario d'utilisation

Supervision de sécurité, détection des menaces avancées

Catégorie

Commande et contrôle

Solutions Splunk requises
Simple Search Assistant
URL Toolbox

Difficulté du SPL
Basique

Méthode de mise en œuvre
La première étape de mise en œuvre de cette détection est l'acquisition d'une liste de fournisseurs de dyndns. Une fois que vous avez téléchargé une liste, vous devez l'adapter au format de lookup de Splunk. Une fois le fichier en place, le reste devrait suivre facilement.

Volume d'alertes
Intermédiaire

Faux positifs connus
Les services de production qui utilisent les DNS dynamiques sont rares, mais ils existent. Ils vont générer un niveau modeste de faux-positifs, mais ils ne devraient jamais concerner des services stratégiques. La plupart du temps, c'est un utilisateur qui contacte le réseau de son domicile pour regarder son chien par la webcam. Autoriser, et donc filtrer ces utilisateurs, ou interdire ces activités est, en fin de compte, une décision politique.

Prise en charge
Lorsque cette alerte se déclenche, recherchez les scénarios acceptables les plus courants, en particulier celui d'utilisateurs accédant à leur réseau domestique. Si cela ne semble pas être le cas :

1. consultez les données du Flux Splunk ou de la capture de paquets pour déterminer le type des données envoyées ;
2. examinez le nom du DNS et l'IP dans une source d'informations open source pour voir s'il y a quoi que ce soit d'anormal (bien que ce soit souvent difficile dans ce scénario) ;
3. s'il s'agit d'un hôte critique, pensez à explorer la journalisation du point de terminaison via Microsoft sysmon ou autre mécanisme de réponse de point de terminaison afin d'identifier le processus qui établit ces connexions.

Aide à la détection basique des DNS dynamiques
Cet exemple emploie une recherche simple avec le langage de recherche ci-dessous pour détecter les communications sortantes vers des serveurs DNS dynamiques, à partir de données en direct. Nous commençons par récupérer le jeu de données des logs de proxy. Pour localiser les fournisseurs DNS dynamiques, nous séparons les sous-domaines du domaine enregistré à l'aide d'URL Toolbox. Nous pouvons ensuite utiliser notre lookup de domaines DDNS. Cela va ajouter un champ appelé « inlist » avec la valeur « true » à toutes les correspondances. Enfin, nous pourrons rechercher les enregistrements qui sont reconnus. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=* sourcetype=pan:threat OR (tag=web tag=proxy)
earliest=-20m@m earliest=-5m@m
| eval list="mozilla" | 'ut_parse_extended(url,list)'
| lookup dynamic_dns_lookup domain as ut_domain OUTPUT
inlist
| search inlist=true
| table _time ut_domain inlist bytes* uri
```

Conformité

Détectez les nouvelles alertes DLP d'exfiltration de données par utilisateur

ÉTAPE 1

Tactiques MITRE ATT&CK

Évitement des mécanismes de défense **Persistance**

Techniques MITRE ATT&CK

Comptes valides **Création de comptes**

Sources de données

Suivi d'audit **Sécurité Windows**

Défi de sécurité
Les comptes d'administration locaux sont utilisés par des techniciens légitimes mais ils sont aussi le Saint-Graal des agresseurs. Une fois qu'un agresseur se trouve sur le réseau, il va vraisemblablement chercher à obtenir des privilèges d'administration pour obtenir un accès discret et sans restriction aux comptes et actifs qui l'intéressent. Un moyen simple d'y parvenir consiste à compromettre un compte existant puis à en augmenter les permissions.

Scénario d'utilisation
Détection des menaces avancées, supervision de sécurité, conformité

Catégorie
Point de terminaison compromis

Solutions Splunk requises
Splunk Security Essentials
Splunk Enterprise

Difficulté du SPL
Intermédiaire

Méthode de mise en œuvre
Avant toute chose, vérifiez que vous recevez bien les logs de sécurité Windows et que vous avez implémenté le suivi des modifications de compte. Consultez la documentation de la source des données de sécurité Windows si vous avez besoin d'aide.

Une fois que vous recevez les logs, vous devriez pouvoir rechercher sourcetype="WinEventLog:Security" EventCode=4720 OU EventCode=4732 pour voir les événements de création ou de modification de compte. Enfin, vérifiez que le nom de votre groupe d'administration local soit bien « administrators » pour être sûr de rechercher des modifications dans le bon groupe.

Volume d'alertes
Intermédiaire

Faux positifs connus
La seule source réelle de faux positifs pour cette recherche serait les administrateurs du help desk, qui créent régulièrement des comptes d'administration locaux. Si c'est une pratique courante dans votre environnement, filtrez leurs messages de création de compte d'administration en excluant leurs noms d'utilisateur de la recherche de base. Si votre groupe d'administration locale n'inclut pas le terme « administrators », la recherche pourrait générer des faux négatifs.

Prise en charge
Lorsque cette recherche renvoie des valeurs, initiez votre processus de réponse aux incidents et consignez :

- le nom du nouveau compte ;
- la date et l'heure de la création ;
- les comptes utilisateur qui ont créé le compte ;
- le système qui a initié la requête ;
- toute autre information utile.

Contactez le propriétaire du système. Si l'événement correspond à un comportement légitime, documentez que le domaine est autorisé en précisant qui l'autorise. Dans le cas contraire, les identifiants de l'utilisateur peuvent avoir été exploités par un tiers et une investigation supplémentaire s'impose. En plus de l'investigation, ce peut être l'occasion de vérifier que les comptes d'administration légitimes ont véritablement besoin des permissions assignées et qu'ils sont bien protégés par des mots de passe longs et complexes.

Aide à la détection de la création d'un nouveau compte d'administration local

Cet exemple emploie une recherche simple avec le langage de recherche ci-dessous pour rechercher les comptes nouvellement créés et ayant reçu le statut d'administrateur local. Notre jeu de données est une collection de logs de sécurité Windows contenant les événements de création de compte ou de modification de l'appartenance à un groupe d'un compte. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=* source="winEventLog:Security" EventCode=4720 OR
(EventCode=4732 Administrators)
| transaction Security_ID maxspan=180m
| search EventCode=4720 (EventCode=4732 Administrators)
| table _time EventCode Account_Name Target_Account_Name
Message
```

