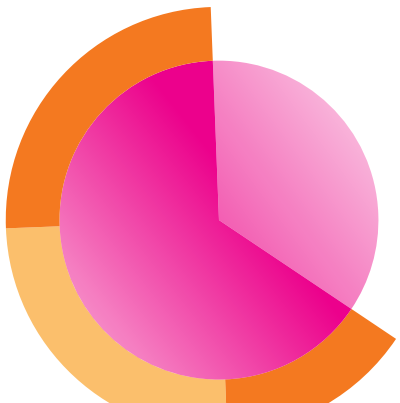
Le guide essentiel des **données de sécurité**

splunk>

Données chronologiques. Données de flux. L'avènement des données.

Nous savons tous qu'elles restent sous-exploitées et sous-estimées dans la plupart des entreprises du monde. Bien que les décisions axées sur les données fassent l'objet de discussions constantes, les entreprises de toutes tailles ne parviennent toujours pas à capturer et à exploiter efficacement les mines de données générées chaque jour, qu'elles proviennent des utilisateurs, de ressources professionnelles extérieures ou de leurs propres dispositifs réseau. Et pourtant, les cybercriminels se rendent compte que les données ont parfois plus de valeur que le pétrole et que, comme pour le pétrole, elles peuvent être raffinées et transformées en marchandises qui seront vendues au plus offrant. Les équipes de sécurité ne font pas seulement face à l'augmentation des données et à l'élargissement des périmètres au sein de l'organisation, elles doivent également gérer la multiplication des cyberattaques sophistiquées. Elles ont besoin de visibilité et d'informations contextuelles pour investiguer les incidents de sécurité qui surviennent dans leurs environnements sur site, hybrides et multicloud, et pour apporter une réponse efficace à ces derniers.

En effet, 73 % des organisations enrichissent leurs analyses de sécurité avec d'autres sources de données, grâce à des outils d'analyse. Des informations essentielles sur votre IT, votre sécurité et vos activités se cachent au cœur de ces données. Les données contiennent les archives complètes de toute l'activité et de tous les comportements de vos clients, utilisateurs, transactions, applications, serveurs, réseaux, dispositifs mobiles et autres. Des informations cruciales sur les configurations, les API, les files de message, les résultats des diagnostics, les données des capteurs industriels, etc. : tout est là, il suffit de savoir y puiser judicieusement.



Avec la bonne approche, les données permettent facilement de :

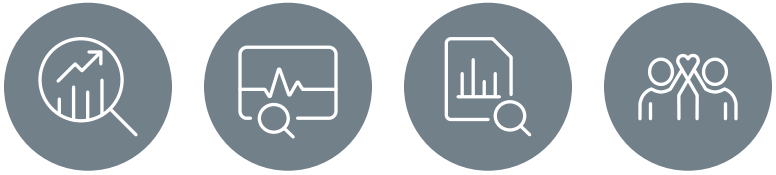
- prendre des décisions mieux informées sur tous les aspects de votre entreprise,
- administrer vos opérations plus efficacement,
- optimiser l'expérience des utilisateurs et des clients,
- détecter la fraude, voire l'empêcher totalement,
- mettre au jour des désastres potentiels avant qu'ils ne se produisent,
- détecter les tendances cachées qui aideront votre entreprise à prendre une longueur d'avance sur la concurrence,
- transformer tous les utilisateurs des données en héros,
- et bien plus encore.

Le défi de l'exploitation des grands volumes de données que recueillent la plupart des entreprises réside dans le fait qu'elles sont générées dans un incroyable éventail de formats, et que les outils traditionnels de supervision et d'analyse n'ont pas été conçus pour les gérer. Beaucoup d'outils sont incapables de gérer la variété des structures, des sources et des échelles temporelles des données. Et cela dépasse le simple cadre des données machine. Mais l'intérêt de puiser dans vos données est extraordinaire, et c'est là que Splunk® intervient.

Avec Splunk, vous pouvez compter sur vos données pour toutes les questions, décisions et actions de votre entreprise, afin de produire des résultats pertinents. Contrairement aux autres plateformes, Splunk est capable de prendre les données de n'importe quelle source et d'orienter des actions concrètes pour le bien de l'entreprise, de la supervision de l'infrastructure IT et de la sécurité au DevOps, en passant par la supervision et la gestion de la performance des applications.

Une plateforme de données pour un monde hybride

Utilisez les données pour :



Investiguer **Superviser** **Analyser** **Agir**

Les entreprises qui extraient le plus de valeur de leurs données sont celles qui parviennent à prendre des types de données disparates, à les enrichir et à en déduire des réponses. Mais ne sachant pas quelles données importer, les entreprises s'arrêtent avant même d'avoir commencé à en tirer le moindre bénéfice.

Familiarisez-vous avec les scénarios d'utilisation classiques de la sécurité, des opérations IT, de l'analyse commerciale, du DevOps, de l'Internet des objets (IoT), et plus encore, y compris avec les types et les sources de données concernés, pour prendre un bon départ.

Voici un exemple :

1. La commande d'un client n'a pas abouti.
2. Le client a appelé le support pour résoudre le problème.
3. Après une trop longue attente au téléphone, il abandonne et publie un tweet négatif sur l'entreprise.

À quoi ressemblent les données machine ?

Figure 1 : Les données peuvent provenir de sources variées et, au premier abord, ressemblent souvent à du texte indéchiffrable.

Les données machine contiennent des informations stratégiques

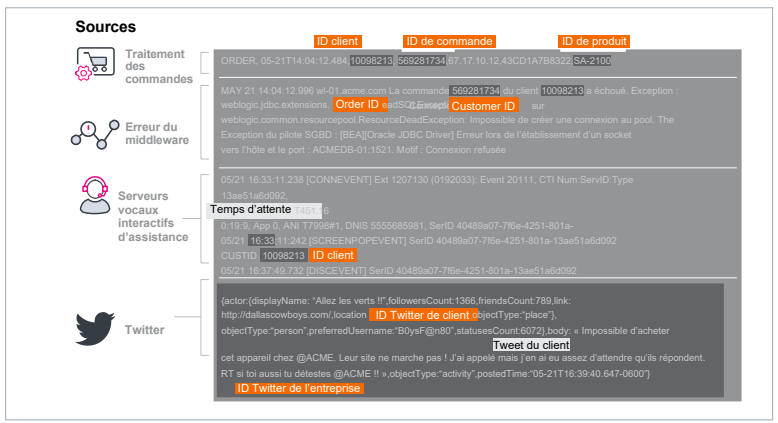


Figure 2 : La valeur des données machine se cache au cœur de ce texte apparemment aléatoire.

Les données machine contiennent des informations stratégiques

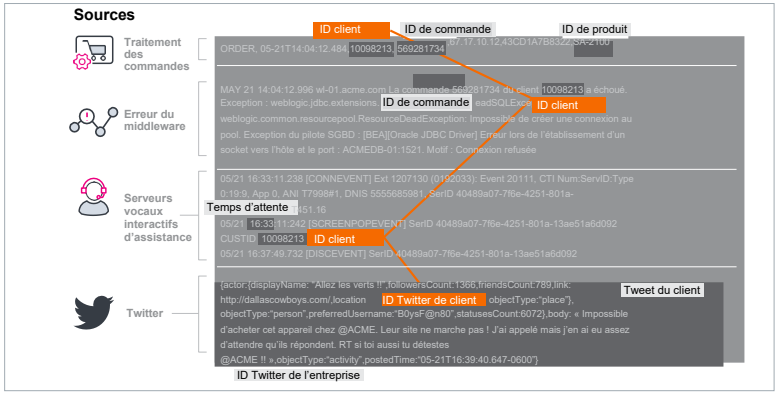


Figure 3 : En établissant des corrélations entre différents types de données, vous pouvez obtenir de précieuses informations sur ce qui se passe dans votre infrastructure, visualiser les menaces de sécurité et même utiliser ces informations pour prendre de meilleures décisions commerciales.

