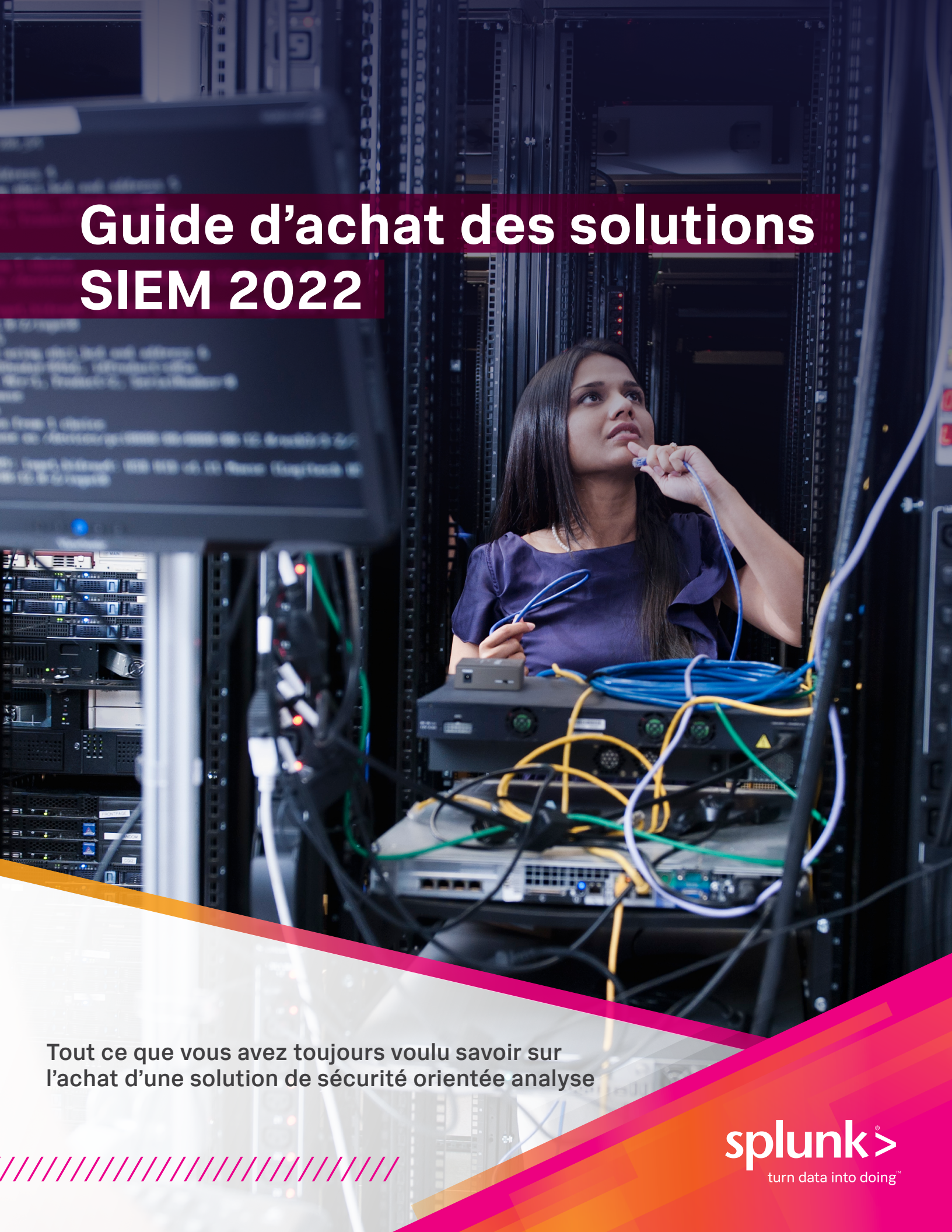


Guide d'achat des solutions SIEM 2022

Tout ce que vous avez toujours voulu savoir sur l'achat d'une solution de sécurité orientée analyse