Retrouvez les utilisateurs connectés à un système protégé normalement hors d'accès

ÉTAPE 4

Tactiques MITRE ATT&CK

Accès des identifiants | Acquisition de privilèges | Collecte

Techniques MITRE ATT&CK

Comptes valides | Données des dépôts d'information | Manipulation de comptes

Sources de données

Authentification | Sécurité Windows

Défi de sécurité

Selon le règlement général sur la protection des données (RGPD), les entreprises ont l'obligation de maintenir un suivi d'audit complet sur les accès autorisés des employés, des fournisseurs et/ou sous-traitants des données aux systèmes et applications qui traitent données à caractère personnel. Le RGPD donne aux citoyens de l'Union européenne et de l'Espace économique européen le droit de demander à une entreprise où sont stockées leurs données et quelles entités y ont accès.

Pour répondre à une telle demande, l'entreprise doit identifier quels employés, fournisseurs et sous-traitants des données ont accédé aux données personnelles en question, mais aussi identifier et déclarer quels autres services traitent régulièrement lesdites données. Si des données personnelles sont traitées pour le compte d'un responsable du traitement, il faudra également prouver que seuls des individus autorisés ont accédé aux données en question. Si une trace d'audit montre un accès non autorisé, il devra être documenté et signalé aux autorités de protection de la confidentialité des données.

Grâce au mappage des données, renforcé par des contrôles visant à détecter les violations, une entreprise peut savoir :

- quels employés, fournisseurs et sous-traitants des données ont accédé aux données,
- où les données peuvent être conservées,
- quels autres services traitent régulièrement les données.

Si vous traitez des données au bénéfice d'un responsable du traitement, cette recherche peut prouver que seuls les individus autorisés y ont accédé.

Scénario d'utilisation
Menaces internes, conformité

Catégorie
RGPD, analyse IAM, mouvements latéraux, opérations

Solutions Splunk requises
Splunk Enterprise

Difficulté du SPL
Basique

Méthode de mise en œuvre
Utilisez d'abord les résultats du mappage de données pour élaborer une lookup associant les systèmes à leur catégorie RGPD. Faites ensuite la même chose pour les utilisateurs. À ce stade, dès lors que vous avez incorporé des données conformes au modèle CIM, tout devrait bien se passer !