En prenant toutes les données impliquées dans le processus, autrement dit en extrayant les informations des systèmes de traitement des commandes, du middleware et de réponse vocale interactive, et celles de Twitter, une entreprise peut bénéficier d'une vue complète des problèmes de l'expérience client.

Données de sécurité

Les entreprises doivent utiliser toutes les ressources disponibles pour garder une longueur d'avance sur les cyberattaques en raison de la nature persistante des menaces avancées et de la facilité avec laquelle les programmes malveillants peuvent paralyser l'ensemble du réseau. Les analystes de sécurité sont submergés par la vitesse et le volume des alertes de sécurité. Ils ne peuvent pas traiter toutes les alertes tous les jours, et cela allonge les temps d'investigation et de réponse. On le sait également, les SOC manquent de personnel : la pénurie d'analystes de sécurité qualifiés est ressentie dans le monde entier.

Ces défis ne vont que croître avec l'ère numérique, marquée par la complexité de la migration du cloud et le passage de la 4G à la 5G. D'autant plus que le nombre d'appareils connectés approche les 80 milliards et que l'automatisation s'enracine progressivement dans notre vie.

S'il est une ressource essentielle, et souvent négligée, à la portée des entreprises pour résoudre ces problèmes de sécurité, ce sont les données. Les données sont partout et elles peuvent servir à garder une longueur d'avance sur les cybermenaces.

Les entreprises capables de tirer parti de la puissance de ces transformations et des données qu'elles créent seront plus efficaces, rentables, innovantes et, au final, mieux protégées.

Cet article explique comment trois entreprises exploitent leurs données pour se protéger contre les cybermenaces les plus récentes et, dans de nombreux cas, pour relever les défis liés aux opérations IT, à l'Internet des objets, au DevOps et à l'analyse commerciale.

Sécurité et conformité

Opérations IT, livraison des applications et DevOps

Sommaire

Transformer la position de sécurité d'Intel avec des innovations dans l'intelligence des données

Secteur d'activité

- Technologie

Scénarios d'utilisation Splunk

- Sécurité
- Gestion de la réponse aux incidents de cybersécurité
- Supervision de la sécurité
- Supervision des applications

Défis

- L'adoption d'un modèle commercial centré sur les données accroît la valeur des données mais aussi leur vulnérabilité
- Les SIEM traditionnels ne suffisent plus
- Des données et des équipes isolées et déconnectés interprètent différemment les analyses de données

Impact sur l'entreprise

- Transformation de la gestion et du contrôle de la sécurité des informations
- Menaces sophistiquées détectées en quelques minutes ou heures, et non plus en plusieurs jours ou semaines
- Création d'une approche collaborative et unifiée de la gestion de la cybersécurité
- Mise à disposition d'une plateforme de cyber-intelligence à l'ensemble de l'organisation InfoSec d'Intel

Produits Splunk

- Splunk Enterprise
- Splunk Enterprise Security
- Splunk IT Service Intelligence (ITSI)
- Splunk On-Call
- Splunk Mission Control

« Nous voyons le potentiel, et parce que nous le voyons, nous investissons du temps, de l'énergie et des ressources pour l'exploiter. Nous voulons que Splunk réussisse parce que nous sommes convaincus que cela nous aidera à remplir notre mission. »

— Brent Conran, Directeur de la sécurité des informations, Intel

Résumé

On peut difficilement surestimer l'impact et l'importance des contributions technologiques d'Intel sur la société. L'expertise technique de l'entreprise participe à sécuriser, alimenter et connecter des milliards d'appareils et l'infrastructure du monde intelligent et connecté. Il serait tout aussi difficile de surestimer l'importance des données sécurisées, qui constituent l'actif le mieux protégé d'une entreprise.

S'appuyant sur Splunk® et Apache Kafka, Intel IT a développé une nouvelle plateforme de cyber-intelligence qui transforme son approche de la sécurité de l'information :

- accélération de l'analyse des données et réduction du temps de détection et de réponse aux menaces avancées,
- émergence d'une organisation collaborative avec un langage et une surface de travail communs,
- mise en place d'outils de traitement des flux et de machine learning qui offrent une valeur métier dans d'autres domaines, comme les opérations de sécurité et l'état de santé du système.

Les données sont au cœur de tout

L'entreprise centrée sur le PC qu'était Intel fait aujourd'hui des données son cœur de métier. Elle développe de nouveaux produits, pénètre de nouveaux marchés et séduit de nouveaux clients par des approches innovantes.

Brent Conran, Directeur de la sécurité des informations d'Intel, affirme : « Les données sont la base de tout. Les données sont reines. Elles sont le moteur de notre activité, le moteur de tout. Elles transforment les industries traditionnelles autant que celles qui sont nées dans le cloud. La capacité à extraire des informations des données fait la différence entre l'entreprise qui réussit et celle qui échoue. »

En raison de cette importance et de cette dépendance accrues aux données, l'organisation Sécurité des informations (InfoSec) d'Intel devait mettre sur pied et maintenir une stratégie complète de « défense en profondeur ». L'équipe a automatisé les outils de prévention et de détection à de nombreux niveaux (périmètre, réseau, points de terminaison, applications et couche de données) pour traiter 99 % des menaces présentes dans l'environnement d'Intel.

À la recherche du dernier pourcent

Les menaces avancées continuent d'augmenter en fréquence et en sophistication. Et l'organisation était aux prises avec un SIEM qui ne répondait plus à ses besoins. Seule une poignée d'experts savaient utiliser cet ancien SIEM, qui ne pouvait pas s'adapter à la demande toujours croissante de diversification des types de données.

L'InfoSec d'Intel avait besoin d'une stratégie pour détecter les menaces sophistiquées qui tentaient de pénétrer dans l'environnement de l'entreprise, ce qu'elle appelle la recherche du dernier pourcent. C'est ce qui a inspiré la création de la Plateforme de cyber-intelligence (CIP) d'Intel, qui s'articule autour de technologies de pointe dont Splunk et Apache Kafka. Avec des serveurs hautes performances basés sur des processeurs Intel® Xeon® Platinum, des unités de stockage SSD NAND Intel 3D et Intel® Optane™, la nouvelle plateforme CIP enregistre plus de 12 téraoctets de données par jour et stocke 15 pétaoctets de données. Les données parviennent de centaines de sources vers un bus de messages Kafka, puis atteignent la plateforme Splunk, où les utilisateurs effectuent plus de 1,3 million de recherches par semaine.

Grâce à la plateforme Data-to- Everything™ de Splunk et des centaines d'outils tiers, l'équipe InfoSec d'Intel bénéficie désormais d'une visibilité richement contextualisée et d'une surface de travail commune qui améliore l'efficacité de toute son organisation. L'équipe peut désormais détecter et traiter les menaces en quelques heures ou minutes, alors qu'il lui fallait auparavant des heures, voire des semaines.