splunk>
turn data into doing™

Sommaire

1. Qu’est-ce qu’un SIEM ?

Une solution de gestion des informations et des événements de sécurité (SIEM) s’apparente au système radar utilisé par les pilotes et les contrôleurs aériens. Sans lui, l’IT d’entreprise vole à l’aveugle. Bien que les dispositifs et logiciels de sécurité parviennent à détecter et enregistrer les attaques isolées et les comportements anormaux, les menaces les plus graves d'aujourd’hui sont distribuées et coordonnées sur plusieurs systèmes, et elles emploient des techniques de dissimulation pour éviter toute détection. Sans SIEM, les attaques peuvent germer et devenir des incidents catastrophiques.

Les solutions SIEM acquièrent d'autant plus d’importance dans l’entreprise d'aujourd'hui que les attaques gagnent en sophistication, et que l'utilisation croissante des services cloud élargit la surface de vulnérabilité.

Dans ce guide d'achat, nous cherchons à expliquer ce qu’est – et n’est pas – une solution SIEM, son évolution, ce qu’elle fait et comment déterminer si c’est la bonne solution de sécurité pour votre entreprise.

Qu’est-ce qu’un SIEM ?

Pour Gartner, **le SIEM** est « une technologie qui aide à la détection des menaces et à la réponse aux incidents de sécurité grâce à la collecte en temps réel et à l’analyse historique des événements de sécurité provenant d'un large éventail de sources de données contextuelles et d'événements. »

Qu’est-ce que tout cela signifie en français ?

Pour résumer, un SIEM est une plateforme de sécurité qui assimile les logs d'événements et offre une vue unifiée de ces données, accompagnée d’informations supplémentaires.

L'évolution du SIEM

Les SIEM sont nés de la nécessité de combiner le stockage à long terme des logs d'événements à la supervision en temps réel, afin de permettre aux équipes IT d'avoir une vision holistique de l'état actuel de la position de sécurité de l'entreprise. Toutefois, les SIEM traditionnels reposaient sur une technologie caractérisée par un manque de maniabilité et d'évolutivité. Et il est souvent difficile pour les professionnels de l'IT d'identifier et de comprendre rapidement les attaques de sécurité. Les solutions SIEM ont donc évolué pour devenir des outils d'analyse robustes offrant plus de flexibilité et de simplicité d'utilisation. Les capacités fondamentales du SIEM se sont élargies au cours des dix dernières années afin d'inclure les rapports de conformité, l'agrégation des logs des produits ponctuels tels que les pare-feux, la supervision des menaces, la corrélation des événements, l'analyse et la réponse aux incidents.

À l'heure où le monde entre dans l'ère du numérique, de plus en plus d'entreprises étudient et mettent en œuvre des solutions cloud. Aujourd'hui, une solution SIEM moderne axée sur l'analyse prend en charge les solutions cloud, contrairement à ses ancêtres. Dans ce guide, nous allons étudier en détail les différences qui séparent les SIEM traditionnels des solutions modernes axées sur l'analyse, et voir si votre entreprise est prête à implémenter un SIEM.

Les SIEM traditionnels appartiennent au passé

Il est relativement facile de trouver un mécanisme pour recueillir, stocker et analyser les données si l'on se limite à la sécurité. Les options de stockage des données sont nombreuses. Par contre, compiler toutes les données utiles pour la sécurité et les transformer en informations exploitables est une toute autre affaire.

Bien des départements IT d'entreprises ont fait la pénible expérience de cette dure vérité après avoir investi dans une plateforme SIEM. Après avoir consacré beaucoup de temps et d'argent à l'enregistrement des événements de sécurité, il apparaît que l'assimilation de ces données a pris un temps considérable, et surtout que le système de données sous-jacent utilisé pour créer le SIEM tend à être statique.