Volume d'alertes
Élevé

Faux positifs connus
Cette recherche déclenche une alerte lorsque quelqu'un accède aux données alors qu'il n'est pas sur la liste documentée. Le scénario de faux-positif le plus vraisemblable est lié à une liste d'utilisateurs autorisés obsolète.

Prise en charge
Cherchez des signes indiquant qu'il faut ajouter une personne à la documentation, mais demandez confirmation à votre délégué à la protection des données (DPD) ou à son équipe avant de faire des modifications. Pensez à automatiser la mise à jour de la liste des utilisateurs autorisés et à l'extraire de la source où votre DPO conserve l'enregistrement définitif des utilisateurs autorisés. Une autre option consiste à généraliser et à enrichir les informations en ajoutant les départements autorisés, et en adjoignant au nom d'utilisateur le nom de son département.

Aide à la localisation des utilisateurs connectés à un système protégé
Cet exemple emploie une recherche simple avec le langage de recherche ci-dessous pour détecter les utilisateurs non autorisés connectés à des systèmes protégés, à partir de données en direct. Le jeu de données est une collection de logs d'authentification Windows incluant les logs de sécurité Windows. Notre recherche examine l'hôte dans la lookup de catégorisation RGPD et filtre uniquement les hôtes concernés par le RGPD. Ensuite, on examine l'utilisateur dans la lookup de catégorisation RGPD et on recherche les utilisateurs sans catégorie RGPD ni autorisation sur les informations couvertes par le RGPD. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=* source=win*security user=* dest=* action=success
| bucket _time span=1d
| stats count by user, dest
| lookup gdpr_system_category.csv host as dest OUTPUT
category as dest_category | search dest_category=*
| lookup gdpr_user_category user OUTPUT category as
user_category
| makemv delim="|" dest_category | makemv delim="|"
user_category
| where isnull(user_category) OR user_category !=
dest_category
```

Analyse et détection des fraudes

Détectez les comptes utilisateurs compromis

ÉTAPE 1

Sources de données

Logs d'applications **Logs d'accès Web**

Défi de sécurité
Qu'il s'agisse d'un compte de banque, de carte de crédit, d'e-mail, de dossier médical ou autre, les fraudeurs peuvent en prendre le contrôle sans que vous le sachiez. Par des attaques d'hameçonnage, de logiciels-espions ou de malware, les pirates acquièrent des informations d'identification qui permettent d'accéder aux comptes. Ces prises de contrôle ont généralement pour but la fraude à la carte bancaire, l'usurpation d'autorisations et l'utilisation des souscriptions du compte.
En se faisant passer pour un client authentique, les fraudeurs peuvent modifier les informations du compte, faire des achats, retirer de l'argent et exploiter les informations volées pour accéder à d'autres comptes, voire à des données plus sensibles encore. Selon l'objectif recherché, un pirate peut laisser le compte parfaitement intact et l'utiliser en même temps que son propriétaire, à son insu.

Scénario d'utilisation
Analyse et détection des fraudes

Catégorie
Appropriation de compte, attaque par liste de mots de passe (bourrage d'identifiants)

Solutions Splunk requises
Splunk Enterprise

Difficulté du SPL
Moyenne à élevée

Méthode de mise en œuvre
Identifiez les données de compte utilisateur critiques et vérifiez que les champs sont correctement extraits. Il est également intéressant de mettre en œuvre des mesures de renforcement de la sécurité, par exemple en bloquant les authentifications malveillantes, en appliquant une authentification à deux facteurs ou un captcha sur toutes les authentifications, ou en utilisant le machine learning et la biométrie. Des améliorations bien pensées rendent vos mesures plus difficiles à contourner, et multiplier les obstacles contribue toujours à prévenir les accès non autorisés. Des outils comme la limitation du taux d'échec, le blocage des IP et le blocage des requêtes erronées peuvent également limiter la portée des attaques.

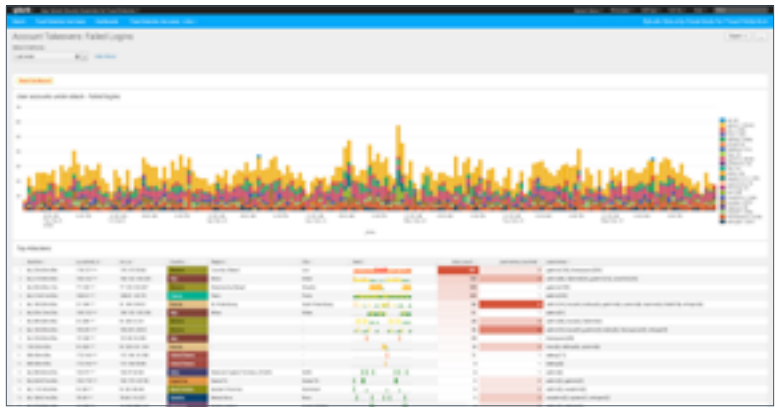
Volume d'alertes
Intermédiaire

Faux positifs connus
Aucun

Prise en charge
Il s'agit essentiellement de tentatives de détournement de comptes d'utilisateur par la force brute. Analysez les IP de l'attaque et le sous-réseau, et ajustez les règles de pare-feu en conséquence pour minimiser les risques de détournement de compte. Observez les pics sur la chronologie et investiguez les comptes qui sont l'objet d'un grand volume d'attaques.

Aide à la détection des comptes utilisateurs compromis
Utilisez les logs web pour visualiser le comportement d'un utilisateur ou d'une adresse IP, et les logs d'authentification pour déterminer quels comptes ont effectivement été compromis. Vous obtiendrez des informations utiles en examinant les taux d'échec élevés. D'autres logs peuvent aussi vous aider à déterminer si des modifications différentes (un changement d'adresse e-mail, par exemple) ont été apportées. Les données doivent contenir des informations sur les tentatives de connexion et indiquer si celles-ci ont abouti ou échoué. Le langage de recherche est fourni ci-dessous. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=web-logs action=login result=failure
| stats count, sparkline as trend by src_ip | where count>5
| sort - count
| table _time src_ip trend count
```