Agrandir la plateforme de cyber-intelligence (CIP) d'Intel

Les résultats de la CIP ont conduit à d'autres sources de données, à de nouveaux scénarios d'utilisation et à de nombreux autres modèles de données. Bientôt, l'utilisation de la CIP s'est étendue aux équipes de la gestion des vulnérabilités, de la conformité, de la gestion des risques et au-delà, ce qui a fait peser des exigences supplémentaires sur l'infrastructure tout en demandant des calculs et un stockage encore plus rapides. Pour optimiser les performances de la plateforme,

« Nous avons bâti la CIP pour gérer des dizaines, et bientôt des centaines, de téraoctets de données par jour et pour permettre à des centaines d'utilisateurs d'élaborer des recherches ad hoc, des recherches planifiées, des accélérations de modèles de données et des modèles de machine learning. Pour être performants à grande échelle, nous avions besoin de serveurs équipés des processeurs évolutifs Intel Xeon et de SSD Intel pour des performances élevées de calcul et de stockage. Chaque seconde compte quand votre mission est de "permettre à Intel d'aller vite en toute sécurité". »

— Jac Noel, Architecte de solutions de sécurité, Intel

l'architecte de solution et les ingénieurs de sécurité d'Intel avaient besoin de mieux comprendre la plateforme Splunk et les technologies Intel.

Une équipe commune de Splunk et d'Intel a développé une configuration de référence commune pour orienter l'expansion de la CIP en termes de puissance de calcul, de mémoire et de stockage à l'aide des derniers produits et technologies Intel. Splunk et Intel partagent désormais leur succès avec leurs confrères de l'IT, ce qui permet à d'autres d'élargir leurs déploiements Splunk et Apache Kafka pour convertir plus efficacement les données brutes en informations opérationnelles, métier et de sécurité.

Offrir de la valeur pour aujourd'hui et demain

L'équipe InfoSec d'Intel élargit son utilisation de Splunk et Kafka. Les analystes et les data scientists transforment, enrichissent, joignent, filtrent et exploitent les flux de données. L'équipe applique également de nouveaux outils de machine learning à la réponse aux incidents, aux opérations et à la supervision de la santé des systèmes, mais aussi à l'orchestration des workflows et aux alertes. En collaborant avec Splunk, Intel libère de la valeur pour aujourd'hui et demain.

M. Conran explique : « L'équipe de sécurité des informations d'Intel est bien plus agile que par le passé. Nous avons mis en place un tout nouveau lac de données Splunk et nous avons modernisé nos outils. En stockant les données aux bons endroits et en développant les compétences de nos collaborateurs, nous avons créé un véritable multiplicateur de force. Nous utilisons le machine learning pour accroître considérablement la profondeur et la vitesse de notre cyber-intelligence. »

NewYork-Presbyterian affronte la crise des opiacés avec Splunk

Secteur d'activité

- Santé

Scénarios d'utilisation Splunk

- Sécurité

Défis

- Il faut pouvoir suivre les données des dossiers médicaux électroniques, des plateformes d'ordonnances électroniques de substances contrôlées, des systèmes de distribution pharmacologique et d'autres sources afin de savoir si des médicaments sont détournés à des fins potentiellement illégales.
- Il est impossible de superviser l'accès aux PHI électroniques en temps réel, ce qui réduit la sécurité et la protection des dossiers médicaux.

Impact sur l'entreprise

- Protection contre le détournement des opiacés et des médicaments les plus chers, dont certains traitements anti-cancer qui peuvent coûter plusieurs dizaines de milliers de dollars par mois.
- Les opérations de sécurité IT sont supervisées pour garantir qu'aucune substance réglementée ni aucun médicament ne soient utilisés ni prescrits illégalement.
- Les institutions membres ont la possibilité d'appliquer les mêmes techniques de supervision et de lutte contre le détournement à leurs propres hôpitaux.

Sources de données

- Logs d'audit
- Données des applications
- EPIC
- Cerner
- Allscripts
- athenahealth

Produits Splunk

- Splunk Enterprise
- Splunk Enterprise Security (ES)

Résumé

Le NewYork-Presbyterian est l'un des systèmes de prestation de soins universitaires les plus complets et les plus intégrés du pays, et l'établissement s'engage à fournir des soins de la plus haute qualité avec compassion aux patients de la région métropolitaine de New York, au niveau national et dans le monde entier. Le NewYork-Presbyterian est régulièrement reconnu comme un leader dans la formation médicale, la recherche de pointe et les soins cliniques innovants centrés sur le patient.

En utilisant la puissance de la technologie Splunk, NewYork-Presbyterian a construit une plateforme pour protéger étroitement les substances contrôlées et d'autres médicaments, ce qui a finalement bénéficié à l'ensemble de la communauté de la santé. Grâce à Splunk, le NewYork-Presbyterian peut désormais :

- effectuer un audit de l'accès aux dossiers des patients et partager les données avec les utilisateurs autorisés afin de recueillir des informations,
- contribuer à réduire le détournement d'opiacés et d'autres substances contrôlées,
- se conformer à la loi HIPAA sur la portabilité et la traçabilité de l'assurance santé et à d'autres exigences de divulgation,
- assurer la confidentialité des données médicales protégées (PHI) et des patients

Protéger les données et la vie privée des patients

Au départ, NewYork-Presbyterian a choisi Splunk pour traiter différents scénarios de sécurité : prévention de l'hameçonnage, renforcement de la sécurité des comptes et automatisation des workflows de sécurité critiques. « Nous avons commencé à construire notre centre d'opérations de sécurité (SOC) quelques mois plus tard », explique Jennings Aske, vice-président senior et directeur de la sécurité des informations de NewYork-Presbyterian. « Aujourd'hui, nous avons une équipe de six personnes qui passent la journée à examiner des tableaux de bord et des visualisations intégrant toutes les sources de données utiles pour la sécurité », explique M. Aske.

Mais ce n'était que le début. « Au cours de la mise en place de notre SOC, nous nous sommes rendu compte que nous devions réfléchir aux problèmes métier liés à la confidentialité des patients. En particulier, nous voulions disposer d'une plateforme qui nous aide à vérifier que les utilisateurs ne commettaient pas d'indiscrétions, qu'ils ne regardaient pas trop de dossiers ou n'accédaient pas aux mauvais enregistrements », poursuit M. Aske. « Donc j'ai dit : "Allons parler à Splunk et voyons si nous pouvons bâtir une plateforme de confidentialité, pour nous et d'autres clients Splunk, qui s'intégrerait aux systèmes cliniques comme EPIC" ».

Ensemble, NewYork-Presbyterian et Splunk ont fait de cette vision une réalité, et créé une plateforme qui permet d'initier des investigations sans délai en avertissant les responsables de la protection de la vie privée si des dossiers médicaux sont consultés pour de mauvaises raisons. Mais l'hôpital s'est rapidement rendu compte que le potentiel de la plateforme allait bien au-delà de ce qu'ils avaient initialement prévu.

Lutter contre les opiacés à l'échelle mondiale

NewYork-Presbyterian a bientôt réalisé que les capacités de corrélation et de machine learning Splunk qui alimentaient la plateforme des patients pourraient également aider à identifier les détournements d'opiacés, un facteur essentiel dans l'épidémie de dépendance aux opiacés qui ravage les États-Unis.