Pire encore, les données disponibles pour l'analyse ne sont basées que sur les événements de sécurité. Il devient donc difficile de corréler les événements de sécurité avec le reste de l'activité de l'environnement IT. En cas de problème, l'investigation d'un événement de sécurité exige un temps précieux, ce que ne peuvent se permettre la plupart des organisations. De plus, une solution SIEM traditionnelle ne parvient pas à tenir le rythme imposé par l'urgence de l'investigation des événements de sécurité. La poursuite de l'adoption des services cloud élargit les vecteurs de menaces et les entreprises doivent superviser l'activité des utilisateurs, les comportements et l'accès aux applications sur les services cloud, en logiciel en tant que service (SaaS), mais aussi locaux, afin de déterminer toute l'envergure des menaces et attaques potentielles.

SIEM traditionnel : problèmes et caractéristiques

PROBLÈME	DIFFICULTÉ
Ne peut pas utiliser les données requises	Limite la détection, l'investigation et la réponse
Difficile à entretenir et à administrer	Complexité nécessitant un personnel très compétent
Taux élevé de faux négatifs et faux positifs	Fardeau pour les SecOps
Instable	Réputé pour ses interruptions de service
Données sans flexibilité	Ne s'adapte pas aux cas critiques
Workflows statiques	Limité et contraignant
Incapacité à détecter les menaces modernes	Risque commercial

L'alternative : un SIEM axé sur l'analyse

Aujourd'hui, l'informatique d'entreprise a besoin d'un moyen simple de corréler l'ensemble des données. Une solution qui permette à l'IT de gérer sa position de sécurité. Au lieu de se contenter d'examiner les événements après qu'ils se sont produits, le service IT doit pouvoir anticiper leur apparition et mettre en place des mesures pour limiter les vulnérabilités en temps réel. Et pour cela, les entreprises ont besoin d'une plateforme SIEM axée sur l'analyse.

C'est là que réside toute la différence entre un SIEM traditionnel et une solution SIEM moderne. Gartner explique que cette distinction réside dans le fait qu'un **« SIEM moderne exploite bien plus que les données de log et fait bien plus qu'appliquer des règles de corrélation pour analyser les données. »**

C'est là qu'un type particulier de SIEM moderne, que nous aimons appeler « SIEM orienté analyse », entre en jeu. Cette solution moderne permet à l'IT de superviser les menaces en temps réel et de réagir rapidement aux incidents, afin que les dommages puissent être évités ou limités. Mais les attaques ne proviennent pas toutes de l'extérieur, et l'IT doit pouvoir superviser l'activité de ses utilisateurs pour minimiser les risques de menaces internes ou de compromission accidentelle. La threat intelligence est cruciale pour comprendre la nature de l'environnement de menaces au sens large, et pour replacer ces menaces en contexte.

Un SIEM orienté analyse doit exceller dans le domaine de l'analyse de sécurité, et mettre à la disposition des équipes IT des méthodes quantitatives sophistiquées et puissantes pour obtenir des informations et hiérarchiser leurs efforts. Enfin, un SIEM moderne doit intégrer, au sein de sa plateforme de base, les outils spécialisés nécessaires pour lutter contre les menaces avancées.

Une autre différence majeure entre un SIEM axé sur l'analyse et un SIEM traditionnel réside dans la nature flexible d'une solution moderne, qui permet de la déployer localement, dans le cloud ou dans un environnement hybride.

Le graphique ci-dessous présente les raisons principales que peut avoir une entreprise d'opter pour une solution SIEM axée sur l'analyse plutôt qu'un SIEM traditionnel.

7 raisons de remplacer votre SIEM traditionnel

Les entreprises sont souvent liées aux architectures obsolètes des SIEM traditionnels, qui reposent généralement sur une base de données SQL au schéma fixe. Ces bases de données peut devenir un point d'interruption de service ou souffrir de limitations en termes de dimensions et de performances.