Détectez les transactions de santé anormales

ÉTAPE 1

Sources de données

Logs d'applications

Défi de sécurité
Dans le pays, plus de 400 personnes ont été poursuivies pour avoir participé à des fraudes au remboursement de médicaments sur ordonnance. Cette fraude peut avoir un impact sur les réglementations et la conformité, empêchant les prestataires de santé d'exercer leurs activités quotidiennes et les patients d'obtenir les prescriptions dont ils ont réellement besoin. Cette recherche identifie les anomalies dans les demandes de remboursement d'ordonnances de médicaments, à l'échelle du pays et de l'état.

Scénario d'utilisation
Analyse et détection des fraudes

Catégorie
Appropriation de compte

Solutions Splunk requises
Splunk Enterprise
Splunk Machine Learning Toolkit (MLTK)
Splunk Stream

Difficulté du SPL
Intermédiaire

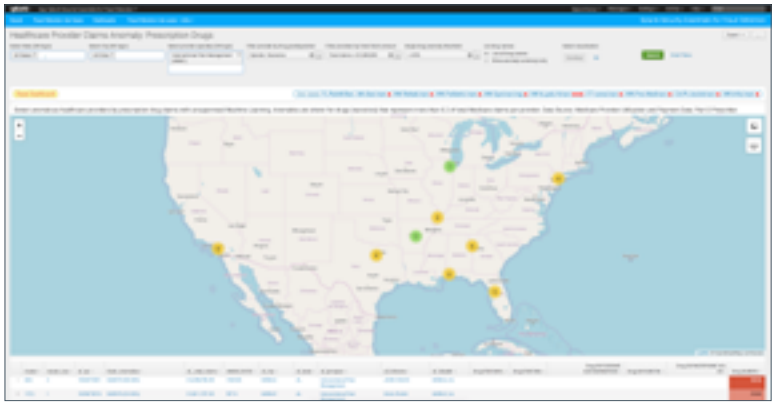
Méthode de mise en œuvre
Les jeux de données sont disponibles sur le site https://data.cms.gov/. Les données sont fournies au format CSV, ce qui facilite leur incorporation. Vous pouvez télécharger l'application pour visualiser le tableau de bord et explorer le SPL source. Notez toutefois que l'application est fournie avec le jeu de données CMS.