« Quand on pense au rôle que jouent les hôpitaux dans la crise des opiacés, il faut savoir que nous avons des employés qui souffrent de taux de dépendance plus élevés que le grand public », explique M. Aske. « Nous savons d'après les statistiques des CDC qu'à certains moments, les hôpitaux ont été la source principale de la circulation de certains médicaments. Une année, environ 25 % de l'OxyContin en vente dans la rue provenaient d'hôpitaux. Nous avons l'obligation éthique et morale de ne pas nous contenter d'audits manuels, et de mettre sur pied une plateforme de détection des détournements potentiels. »

Pour remplir cette mission, la plateforme d'analyse des médicaments va permettre à NewYork-Presbyterian de suivre les données provenant des dossiers médicaux électriques (EHR), des plateformes de prescription électronique des substances réglementées (EPCS), des systèmes de distribution des pharmacies et d'autres sources. Les informations qu'elle va en tirer vont appuyer l'organisme dans la lutte contre le détournement de ces médicaments. La plateforme peut, par exemple, avertir immédiatement NewYork-Presbyterian si un médecin prescrit une substance réglementées à un patient qui n'est pas traité par l'hôpital, ou si un technicien en pharmacie utilise une armoire de distribution automatisée plus souvent que l'un de ses collègues.

« En fin de compte, nous avons pensé que d'autres institutions du pays pourraient facilement bénéficier de l'élaboration de cette plateforme avec Splunk. On peut affirmer que Splunk est utilisé par les 20 meilleurs hôpitaux selon le classement de *U.S. News*. C'est avec la force du nombre que ces plateformes pourraient jouer un rôle majeur dans l'amélioration du soin et de la santé publique. »

— Jennings Aske, vice-président senior et directeur de la sécurité informatique du NewYork-Presbyterian.

« Quand je pense à la plateforme d'analyse des médicaments, je me dis que dès que l'on sort de son cercle proche ou de celui de sa famille, on peut avoir des parents touchés par ce problème », rappelle M. Aske. « Je repense au jour où on m'a proposé des opiacés pour une chirurgie des gencives alors que je n'en avais pas besoin. J'ai une petite fille, et je veux être sûr que si on lui prescrit un jour des opiacés, ce sera pour une raison légitime et qu'ils ne sont pas détournés. »

Un avenir prometteur

Tout en continuant de fournir des soins empathiques dans le monde entier, NewYork-Presbyterian explore de nouvelles utilisations de Splunk dans le système hospitalier, notamment pour détecter plus rapidement les problèmes de codage d'assurance et mieux investiguer les refus opposés aux demandes de remboursement. « Splunk est une plateforme qui exploite et explore les données sous des angles qui ne sont pas nécessairement évidents », poursuit M. Aske. « En mobilisant Splunk pour davantage de questions, comme la facturation des assurances, nous pourrions potentiellement faire économiser des millions de dollars à l'hôpital. »

Grâce à la collaboration entre Splunk et le NewYork-Presbyterian, « les possibilités d'approche des données de l'hôpital sont quasiment illimitées », affirme M. Aske. « Nous avons l'intention de doubler notre utilisation de Splunk pour exploiter tout le potentiel de ce partenariat, non seulement pour nous, mais pour tous les organismes de santé du pays. »

Intégrer la threat intelligence aux procédures de sécurité

Pourquoi les clients de Recorded Future choisissent la plateforme Splunk

Secteur d'activité

- Technologie

Scénarios d'utilisation Splunk

- Sécurité
- Cybersécurité
- Orchestration, automatisation et réponse de sécurité
- Gestion de la réponse aux incidents
- Supervision de la sécurité
- Supervision des applications

Défis

- Clients contraints d'effectuer des opérations manuellement
- Refonte des processus pour certains clients

Impact sur l'entreprise

- Les clients peuvent identifier les menaces 10 % plus rapidement
- Les clients peuvent traiter les événements 63 % plus rapidement
- Une augmentation de 32 % de l'efficacité globale a été constatée

Produits Splunk

- Splunk SOAR
- Splunk Enterprise Security

« Sans recourir à l'automatisation et à l'orchestration, je ne vois pas comment les entreprises pourront faire face aux défis qu'elles rencontrent aujourd'hui. Avec tout ce qui se passe, elles sont submergées. Les humains ne peuvent pas s'en sortir seuls. »

— Seth Whitten, VP des intégrations et des partenariats stratégiques

Près de 40 000 professionnels de la sécurité répartis dans 22 secteurs et 6 continents s'appuient sur Recorded Future pour obtenir des informations détaillées sur les menaces. Recorded Future collecte et analyse de grandes quantités de données pour fournir des informations pertinentes sur les cybermenaces en temps réel. Ces informations permettent à leurs clients d'améliorer la détection et la réponse, ce qui aide leurs équipes de sécurité à prendre de meilleures décisions plus rapidement.

Rencontrez Seth Whitten, VP des intégrations et des partenariats stratégiques de Recorded Future. Nous avons pris un moment pour parler avec lui du partenariat entre Splunk et Recorded Future, et de l'impact de l'intégration de Splunk® SOAR. Il explique : « Notre plus vaste intégration aujourd'hui, c'est Splunk® Enterprise. Pour nous, c'était normal d'adopter SOAR. Nous avons beaucoup de clients qui extraient des événements de leurs outils SIEM et souhaitent pouvoir en faire un meilleur usage. »

Pourquoi SOAR

Avant SOAR, les clients de Recorded Future effectuaient leurs opérations à la main. « Ils devaient accéder à notre plateforme, extraire les informations qu'ils recherchaient et décider s'ils devaient agir ou non au cours de l'exploration d'une alerte ou du tri des événements dans leur environnement », explique M. Whitten.

Avec SOAR, les clients de Recorded Future peuvent automatiser ces opérations de sécurité manuelles et répétitives. Les alertes de sécurité qui prenaient plusieurs minutes ou des heures auparavant pour être résolues sont aujourd'hui traitées en quelques secondes grâce aux capacités d'automatisation du SOAR. Les clients de Recorded Future ont ainsi gagné en efficacité opérationnelle et considérablement réduit le temps de réponse aux événements de sécurité.

Pour M. Whitten, le point fort de SOAR réside dans la façon dont son équipe peut structurer les procédures. « SOAR nous facilite le travail sur le terrain parce que nous avons des procédures prédéfinies qui sont rapidement opérationnelles pour nos clients et nous évitent toutes les étapes de refonte des processus, » poursuit-il.

Recorded Future et SOAR

Les procédures SOAR automatisent une séquence d'actions de sécurité en un clin d'œil, ce qui permet aux clients de créer des workflows de sécurité personnalisés et reproductibles. Par exemple, une procédure SOAR peut demander à votre sandbox de déclencher un fichier ou indiquer à votre outil de sécurité de point de terminaison de mettre un appareil en quarantaine. Avec plus de 100 procédures prédéfinies et prêtes à l'emploi, SOAR permet aux clients de se munir d'un processus reproductible et vérifiable pour leurs opérations de sécurité.