1. **DES TYPES DE DONNÉES DE SÉCURITÉ LIMITÉS**	En limitant les types de données assimilés, on limite également la détection, l'investigation et la rapidité d'intervention.
2. **INCAPACITÉ À ASSIMILER EFFICACEMENT LES DONNÉES**	Avec les SIEM traditionnels, l'assimilation des données peut être un processus extrêmement laborieux ou coûteux.
3. **LENTEUR DES INVESTIGATIONS**	Avec les SIEM traditionnels, des opérations de base comme les recherches dans les logs bruts peuvent prendre un temps considérable, qui se compte souvent en heures et en jours.
4. **INSTABILITÉ ET ÉVOLUTIVITÉ**	Une base de données SQL perd en stabilité lorsqu'elle prend du volume. Les clients souffrent souvent de mauvaises performances ou de coupures fréquentes, qui surviennent lorsque des pics d'événements surchargent les serveurs.
5. **FIN DE VIE OU FEUILLE DE ROUTE INCERTAINE**	Lorsque les éditeurs de SIEM traditionnels sont rachetés par d'autres entreprises, la R&D est rapidement mise à l'arrêt. Sans des investissements et une innovation continus, les solutions de sécurité ne parviennent pas à tenir le rythme de l'évolution du paysage des menaces.
6. **UN ÉCOSYSTÈME FERMÉ**	Les fournisseurs de SIEM traditionnels n'ont souvent pas la possibilité d'intégrer leur solution à d'autres outils du marché. Les clients sont contraints d'utiliser les outils fournis dans le SIEM ou d'investir dans des développements personnalisés et des services professionnels.
7. **LIMITÉ À UNE INSTALLATION LOCALE**	Les SIEM traditionnels sont souvent restreints à un déploiement local. Les praticiens de sécurité doivent pouvoir exploiter des applicatifs dans le cloud, locaux et hybrides.

Votre SIEM dans le cloud

Exploiter un SIEM dans le cloud ou en SaaS peut résoudre de nombreux problèmes liés à l'information de sécurité mais beaucoup de décideurs informatiques n'ont toujours pas confiance dans la sécurité et la fiabilité du cloud. Avant de rejeter l'option du SIEM dans le cloud, sachez que les pratiques et les technologies de sécurité de la plupart des grands services cloud peuvent être bien plus sophistiquées que celles d'une entreprise classique.

Le SaaS est déjà largement employé pour des systèmes stratégiques tels que le CRM, les RH, l'ERP et l'analyse commerciale. Les mêmes raisons qui font du SaaS une option judicieuse pour les applications d'entreprise (rapidité, déploiement facile, faibles coûts, mises à jour automatiques, facturation à l'utilisation, infrastructure évolutive et renforcée) expliquent que le cloud soit idéal pour le SIEM.

Les solutions cloud offrent la possibilité d'utiliser un large éventail de groupes de données provenant d'installations locales comme du cloud. À l'heure actuelle, les entreprises déplacent leurs applicatifs vers l'infrastructure en tant que service (IaaS), les plateformes en tant que service (PaaS) et le SaaS. Dans ce contexte, sa simplicité d'intégration avec les systèmes tiers rend une approche cloud du SIEM encore plus pertinente. Les avantages stratégiques d'un SIEM dans le cloud sont nombreux : souplesse d'une architecture hybride, mises à jour automatiques et configuration simplifiée des logiciels, infrastructure instantanée et évolutive, contrôles stricts et disponibilité élevée.

Scénarios d'utilisation du SIEM en entreprise

Maintenant que vous comprenez comment le SIEM a évolué et quelles sont les caractéristiques qui distinguent un SIEM moderne, orienté analyse, d'un SIEM traditionnel, il est temps de voir quels scénarios de sécurité sont concrètement pris en charge par cette technologie.

