Top 5 des scénarios d'utilisation de Splunk

Security Analytics

splunk>

turn data into doing™

Les événements de sécurité sont difficiles à détecter et à prendre en charge rapidement. Un analyste de sécurité peut passer plusieurs minutes (parfois des heures) sur une alerte. Maintenant, multipliez cela par les centaines d'alertes de sécurité à gérer quotidiennement : vous comprenez qu'il y a bien trop de tickets et trop peu d'analystes. Vous entrevoyez le problème ?

Nous devons aider les équipes de sécurité à réduire leur temps de réponse de même que le nombre d'alertes qu'elles reçoivent. Nous pouvons commencer par leur donner une meilleure visibilité sur leur environnement pour qu'elles puissent détecter et prendre en charge les menaces plus rapidement. Mieux encore, une réponse automatisée au triage des alertes peut réduire les minutes en secondes et les heures en minutes. Ça fait rêver, non ?

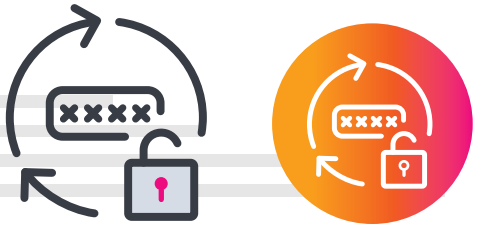
On limite ainsi le terrain pour les menaces trompeuses et difficiles à détecter comme les logiciels malveillants, ainsi que la quantité de dommages qu'elles peuvent causer, pour le bonheur de nos analystes de sécurité stressés.

Mais même si l'on veut faire le bonheur des analystes, la réalité du monde trépidant de la sécurité n'est pas toujours aussi simple, et les équipes de sécurité doivent encore déterminer le point de départ de leur parcours de sécurité. Et comme nous l'avons vu, même les meilleurs analystes risquent d'être débordés en sachant que n'importe quelle partie de leur organisation peut faire l'objet d'une intrusion et qu'ils doivent identifier les failles de sécurité à l'avance.

Heureusement pour eux, et pour les analystes de sécurité du monde entier, nous œuvrons depuis des années à la résolution de ce problème avec les clients de Splunk. Nous les avons aidés à résoudre leurs questions de sécurité les plus difficiles en libérant les réponses cachées dans leurs données.

Nous avons regroupé ces conversations dans ce guide pratique, qui regroupe des scénarios de sécurité et des conseils pour prendre un bon départ. Ce sont les problèmes de sécurité qui nous sont fréquemment présentés, accompagnés de bonnes pratiques de contenu et d'idées qui aideront les équipes de sécurité à être opérationnelles immédiatement au fil du déploiement et du perfectionnement de Splunk Enterprise Security (ES).

01



Identifiants compromis

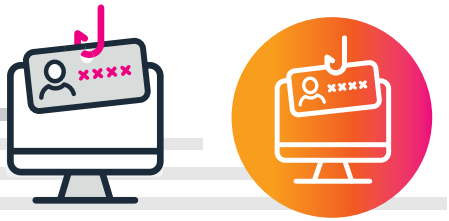
Qu'est-ce que la compromission d'identifiants utilisateur ?

La compromission d'identifiants d'utilisateurs consiste, pour un malfaiteur, à obtenir les identifiants d'un employé par le biais de méthodes éprouvées (hameçonnage ou compromission de la messagerie professionnelle). Une fois les malfaiteurs (et malfaitrices) entrés dans un environnement avec des identifiants valides, ils se mettent en quête de vulnérabilités pour atteindre leur objectif (et gâcher la journée d'un analyste de sécurité). Pire encore, puisque le pirate a réussi à se connecter avec des identifiants valides, il a l'apparence d'un utilisateur totalement légitime, ce qui en fait une menace difficile à détecter.

Comment Splunk fait face à la compromission des identifiants d'utilisateurs ?

Splunk Security Analytics (SSA) peut identifier les cas où les identifiants d'un utilisateur ont été compromis et sont utilisés par une entité autre que la personne ou l'application autorisée. SSA peut également fournir une couverture pour l'utilisation de comptes partagés et génériques. La modélisation comportementale de SSA avertit les analystes lorsqu'un utilisateur a une activité inhabituelle par rapport à la norme de comportement établie. La détection comprend l'identification d'activités Active Directory (AD) inhabituelles ou malveillantes : opérations sur soi-même, utilisateur résilié, comptes désactivés et récupération de compte.