« Nous utilisons le traitement du langage naturel et l'intelligence artificielle pour corréler les données et les mettre à disposition des clients pour résoudre les problèmes. »

— Seth Whitten, VP des intégrations et des partenariats stratégiques

« Nos clients veulent pouvoir passer en revue toutes leurs alertes. Ils veulent les hiérarchiser. Ils veulent agir. Ils veulent obtenir des résultats. SOAR était idéal pour accueillir nos données et les rendre exploitables afin d'obtenir des résultats. »

— Seth Whitten, VP des intégrations et des partenariats stratégiques

L'intégration à Recorded Future permet à ces procédures d'accéder aux données de threat intelligence. Lorsqu'une alerte est transmise à SOAR, soit en provenance de Splunk® Enterprise Security, soit en tant que nouvel artefact, une procédure est invoquée et automatiquement enrichie avec les scores de risque et le contexte associé de Recorded Future. La logique de décision de la procédure peut déterminer si l'alerte doit être transmise à un analyste humain si elle est risquée, ou ignorée si elle ne l'est pas. Comme SOAR aide à éliminer les faux positifs du flux, les analystes humains ont plus de temps pour se concentrer sur les problèmes importants.

Trois grands avantages

- Identification des menaces 10 % plus rapide
- Réponse aux événements 63 % plus rapide
- Augmentation de 32 % de l'efficacité globale

Données d'authentification

Scénario d'utilisation : Sécurité et conformité, Opérations IT, Livraison des applications

Exemples et sources de données : Active Directory, LDAP, gestion des identités, authentification unique

Les données d'authentification fournissent des informations sur l'activité des utilisateurs et des identités. Il existe plusieurs sources de données d'authentification courantes :

- **Active Directory :** répertoire distribué dans lequel les organisations définissent les identités des utilisateurs et des groupes, les stratégies de sécurité et les contrôles de contenu.
- **LDAP :** norme ouverte définie par l'IETF (Internet Engineering Task Force) et généralement utilisée pour l'authentification des utilisateurs (nom et mot de passe). LDAP dispose d'une structure de répertoire flexible qui peut être utilisée pour stocker un large éventail d'informations : nom complet, numéros de téléphone, adresses e-mail et physiques, unités organisationnelles, groupe de travail et nom du supérieur.
- **Gestion des identités :** la gestion des identités est la méthode qui permet de relier les utilisateurs de ressources numériques, qu'il s'agisse de personnes, de périphériques IoT, de systèmes ou d'applications, à un ID en ligne vérifiable.
- **Authentification unique (SSO) :** processus consistant à utiliser une gestion des identités fédérée de manière à ce qu'une source unique puisse fournir des identités vérifiables et certifiables à plusieurs systèmes. Le SSO renforce considérablement la sécurité en liant les informations d'identification de l'utilisateur à une source unique : grâce à cela, il suffit de modifier une fois les droits d'utilisateur et l'état du compte pour que cela s'applique à chaque application ou service auquel l'utilisateur a accès. Le SSO est particulièrement important dans le cas des utilisateurs disposant de droits de sécurité élevés, comme les administrateurs système ou réseau qui ont accès à un grand nombre de systèmes.

Scénario d'utilisation

Sécurité et conformité : en matière de sécurité, les données d'authentification fournissent une mine d'informations sur l'activité des utilisateurs : multiplicité de connexions inabouties ou réussies sur plusieurs hôtes dans une fenêtre de temps donnée, activités provenant de lieux différents sur une même période, tentatives par force brute. Plus précisément :

- Les logs du contrôleur de domaine Active Directory contiennent des informations sur les comptes utilisateur, notamment l'activité des comptes privilégiés, ainsi que des détails sur les accès distants, la création de nouveaux comptes et l'activité des comptes expirés.
- Les logs LDAP enregistrent qui se connectent à un système, à quel moment et depuis quel lieu, et de quelle manière les informations sont consultées.
- Les données de gestion des identités indiquent les droits d'accès par utilisateur, groupe et fonction (par exemple, PDG, superviseur ou utilisateur ordinaire). Ces données peuvent être utilisées pour identifier les anomalies d'accès qui pourraient traduire des menaces potentielles, comme un PDG accédant à un périphérique réseau de bas niveau ou un administrateur réseau se connectant au compte du PDG.

Opérations IT et livraison des applications : les données d'authentification aident les équipes des opérations IT à résoudre les problèmes liés à l'authentification. Par exemple, le support des applications peut être associé aux connexions pour permettre aux opérations IT de déterminer si les utilisateurs peinent à se connecter aux applications. Pour les équipes des opérations IT qui exploitent Active Directory, les logs peuvent être utilisés pour dépanner et comprendre l'état d'Active Directory.

DONNÉES DES UTILISATEURS

Antivirus

Scénarios d'utilisation : Sécurité et conformité

Exemples : Kaspersky, McAfee, Norton Security, F-Secure, Avira, Panda, Trend Micro

Les individus sont le maillon le plus faible de la sécurité de l'entreprise, et l'antivirus est l'un des moyens de les protéger contre les gestes nuisibles qu'ils accomplissent à leur insu. Qu'il s'agisse de cliquer sur un lien web peu fiable, de télécharger un logiciel malveillant ou d'ouvrir un document piégé (souvent envoyé par un collègue peu méfiant), l'antivirus peut souvent empêcher, atténuer ou annuler les dommages.

Les menaces persistantes avancées (APT) pénètrent souvent via une seule machine compromise connectée à un réseau de confiance. Bien qu'ils ne soient pas parfaits, les logiciels antivirus peuvent reconnaître et contrecarrer les méthodes d'attaque courantes avant qu'elles ne se propagent.

Scénario d'utilisation

Sécurité et conformité : les logs d'antivirus prennent en charge l'analyse des programmes malveillants et des vulnérabilités des hôtes, des ordinateurs portables et des serveurs, et ils peuvent être utilisés pour repérer les chemins de fichiers suspects. Ils peuvent aider à identifier :

- les fichiers binaires, hash de fichiers, fichiers du système de fichiers et registres récents,
- les binaires, les hash ou les registres qui correspondent à de la threat intelligence,
- les systèmes d'exploitation non corrigés,
- les signatures de programmes malveillants connues.

Serveur de messagerie

Scénario d'utilisation : Sécurité et conformité, Opérations IT

Exemples : Exchange, Office 365

L'e-mail reste la principale forme de communication formelle dans la plupart des organisations. Les bases de données et les logs du serveur de messagerie figurent donc parmi les enregistrements les plus importants de l'entreprise. En raison de leur taille et de leur tendance à se développer sans limites, la gestion des données de messagerie nécessite généralement des politiques de conservation et d'archivage des données, afin que seuls les enregistrements importants soient conservés et que les données inactives soient déplacées vers un stockage à faible coût.

Scénario d'utilisation

Sécurité et conformité : les données du serveur de messagerie peuvent aider à identifier les pièces jointes malveillantes, les liens et redirections de domaine malveillants, les e-mails provenant de domaines malveillants connus et de domaines inconnus. Elles peuvent également être utilisées pour identifier les e-mails dont la taille est anormale ou excessive, ainsi que les heures d'activité anormales de messagerie.

Opérations IT : les e-mails et les logs d'activité peuvent être nécessaires pour assurer la conformité aux processus de sécurité et de conservation des informations ainsi qu'aux obligations réglementaires de l'entreprise. Les logs de transactions et d'erreurs du serveur de messagerie sont également des outils de débogage indispensables pour la résolution des problèmes IT et peuvent également être utilisés pour la facturation basée sur l'utilisation.