Volume d'alertes
Intermédiaire

Faux positifs connus
Les résultats sont présentés comme des anomalies et des valeurs extrêmes. Il n'existe pas d'indicateur permettant d'établir définitivement si les prestataires affichés sont frauduleux ou non. Toutefois, en faisant des recherches complémentaires, nous avons découvert que, dans de nombreux cas, les prestataires anormaux (notamment ceux qui prescrivent des opioïdes en grandes quantités) étaient impliqués dans des pratiques douteuses parfois des années après la publication des jeux de données.

Prise en charge
Cliquez sur le nom d'un prestataire pour ouvrir le tableau de bord d'analyse de profil détaillée. Cela vous permet d'analyser les données détaillées de la prescription et vérifier que le comportement du prestataire ne correspond pas au comportement de prescription de son groupe de pairs à l'aide du tableau « profil des prestataires nationaux / profil de ce prestataire ».

Aide à l'identification des prestataires de santé anormaux
Les anomalies sont présentées sur une carte. Cliquez sur le cercle jaune pour afficher les données résumées concernant une anomalie en particulier. Cliquez sur le nom d'un prestataire pour ouvrir le tableau de bord d'analyse de profil détaillées contenant des données spécifiques en lien avec le prestataire.



Détection des menaces internes

Détectez les envois massifs de données sur le web

ÉTAPE 1

Tactiques MITRE ATT&CK

Exfiltration

Techniques MITRE ATT&CK

Exfiltration sur un canal de commande et contrôle

Exfiltration sur un protocole alternatif

Sources de données

Proxy web **NGFW**

Défi de sécurité
L'exfiltration de données se produit généralement via des canaux standards de nos jours : les utilisateurs envoient les données vers Google, Dropbox, Box, de petits sites de partage de fichiers, voir des sites de dépôt non référencés. Comme HTTPS est toujours autorisé en sortie, l'exfiltration devient relativement facile dans la plupart des entreprises.

Scénario d'utilisation
Supervision de sécurité, menaces internes

Catégorie
Exfiltration des données

Solutions Splunk requises
Splunk Enterprise
Splunk UBA
Recherche simple Splunk

Difficulté du SPL
Basique

Méthode de mise en œuvre
Cette recherche doit fonctionner immédiatement dans n'importe quel environnement Palo Alto Networks, et s'adaptera facilement à toute autre source de visibilité sur proxy. On pense notamment aux proxys dédiés et outils de visibilité réseau tels que Splunk Stream ou Bro. Ajustez simplement le sourcetype et les champs en fonction.

Volume d'alertes
Intermédiaire

Faux positifs connus
Cette recherche se déclenchera dans de nombreuses situations innocentes (envoi de photos de vacances, par exemple). De nombreuses entreprises essaieront de filtrer ces alertes en se concentrant sur les utilisateurs qui figurent sur une liste de supervision, soit parce qu'ils ont accès à des données sensibles (cadres, data scientists, etc.), soit pour des raisons liées à leur emploi (plan de performance, préavis donné, fin de contrat, etc.). Ces listes de supervision peuvent être mises en œuvre à l'aide de lookups.

Prise en charge
Lorsque cette alerte se déclenche, il s'agit généralement d'envois légitimes (envoi de photos de vacances, par exemple). Face à cela, de nombreux analystes vont chercher à savoir où les données ont été envoyées, et si l'utilisateur a déjà envoyé des données sur ce site. Ils vont appeler l'utilisateur pour vérifier l'activité, de préférence en sachant quel est son statut dans l'entreprise. Par exemple, s'il suit un plan de performance ou a atteint la fin de son contrat, le risque d'exfiltration de données est plus grand. Si vous avez activé l'inspection SSL pour le site de destination via votre système NGFW ou DLP, vous pouvez parfois voir quels fichiers ont été transférés, ce qui peut fournir du contexte.