Les exigences de détection précoce, de réponse rapide et de collaboration dans la lutte contre les menaces avancées exercent une lourde pression sur les équipes de sécurité d'entreprise d'aujourd'hui. Il ne suffit plus de produire des rapports ou de superviser les logs et les événements de sécurité. Les professionnels de la sécurité ont besoin d'informations plus riches, issues de toutes les sources données dispersées dans toute l'entreprise, des systèmes informatiques aux outils métier en passant par le cloud. Pour garder une longueur d'avance sur les attaques externes et les acteurs malveillants en interne, les entreprises ont besoin de solutions de sécurité sophistiquées permettant de détecter rapidement les problèmes, d'y répondre rapidement, d'investiguer les incidents et de coordonner des scénarios de faille selon une approche de CSIRT. Les entreprises doivent également pouvoir détecter et prendre en charge les menaces connues, inconnues et avancées.

Les équipes de sécurité d'entreprise doivent disposer d'une solution SIEM qui ne résout pas seulement les cas de sécurité mais aussi des scénarios plus complexes. Pour rester à la hauteur face au dynamisme du paysage des menaces, les SIEM modernes doivent être capables de :

- centraliser et agréger tous les événements de sécurité au fur et à mesure de leur génération ;
- prendre en charge un éventail de mécanismes de réception et de collecte (syslog, transmission et collecte de fichiers, etc.) ;
- ajouter des éléments de contexte et de threat intelligence aux événements de sécurité ;
- établir des corrélations et produire des alertes sur un large éventail de données ;
- détecter les menaces avancées et inconnues ;
- établir des profils de comportement dans toute l'organisation ;
- assimiler toutes les données (utilisateurs, applications) et les mettre à disposition à des fins de supervision, d'alerte, d'enquête et de recherche ad hoc ;
- permettre de créer des recherches ponctuelles et des rapports à partir des données à des fins d'analyse de faille avancée ;
- étudier les incidents et mener des investigations pour procéder à une analyse détaillées des incidents ;
- évaluer la position de conformité et produire des rapports à ce sujet ;
- utiliser l'analyse pour produire des rapports de position de sécurité ;
- tracer les actions des pirates grâce à des analyses ponctuelles normalisées et au séquençage des événements.

Bien que les données du SIEM proviennent principalement des serveurs et des logs des périphériques réseau, elles peuvent également être issues des systèmes de sécurité des points de terminaison et du réseau, d'applications, de services cloud, de systèmes d'authentification et d'autorisation, et de bases de données en ligne de vulnérabilités et de menaces.

Mais l'agrégation des données n'est qu'un aspect de l'histoire. Le logiciel SIEM procède ensuite à la corrélation des données du dépôt ainsi obtenu et recherche les comportements inhabituels, les anomalies et autres indicateurs d'incidents de sécurité. Les informations ne sont pas seulement utilisées pour produire des notifications en temps réel, elles servent aussi pour les audits et les rapports de conformité, les tableaux de bord de performance, les analyses de tendances historiques et les investigations post-incident.

Face au nombre croissant et à la sophistication des menaces de sécurité, et devant la valeur toujours plus grande des actifs numériques de toute entreprise, on ne sera pas surpris d'apprendre que l'adoption de solutions SIEM axées sur l'analyse s'intensifie dans l'écosystème global de la sécurité IT.

Avez-vous vraiment besoin d'un SIEM ?

Vous comprenez à présent à quoi sert un SIEM : prenons maintenant un peu de recul. Votre entreprise a-t-elle réellement besoin d'un SIEM… ou d'un autre type de solution ?

Il se peut que votre entreprise ne soit pas prête à prendre en charge des cas de sécurité avancés et ait plutôt besoin d'une solution capable de lui fournir des informations sur ses données machine ; on pense par exemple à un système de gestion centralisée des logs, ou CLM. Petit placement de produit éhonté : découvrez **Splunk Enterprise pour la sécurité et la gestion des logs**.