Détecteurs de vulnérabilités

Scénario d'utilisation : Sécurité et conformité

Exemples : ncircle IP360, Nessus

Une façon efficace de détecter des failles de sécurité consiste à examiner l'infrastructure du point de vue de l'adversaire. Les analyses de vulnérabilité permettent de rechercher, dans le réseau d'une entreprise, les défauts logiciels connus qui fournissent des points d'entrée pour les agents externes. Ces analyses fournissent des données sur les ports ouverts et les adresses IP qui peuvent être utilisées par des agents malveillants pour accéder à un système particulier ou à l'ensemble du réseau.

Par défaut, les systèmes maintiennent souvent les services réseau en fonctionnement, même lorsqu'ils ne sont pas requis pour un serveur particulier. Ces services non supervisés et constamment en cours d'exécution constituent un biais courant d'attaque externe, car ils ne bénéficient pas toujours des correctifs des dernières mises à jour du système d'exploitation. Les analyses de vulnérabilité à grande échelle peuvent révéler des failles de sécurité susceptibles d'être exploitées pour accéder à l'ensemble du réseau de l'entreprise.

Scénario d'utilisation

Sécurité et conformité : ces analyses de vulnérabilité fournissent des données sur les ports ouverts et les adresses IP qui peuvent être utilisées par des agents malveillants pour accéder à un système particulier ou à l'ensemble du réseau. Ces données peuvent être utilisées pour identifier :

- un défaut de configuration du système à l'origine d'une vulnérabilité de sécurité,
- des correctifs obsolètes,
- des ports de service réseau inutiles,
- les systèmes de fichiers, utilisateurs ou applications mal configurés,
- les modifications de configuration du système,
- les modifications des autorisations des utilisateurs, des applications ou des systèmes de fichiers,

DONNÉES DES APPLICATIONS

Serveur web

Scénario d'utilisation : Sécurité et conformité, Opérations IT, Livraison des applications

Exemples : Java J2EE, Apache, logs d'utilisation des applications, logs IIS, nginx

Le serveur web est l'application de back-end qui sous-tend chaque site web et délivre tout le contenu affiché dans le navigateur. Les serveurs web accèdent à des pages HTML statiques et exécutent des scripts d'application dans une variété de langages qui génèrent du contenu dynamique et appellent d'autres applications, notamment middleware.

On recense d'innombrables types de serveurs web :

- **Java – J2EE :** Java est le langage de programmation le plus populaire en raison de sa polyvalence, de sa relative facilité d'utilisation et de son riche écosystème d'outils de développement. Via la plateforme J2EE, qui inclut des API, des protocoles, des SDK et des modules d'objets, Java est largement utilisé pour les applications d'entreprise, et en particulier les applets web, la logique métier de couche intermédiaire et le front-end graphique. Java est également utilisé pour les applications mobiles Android natives.
- **Apache :** Apache est l'un des serveurs web les plus anciens et les plus utilisés sur Internet, et il fait fonctionner des millions de sites d'entreprise, gouvernementaux et publics. Apache conserve des enregistrements détaillés de chaque transaction : chaque fois qu'un navigateur demande une page web, les détails du log Apache incluent des éléments tels que l'heure, l'adresse IP distante, le type de navigateur et la page demandée. Apache consigne également diverses conditions d'erreur : demande de fichier manquant, tentatives d'accès à un fichier sans autorisations appropriées, problèmes avec un plug-in Apache, etc. Les logs Apache sont essentiels au débogage des problèmes des applications et des serveurs web, mais ils sont également utilisés pour produire des statistiques de trafic, suivre le comportement des utilisateurs et signaler les attaques de sécurité telles que les tentatives d'entrée non autorisée ou les attaques DDoS.
- **Logs d'utilisation des applications :** tout comme les logs web Apache, la collecte de données sur l'utilisation des applications peut fournir des informations précieuses à de multiples parties prenantes, notamment les développeurs, l'IT, les ventes et le marketing. En fonction de la granularité des mesures, le suivi de l'utilisation peut aider les développeurs à identifier les fonctionnalités d'application les plus utilisées, celles qui ne le sont que rarement, celles qui posent problèmes aux utilisateurs, ainsi que les domaines à améliorer ultérieurement. Pour les applications orientées client, les logs d'utilisation fournissent aux équipes commerciales et marketing un aperçu de l'efficacité des canaux de vente et des promotions en ligne et dans les applications, des informations sur les ventes et les abandons de transaction, et des informations sur les promotions croisées potentielles.

Scénario d'utilisation

Sécurité et conformité : les logs web enregistrent les erreurs telles que les demandes d'accès à un fichier sans autorisation et suivent également les activités utilisateur qui peuvent signaler des attaques de sécurité telles que des tentatives d'entrée non autorisée ou des attaques DDoS. Ils peuvent également aider à identifier les injections SQL et appuyer la corrélation des transactions frauduleuses.

- Comme les applications Java accèdent fréquemment aux services réseau et aux bases de données sensibles, les équipes de sécurité peuvent utiliser les données de log pour vérifier l'intégrité des applications J2EE, identifier les comportements suspects et les vulnérabilités des applications.
- Les logs web Apache peuvent alerter en cas d'attaque de sécurité telle qu'une tentative d'entrée non autorisée, un XSS, un dépassement de mémoire tampon ou une attaque DDoS.
- Tout comme les logs web, les logs génériques d'utilisation des applications peuvent alerter les équipes de sécurité des accès non autorisés, par exemple lorsqu'une personne consomme plus de ressources que la normale ou utilise des applications à des heures inhabituelles.

Opérations IT et livraison des applications : les logs web sont essentiels au débogage des problèmes des applications et des serveurs web, mais ils sont également utilisés pour générer des statistiques de trafic utiles à la planification des capacités. Les données des serveurs web peuvent fournir diverses informations aux équipes des opérations IT :

- les données de J2EE peuvent aider les équipes des opérations à diagnostiquer les problèmes liés aux applications à trois niveaux qui impliquent l'interaction entre le web, le middleware et les serveurs de base de données,
- sous forme agrégée, les logs web Apache peuvent témoigner de l'activité d'un service web. L'analyse des détails peut révéler les goulots d'étranglement de l'infrastructure et indiquer des problèmes en aval,
- les logs d'utilisation des applications peuvent aider les équipes des opérations IT à planifier, optimiser, équilibrer et facturer les ressources en fournissant des enregistrements détaillés de la consommation.

DONNÉES MIDDLEWARE

Pare-feu

Scénario d'utilisation : Sécurité et conformité, Opérations IT

Exemples : Palo Alto, Cisco, Check Point

Les pare-feux délimitent les zones d'application de différentes politiques de sécurité. En contrôlant le flux du trafic réseau, les pare-feux agissent comme des portiers qui collectent des données précieuses impossibles à capturer à d'autres points en raison de la position unique du pare-feu sur le réseau. Les pare-feux appliquent également une politique de sécurité et peuvent donc interrompre les applications qui utilisent des protocoles réseau inhabituels ou non autorisés.