02



Compromission d’utilisateur privilégié

Splunk UBA participe à évaluer la gravité du risque en s’appuyant sur un comportement normal de référence.

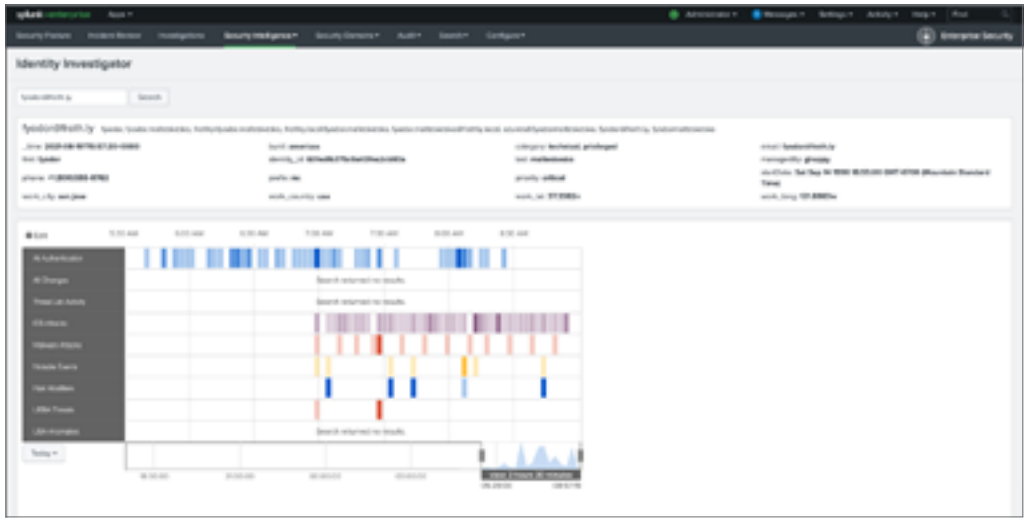
Qu’est-ce que la compromission d’utilisateur privilégié ?

La compromission d’utilisateur privilégié se produit lorsqu’un pirate accède à un compte privilégié par le biais de techniques d’ingénierie sociale ou d’exploits Zero Day. Dans ces attaques, les pirates ciblent généralement les utilisateurs hautement prioritaires disposant d’un accès administratif aux actifs sensibles ou d’une autorité décisionnelle. Les analystes en sécurité doivent donc pouvoir identifier immédiatement la compromission d’un compte privilégié. Concrètement, cette technique implique généralement de contourner les outils de sécurité traditionnels (pare-feux ou solutions de gestion des événements d’information de sécurité (SIEM) d’ancienne génération) qui sont conçus pour se défendre contre les menaces connues. Une fois que le pirate est entré, il cherche à obtenir davantage d’accès en collectant d’autres informations sensibles, comme des mots de passe ou des clés SSH.

Comment Splunk fait face à la compromission d’utilisateur privilégié ?

Splunk Security Analytics établit une référence du comportement de chaque compte et identifie les irrégularités par rapport à cette norme, car elles sont généralement le signe d’une utilisation excessive, d’un accès rare, d’un sabotage potentiel ou d’un effort pour brouiller les pistes. Si le comportement de l’utilisateur continue de différer du comportement de référence, la confiance de SSA augmente, ce qui se traduit par une hausse de la probabilité et de la gravité du risque. SSA va notamment détecter les accès à des connexions VPN ou interactives provenant de comptes de service, l’espionnage de données, la suppression de journaux d’audit et l’accès à des informations confidentielles.

03



Exemple de tableau de bord Splunk facilitant l'identification des menaces internes.

Menaces internes

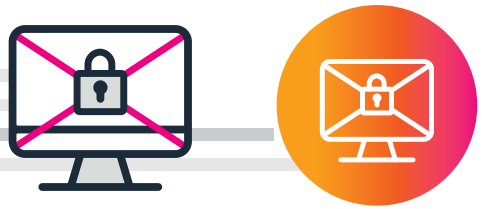
Qu'est-ce qu'une menace interne ?