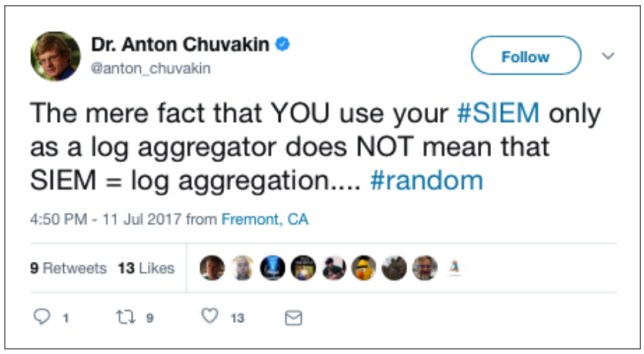
Commençons donc par voir ce qu'est une solution de gestion centralisée des logs. La CLM est une solution qui offre une vision centralisée sur les données de log.

Pour plus de contexte, permettez-nous de poser la question suivante : que sont les données de log ?

Les données de log sont des messages de journaux générés par les ordinateurs qui représentent une archive définitive des activités de toutes les entreprises, organisations et agences, et elles sont rarement exploitées à des fins de dépannage ou pour appuyer les objectifs plus larges de l'entreprise.

Revenons à la CLM. La gestion des logs a pour but de recueillir ces journaux produits par des ordinateurs et de permettre à des utilisateurs de les interroger et de générer des rapports. Du point de vue de la sécurité, la CLM peut faciliter l'investigation des incidents et le tri des alertes.

La gestion des logs est une fonction centrale des SIEM depuis leur apparition. Mais si vous cherchez simplement à extraire des informations de vos données de log, le SIEM orienté analyse est-il vraiment l'outil qu'il vous faut ? Demandons à **Anton Chuvakin, célèbre analyste SIEM**, de répondre à cette question :



On peut résumer la problématique comme ceci : si vous utilisez une solution SIEM pour agréger des logs, vous payez trop cher. Le point important, c'est que vous pouvez utiliser un SIEM pour des applications de sécurité aussi bien basiques que sophistiquées.

De l'autre côté du spectre de la maturité, il y a l'analyse du comportement des utilisateurs et des entités (UEBA) **comme l'a baptisée Gartner**. Cette catégorie porte d'autres noms : **Forrester a préféré** analyse sécuritaire des comportements des utilisateurs et **Splunk a opté pour analyse des comportements des utilisateurs (UBA)**, et c'est ce dernier terme que nous emploierons dans le reste de ce rapport. Toutes ces expressions désignent la même technologie.

L'UBA est utilisée pour découvrir et corriger des menaces internes et externes. On considère souvent l'UBA comme une application de sécurité plus sophistiquée, en partie parce qu'elle possède, par exemple, la capacité d'apprendre les habitudes d'un utilisateur, d'en déduire un comportement de référence puis de générer une alerte quand il se produit quelque chose d'anormal.

Dans la continuité de cet exemple, pour établir une référence, la solution UBA va suivre les habitudes propres à certaines activités :

- la localisation depuis laquelle les utilisateurs se connectent généralement ;
- les permissions dont disposent les utilisateurs ;
- les fichiers, serveurs et applications auxquels accèdent les utilisateurs ;
- les appareils depuis lesquels les utilisateurs se connectent généralement.

Pour plus de contexte, certains fournisseurs d'UBA essaient de se faire une place sur le marché du SIEM. Ce sont des nouveaux venus dans le domaine. L'UBA est une solution utile, certes, mais elle ne peut pas à elle seule remplir toutes les fonctions d'un SIEM. Et l'UBA n'est pas une nouvelle catégorie de SIEM. C'est une technologie de sécurité à part entière. Idéalement, une solution UBA doit pouvoir fonctionner de concert avec un SIEM orienté analyse.