Aide à la détection des envois massifs de données sur le web
Cet exemple emploie une recherche simple avec le langage de recherche ci-dessous. La recherche en direct utilise un jeu de données de logs de proxy pour tout événement supérieur à 35 Mo. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=* sourcetype=pan:traffic OR (tag=web
tag=proxy) OR (sourcetype=opsec URL Filtering) OR
sourcetype=bluecoat:proxysg* OR sourcetype=websense*
earliest=-10m
| where bytes_out>35000000
| table _time src_ip user bytes* app uri
```

Détectez les connexions réussies au compte d'un ancien employé

ÉTAPE 4

Tactiques MITRE ATT&CK

Acquisition de privilèges | Accès des identifiants

Techniques MITRE ATT&CK

Comptes valides | Manipulation de comptes

Sources de données

Authentification | Sécurité Windows

Défi de sécurité
Les utilisateurs qui ont quitté votre entreprise ne devraient généralement pas se reconnecter. Cela peut signifier que leurs identifiants ont été compromis antérieurement ou qu'ils essaient de se connecter à des fins potentiellement inappropriées. Dans un cas comme dans l'autre, vous voulez détecter ces situations.

Scénario d'utilisation
Supervision de sécurité, menaces internes

Catégorie
Compromission de compte, menaces internes

Solutions Splunk requises
Splunk Simple Search Assistant

Difficulté du SPL
Basique

Méthode de mise en œuvre
Si vous avez suivi les guides d'intégration des données de l'application Splunk Security Essentials, la recherche fonctionnera immédiatement. Vous devrez généralement préciser l'index où vous stockez les logs de sécurité Windows (par exemple, index=oswinsec). Si vous utilisez un mécanisme autre que le forwarder universel Splunk pour intégrer ces données, vous devez vérifier le sourcetype et les champs utilisés.
Le reste est simple !

Volume d'alertes
Bas

Faux positifs connus
Si votre entreprise ne désactive pas ni ne supprime réellement les comptes, cette recherche peut être inexploitable. Si c'est le cas, pensez à installer des barrières autour de ce comportement en spécifiant sur quels systèmes on peut attendre une activité acceptable après la fin d'un contrat, par exemple dans l'environnement de messagerie. Mettez également en place un contrôle de détection pour veiller à ce que les mots de passe soient modifiés lorsqu'un employé devient inactif. Ensuite, essayez de limiter l'utilisation des comptes après le départ d'un employé.

Prise en charge
Lorsque cette alerte se déclenche, il faut avant tout déterminer s'il s'agit du prolongement du fonctionnement normal du système (le poste de travail est resté connecté ou le compte iPhone est encore actif, par exemple) ou d'une action délibérée. Naturellement, le succès ou l'échec de l'opération représente également un indice. Enfin, en particulier pour les administrateurs système dans les entreprises moins structurées, vérifiez qu'aucun service ni aucune tâche planifiée ne s'exécute avec ce compte, car la désactivation du compte aurait un impact immédiat sur les opérations.

Aide à la détection des connexions réussies au compte d'un ancien employé

Cet exemple emploie une recherche simple avec le langage de recherche ci-dessous pour détecter les activités d'authentification réussie sur les comptes d'anciens employés, à partir de données en direct. Notre jeu de données est une collection de logs d'authentification Windows présentant des connexions réussies. Une lookup indique le statut de l'utilisateur et nous permet de filtrer ceux qui ont expiré depuis au moins un jour ou qui sont désactivés. La capture d'écran ci-dessous indique les résultats d'une recherche sur des données de démonstration.

```
index=* (source=win*security OR sourcetype=linux_secure OR
tag=authentication) user=* user!="" action=success
| lookup user_account_status.csv user
| where _time > relative_time(terminationDate, "+1d")
```

En savoir **plus.**

Vous souhaitez approfondir vos connaissances pour améliorer votre position de sécurité avec l'approche axée sur l'analyse de Splunk ? Apprenez à relever plus de 300 défis de sécurité différents gratuitement en téléchargeant l'application Splunk Security Essentials sur Splunkbase. Travaillez ensuite avec les professionnels de sécurité et les partenaires de Splunk pour mettre en œuvre les scénarios d'utilisation dans votre environnement. Contactez-nous pour commencer dès aujourd'hui !

splunk>

21-13315-Splunk-Essential Guide to Security-EB-125