Une menace interne pèse lorsqu'un employé ou un sous-traitant ayant accès à des informations confidentielles abuse intentionnellement (ou accidentellement) de son accès pour nuire à l'entreprise pour laquelle il travaille. Ce problème est tellement courant que les menaces internes représentent les deux tiers d'attaques ou de perte de données. Les compromissions d'identifiants, les compromissions d'utilisateur privilégié et les menaces internes correspondent toutes au même type de comportement : des informations d'identification valides sont exploitées pour des motifs néfastes.

Comment Splunk traite-t-il les menaces internes ?

Splunk Security Analytics capture l'empreinte de l'adversaire lorsqu'il se déplace dans les environnements d'entreprise, cloud et mobiles. Son activité est analysée par des algorithmes avancés de machine learning qui établissent une ligne de référence, détectent les déviations et repèrent des anomalies en quasi-temps réel. La totalité des actions du pirate dans l'environnement est intégrée dans une séquence descriptive qui utilise la détection de patterns et la corrélation avancée pour mettre au jour la kill chain et donner aux équipes de sécurité les moyens d'agir immédiatement.

04



Ransomware

Qu’est-ce qu’un ransomware ?

Le ransomware, ou rançongiciel, est un type de logiciel malveillant qui gagne malheureusement en popularité. Cette menace a même attiré l’attention du président américain Joe Biden. Pour mener ce type d’attaque, les pirates utilisent d’abord l’hameçonnage pour contraindre des utilisateurs à donner leur accès privilégié à leur insu. Ensuite, le logiciel malveillant entre en action et chiffre tout ou partie des fichiers de l’utilisateur. Les malfaiteurs demandent alors une rançon (d’où le nom de la technique) de dizaines de milliers (voire de millions) de dollars en cryptomonnaie, en échange du déverrouillage des fichiers.

Comment Splunk aborde-t-il les ransomwares ?

Splunk Security Analytics reçoit les mises à jour de Splunk ES Content Update (ESCU) ; celles-ci fournissent aux analystes de sécurité du contenu de sécurité pré-packagé qui les aide à lutter contre les menaces urgentes, les méthodes d’attaque et d’autres problèmes de sécurité. L’ESCU couvre actuellement 35 scénarios d’utilisation de ransomwares, et lorsque de nouvelles menaces sont repérées, l’équipe de Threat Intelligence de Splunk les analyse par rétro-ingénierie pour ajouter à l’ESCU les méthodes de détection correspondantes.

05

Sécurité cloud

Qu’est-ce que la sécurité cloud ?

La sécurité cloud est fondée sur le principe selon lequel la cybersécurité doit s’éloigner du périmètre et abandonner son approche centrée sur le réseau (à laquelle de nombreuses solutions de sécurité traditionnelles souscrivent encore). Pour cela, vous pouvez remercier le COVID et le passage au télétravail qui a impulsé notre migration collective vers le cloud.

Avec l’essor du cloud computing, et parce que de plus en plus d’entreprises migrent des aspects critiques de leur activité vers un cloud public comme Google Cloud Platform (GCP), Amazon Web Services (AWS) ou Microsoft Azure, il est essentiel que les entreprises puissent analyser facilement leurs données en temps réel et obtenir la visibilité nécessaire pour garder une longueur d’avance sur les pirates.

Comment Splunk renforce-t-il la couverture de sécurité du cloud ?

Splunk Security Analytics facilite l’intégration des informations sur les actifs et les identités (A&I) de GCP, d’AWS et d’Azure afin de renseigner les tables d’A&I Splunk de façon transparente. SSA fournit également des détections prêtes à l’emploi concernant l’authentification, le trafic réseau et les changements de configuration pour les trois grands fournisseurs de cloud. En associant les modèles de données de ces fournisseurs de cloud au modèle de données unifié de Splunk, les flux de travail de détection et d’investigation existants d’une entreprise intègrent naturellement la couverture indispensable des données cloud.

Prêt à sauter le pas

avec une solution SIEM orientée analyse basée dans le cloud ? Découvrez comment prendre un bon départ avec Splunk.

En savoir plus

21-20968-Splunk-Top 5 Use Cases for Splunk Security Analytics-LS-104