Et prosaïquement : tout comme une solution CLM n'est pas un SIEM, l'UBA n'en est pas une non plus. Si seulement Dr Chuvakin avait **twitté à ce sujet.**

2. Bases essentielles du SIEM

Nous allons maintenant plonger au cœur de ce qui compose un SIEM orienté analyse. Un SIEM orienté analyse doit rassembler sept fonctionnalités essentielles :

SUPERVISION EN TEMPS RÉEL	Les menaces évoluent rapidement et l'IT doit pouvoir les superviser et corréler les événements en temps réel pour localiser et arrêter les menaces.
RÉPONSE AUX INCIDENTS	L'IT doit disposer d'une approche structurée pour prendre en charge et gérer les failles potentielles ainsi que les conséquences d'un incident ou d'une attaque, afin de limiter les dommages et de réduire les coûts et le délai de rétablissement.
SUPERVISION DES UTILISATEURS	Il est indispensable de superviser l'activité des utilisateurs en contexte pour localiser les failles avec précision et mettre au jour les usages illégaux. La supervision des utilisateurs privilégiés est une exigence courante dans les rapports de conformité.
THREAT INTELLIGENCE	La threat intelligence aide l'IT à identifier les activités anormales, à évaluer les risques pour l'entreprise et à hiérarchiser la réponse.
ANALYSES AVANCÉES	L'analyse est la clé qui permet d'extraire des informations à partir de montagnes de données, et le machine learning peut automatiser cette analyse pour identifier les menaces invisibles.
DÉTECTION DES MENACES AVANCÉES	Les professionnels de sécurité ont besoin d'outils spécialisés pour superviser, analyser et détecter les menaces sur toute la kill chain.
BIBLIOTHÈQUE DE CAS D'USAGE	Les entreprises doivent impérativement comprendre et prendre en charge les menaces en temps réel pour réduire leur niveau de risque.

Ces capacités leur permettent d'exploiter leur SIEM dans une large gamme de cas d'usage de sécurité et de conformité. On peut aussi définir un SIEM moderne en fonction de ses capacités. Examinons de plus près chaque fonction clé d'un SIEM axé sur l'analyse.

Supervision en temps réel

Plus il faut de temps pour découvrir une menace, et plus elle peut infliger de dommages. Les organisations IT doivent être armées d'un SIEM offrant des fonctions de supervision pouvant s'appliquer en temps réel à n'importe quel jeu de données, qu'il soit stocké localement ou dans le cloud. De plus, cette fonction de supervision doit pouvoir extraire à la fois les flux de données contextuels tels que les données d'actifs et d'identité, mais aussi les flux de threat intelligence, qui permettent de produire des alertes.

Un SIEM axé sur l'analyse doit être capable d'identifier toutes les entités de l'environnement IT (utilisateurs, machines et applications) et toute activité qui n'est pas spécifiquement rattachée à une identité. Le SIEM doit pouvoir utiliser ces données en temps réel pour identifier un large éventail de types et de classes de comportements anormaux. Une fois cela fait, il faut pouvoir injecter facilement les données dans un workflow créé pour évaluer les risques qu'une anomalie peut présenter pour l'entreprise.

Le SIEM doit être accompagné d'une bibliothèque de règles de corrélation prédéfinies et personnalisables, d'une console d'événements de sécurité qui présente en temps réel les incidents et les événements de sécurité, et des tableaux de bord montrant des visualisations en temps réel des activités menaçantes.

Enfin, toutes ces compétences doivent s'enrichir de recherches de corrélation prêtes à l'emploi pouvant être invoquées en temps réel ou selon un planning défini. Tout aussi utiles, ces recherches doivent être accessibles à l'aide d'une interface intuitive évitant d'avoir recours à un administrateur IT ou de maîtriser un langage de recherche.

N'oublions pas non plus qu'un SIEM orienté analyse doit permettre de faire des recherches localement dans les données temps réel et historiques, de façon à réduire le trafic réseau lié à l'accès aux données de recherche.