Scénario d'utilisation

Sécurité et conformité : les logs de pare-feu fournissent un enregistrement détaillé du trafic entre les différents segments du réseau, enregistrant les adresses IP, ports, protocoles source et de destination, qui sont tous essentiels lors de l'investigation des incidents de sécurité. Les données peuvent également révéler des lacunes dans la politique de sécurité, lacunes qui peuvent être comblées par des règles de pare-feu plus strictes. Les données de pare-feu contribuent à identifier et à détecter :

- les déplacements latéraux,
- toute commande et tout contrôle du trafic,
- un trafic DDoS,
- un trafic vers des domaines malveillants,
- un trafic vers des domaines inconnus,
- un trafic depuis des emplacements inconnus.

Opérations IT : lorsque les applications réseau rencontrent des problèmes de communication, les politiques de sécurité réseau peuvent en être responsables. Les données du pare-feu peuvent fournir une visibilité sur le trafic bloqué et le trafic autorisé, ce qui vous permet de déterminer si vous avez un problème d'application ou de réseau.

Détection et prévention des intrusions

Scénario d'utilisation : Sécurité et conformité

Exemples : Tipping Point, Juniper IDP, Netscreen Firewall, Juniper NSM IDP, Juniper NSM, Snort, McAfee IDS

Les IDS et IPS sont des systèmes de sécurité parallèles et complémentaires qui s'ajoutent aux pare-feux : les IDS exposent les attaques réseau et serveur qui traversent le pare-feu et les IPS fournissent des défenses plus avancées contre les attaques sophistiquées. Les IDS sont généralement placés à la périphérie du réseau, juste à l'intérieur du périmètre d'un pare-feu, bien que certaines entreprises placent également un système à l'extérieur du pare-feu pour collecter davantage d'informations sur toutes les attaques. De même, l'IPS est généralement placé à la périphérie du réseau, mais il peut également être utilisé en plusieurs couches à d'autres points du réseau ou sur des serveurs spécifiques. L'IPS fonctionne généralement en abandonnant des paquets, en réinitialisant les connexions réseau et en mettant des adresses ou des plages IP spécifiques sur liste noire.

Scénario d'utilisation

Sécurité et conformité : les logs IDS fournissent aux équipes de sécurité des enregistrements détaillés des attaques, dont le type, la source, la destination et les ports utilisés, ce qui délivre une signature d'attaque globale. Des signatures spéciales peuvent déclencher des alarmes ou d'autres mesures d'atténuation. Les IPS fournissent le même ensemble de données de signature d'attaque, mais ils peuvent aussi inclure une analyse des menaces des paquets réseau défectueux et une détection des mouvements latéraux. Ces données peuvent encore détecter le trafic de commande et de contrôle, le trafic DDoS et le trafic de domaines malveillants ou inconnus.

Contrôle de l'accès au réseau (NAC)

Scénario d'utilisation : Sécurité et conformité

Exemples : Aruba ClearPass, Cisco ACS

Le contrôle d'accès ou d'admission au réseau (NAC) est une forme de sécurité client/point de terminaison qui utilise un agent logiciel installé localement pour pré-autoriser les connexions à un réseau protégé. Le NAC examine les dispositifs clients pour repérer les éventuelles contaminations par des programmes malveillants connus et vérifier le respect des politiques de sécurité, telles que l'exécution d'un système d'exploitation approuvé avec les correctifs les plus récents. Les clients qui échouent aux analyses du NAC sont redirigés vers un réseau de quarantaine isolé jusqu'à ce que les problèmes détectés soient corrigés.

Scénario d'utilisation

Sécurité et conformité : le logiciel NAC collecte des données sur les clients connectés : il effectue un inventaire des logiciels clients installés, contrôle la conformité aux stratégies de sécurité, les versions des correctifs du système d'exploitation et des applications, et vérifie l'accessibilité par les clients d'accès à distance et l'accès des utilisateurs aux réseaux protégés. Les logs NAC fournissent aux équipes de sécurité un profil détaillé de l'état et de l'activité d'un client. Ils délivrent des informations sur les connexions de dispositifs non autorisées et peuvent servir à mettre en corrélation les utilisateurs/IP avec un emplacement réseau physique.

Switches réseau

Scénario d'utilisation : Sécurité et conformité, Opérations IT

Exemples : switches Ethernet, switches virtuels

Les switches sont des intersections de réseau où les paquets se déplacent d'un segment à un autre. Dans leur forme la plus pure, les switches fonctionnent au sein d'un sous-réseau IP particulier et ne peuvent pas acheminer les paquets de couche 3 vers un autre réseau. Les concepts modernes de datacenters utilisent généralement une hiérarchie de switches à deux niveaux : commutateurs « top of rack » (ToR) connectant les serveurs et les baies de stockage à la périphérie, et switches d'agrégation ou de colonne vertébrale, qui établissent la connexion au cœur du réseau. Bien que les switches Ethernet soient beaucoup plus répandus, certaines entreprises utilisent également des canaux fibre optique ou infiniband pour les réseaux de stockage ou les interconnexions HPC, chacune ayant son propre type de switch.

Scénario d'utilisation

Sécurité et conformité : les données des switches, souvent capturées sous forme d'enregistrements NetFlow, constituent une source essentielle pour repérer les menaces persistantes avancées, analyser les flux de trafic pour détecter toute activité inhabituelle et identifier les éventuelles exfiltrations de données. En tant que source de données de niveau filaire, les statistiques des switches sont presque impossibles à altérer et constituent donc une source essentielle de données de sécurité. Ces données peuvent également être utilisées pour mettre en corrélation des utilisateurs ou des adresses IP avec un emplacement réseau physique.

Opérations IT : les équipes d'exploitation utilisent les logs des switches pour observer l'état du trafic, comme la source et la destination, la classe de service et les causes de congestion. Les logs peuvent également afficher les statistiques de trafic sous forme agrégée, par port et par client, et indiquer si certains ports sont congestionnés, défaillants ou à l'arrêt.

Proxys

Scénario d'utilisation : Sécurité et conformité, Opérations IT

Exemples : Blue Coat, Fortinet, Juniper IDP, Netscreen Firewall, Palo Alto Networks, Palo Alto Networks config, Palo Alto Networks system, Palo Alto Networks threat, Palo Alto Networks traffic, nginx

Les proxys réseau sont utilisés de plusieurs façons dans l'infrastructure IT : comme accélérateurs d'applications web, comme pare-feu intelligent d'orientation du trafic à l'échelle des applications et comme filtres de contenu. En agissant en tant qu'intermédiaire transparent de type « bump-in-the-wire », les proxys voient l'ensemble de la pile de protocoles réseau de couche 7, ce qui leur permet de mettre en œuvre des politiques de sécurité et de gestion du trafic spécifiques aux applications.

Scénario d'utilisation

Sécurité et conformité : les équipes de sécurité s'intéressent aux proxys en tant que pare-feux de la couche applicative. Ici, les enregistrements proxy peuvent identifier des informations sur le contenu spécifique qui passe les points de contrôle du réseau, comme les noms de fichier, les types, la source et la destination, ainsi que les métadonnées du client demandeur, telles que la signature du système d'exploitation, l'application et le nom d'utilisateur/ID (selon l'implémentation du proxy). Les données peuvent également être utilisées pour détecter le trafic de commande et de contrôle et le trafic de domaines malveillants ou inconnus.

Les proxys web et certains pare-feux de nouvelle génération peuvent agir en mode transparent ou explicite et communiquer avec les serveurs HTTP(S) pour le compte d'un client. En utilisant un certain nombre de technologies connexes, la requête et la réponse peuvent être inspectées puis autorisées ou bloquées, en fonction du rôle de l'utilisateur, de la catégorie de site ou de ressource, ou d'un indicateur d'attaque. Les données enregistrées dans les événements peuvent potentiellement être utilisées dans la corrélation de détection.

Opérations IT : les équipes des opérations utilisent souvent des proxys intégrés dans un contrôleur de livraison d'application (ADC), version plus avancée et compatible avec la couche 7 d'un équilibreur de charge. Dans ce contexte, les logs de proxy peuvent fournir des informations sur les requêtes entrantes et la répartition du trafic entre les ressources disponibles.

Logs systèmes

Scénario d'utilisation : Sécurité et conformité, Opérations IT, Livraison des applications

Exemples : Unix, Windows, Mac OS, Linux

Chaque système d'exploitation enregistre des informations sur ses conditions de fonctionnement et ses erreurs, et ces logs horodatés constituent la source fondamentale de référence de la télémétrie du système. Selon le système d'exploitation, il peut exister des logs distincts pour différentes classes d'événements, comme les mises à jour informatives de routine, les erreurs système, les enregistrements du chargeur de démarrage, les tentatives de connexion et les résultats de débogage. Les logs d'erreurs regroupent souvent des enregistrements provenant de plusieurs sous-systèmes et services ou démons du système d'exploitation, et constituent donc une source définitive d'informations de dépannage.

Scénario d'utilisation

Sécurité et conformité : les logs système incluent une variété d'informations de sécurité telles que les tentatives de connexion, l'accès aux fichiers et l'activité du pare-feu système. Ces entrées peuvent avertir les équipes de sécurité des attaques réseau, d'une violation de sécurité ou de la compromission d'un logiciel. Elles constituent également une source inestimable d'informations dans l'investigation d'un incident de sécurité. Par exemple, les données peuvent être utilisées pour identifier les modifications apportées aux configurations système et aux commandes exécutées par des utilisateurs ou des utilisateurs privilégiés.

Opérations IT et livraison des applications : les logs système sont souvent le premier recours des équipes des opérations lors du diagnostic des problèmes qui touchent le système d'exploitation, le matériel ou diverses interfaces d'E/S. Comme un problème particulier se manifeste souvent par des erreurs dans plusieurs sous-systèmes, la corrélation des entrées de log est l'une des meilleures façons d'identifier la cause profonde d'une défaillance subtile du système.

Logs de serveurs

Scénario d'utilisation : Sécurité et conformité, Opérations IT, Livraison des applications

Les systèmes d'exploitation des serveurs enregistrent en permanence une variété de données de fonctionnement, de sécurité, d'erreurs et de débogage : librairies système chargées au démarrage, processus d'application ouverts, connexions réseau, systèmes de fichiers montés, utilisation de la mémoire système, etc. Le niveau de détail est configurable par l'administrateur système, mais il y a suffisamment d'options pour obtenir une image complète de l'activité du système tout au long de son service. Selon le sous-système, les logs des serveurs seront utiles aux équipes chargées du système, du réseau, du stockage ou de la sécurité.

Scénario d'utilisation

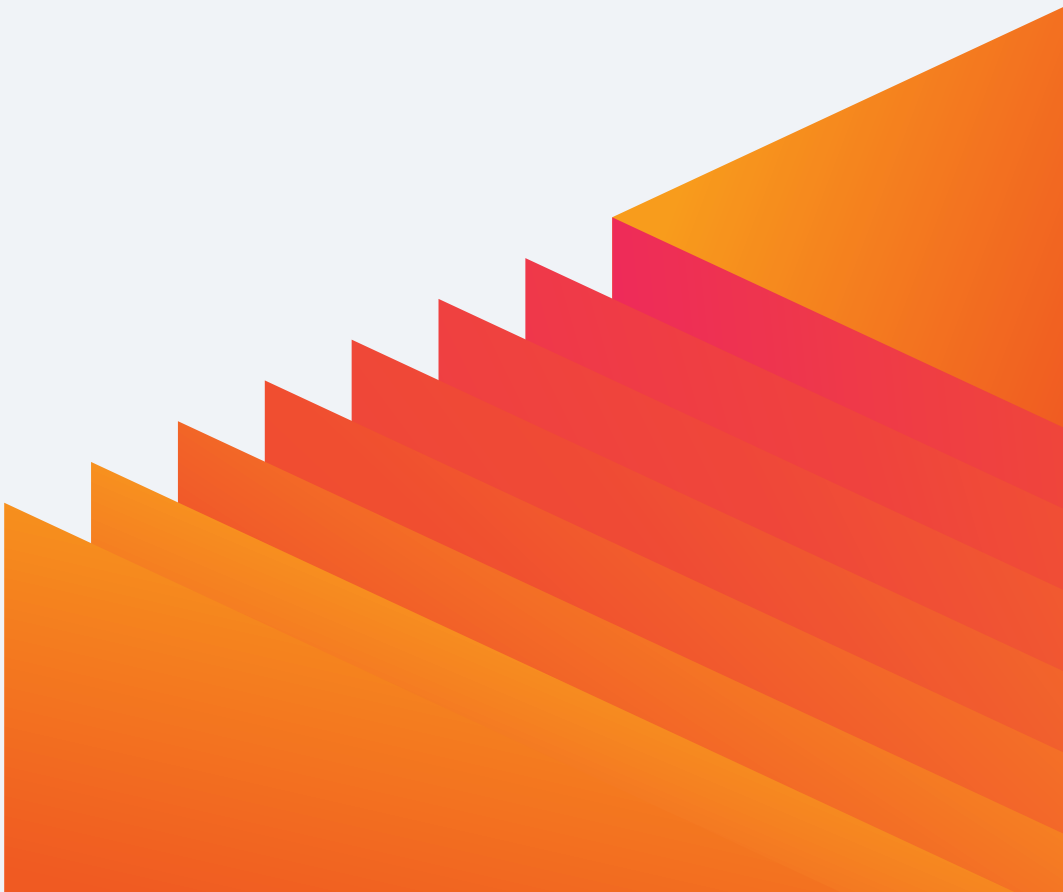
Sécurité et conformité : les logs de serveurs regroupent les données des sous-systèmes de sécurité : événements des pare-feux locaux, tentatives de connexion et erreurs d'accès aux fichiers. Les équipes de sécurité savent exploiter ces données pour identifier les tentatives d'infraction, tracer les infiltrations réussies et corriger les vulnérabilités. Superviser les logs de serveurs qui consignent les accès aux fichiers, les authentifications et l'utilisation des applications peut contribuer à sécuriser les composants d'infrastructure.

Opérations IT et livraison des applications : les logs de serveurs fournissent un enregistrement détaillé de l'état général du système et des informations sur l'heure exacte des erreurs et des situations anormales, qui sont inestimables lorsque l'on recherche la cause profonde des problèmes d'un système.

À propos de **Splunk.**

Splunk transforme les données en actions grâce à la plateforme de sécurité unifiée et d'observabilité. La technologie Splunk est conçue pour investiguer, superviser, analyser et exploiter les données à toutes les échelles. Rejoignez des millions d'utilisateurs passionnés en essayant Splunk gratuitement.

Essai gratuit



splunk>

24-122987-Splunk-theessentialguidetosecuritydata-101