Autodesk gagne du temps et réduit ses dépenses d'investissement avec Splunk sur AWS

Dans des secteurs aussi variés que la fabrication, l'architecture, le bâtiment, la construction, et les médias et le divertissement (y compris les 20 derniers lauréats de l'Oscar pour les meilleurs effets spéciaux) le logiciel Autodesk est utilisé pour concevoir, visualiser et modéliser des idées. Avec une telle présence internationale, Autodesk est confronté à deux défis de taille : la nécessité d'acquérir des informations métier, opérationnelles et de sécurité sur de multiples groupes internes dispersés dans le monde, et celle de choisir la bonne infrastructure pour déployer un logiciel d'intelligence opérationnelle. Depuis le déploiement de la plateforme Splunk, la société a observé plusieurs avantages :

- des centaines de milliers de dollars économisés ;
- des informations stratégiques sur les opérations et la sécurité ;
- une visibilité en temps réel sur les performances des produits.

Pourquoi Splunk

Splunk a d'abord trouvé sa place chez Autodesk en 2007, où il servait à exploiter les données machine pour résoudre les problèmes opérationnels. Cet usage s'est élargi pour inclure de la supervision en temps réel, des informations de sécurité détaillées et des analyses commerciales destinées à la direction, et ce sur trois divisions d'Autodesk :

- le service informatique d'entreprise (EIS), chargé de la gestion globale de l'informatique d'entreprise, et notamment de la sécurité et de la gestion des informations ;
- le groupe consommateurs Autodesk (ACG), responsable de tous les produits Autodesk en contact avec les consommateurs ;
- les produits de modélisation de l'information et plateformes (IPG), en charge des solutions Autodesk destinées aux clients commerciaux, principalement des concepteurs et des ingénieurs dans tous les secteurs d'activité.

Autodesk utilise Splunk Enterprise Security (Splunk ES) pour réduire le temps nécessaire à l'identification et à la résolution des problèmes de sécurité. La société utilise également l'application Splunk pour AWS pour fournir et administrer de façon flexible les ressources de Splunk Enterprise et d'autres applications stratégiques.

Prendre des décisions basées sur les données

Splunk Enterprise, l'application Splunk pour AWS, Splunk Enterprise Security et d'autres solutions Splunk permettent à Autodesk d'obtenir de précieuses informations en temps réel sur ses opérations, la sécurité et les performances de ses produits. La plateforme flexible de Splunk, orientée analyse et basée sur AWS, permet à Autodesk de gagner du temps, de réduire ses dépenses d'investissement et d'élargir le champ et la profondeur de ses décisions stratégiques. **En savoir plus**.

Réponse aux incidents

Au cœur d'une stratégie efficace de réponse aux incidents se trouve une plateforme SIEM robuste qui permet non seulement d'identifier les différents incidents, mais offre également les moyens de les suivre, de les affecter et de les annoter.

L'IT doit fournir aux autres membres de l'entreprise des niveaux d'accès variables en fonction de leur rôle. Une organisation IT souhaitera aussi agréger des événements de façon manuelle ou automatique, bénéficier d'interfaces de programmation (API) utilisables pour échanger des données avec des systèmes tiers, collecter des données probantes légalement valables et mettre en place des procédures pour guider les équipes pas-à-pas dans la prise en charge d'incidents spécifiques.

Surtout, un SIEM axé sur l'analyse doit inclure des capacités de réponse automatique pouvant interrompre les cyberattaques en cours.

En effet, la plateforme SIEM doit être le centre autour duquel s'articulera un workflow personnalisable de gestion des incidents. Bien sûr, les incidents ne présentent pas tous le même degré d'urgence. Une plateforme SIEM axée sur l'analyse fournit aux départements IT les moyens de catégoriser la gravité d'une menace potentielle grâce à des tableaux de bord utilisables pour trier les nouveaux événements notables, les affecter à des analystes et examiner les informations associées pour produire des pistes d'investigation. Un SIEM axé sur l'analyse arme ainsi les départements IT des informations contextuelles nécessaires pour déterminer la réponse appropriée à tout type d'événements.

On doit aussi pouvoir identifier les événements notables et leur état, indiquer la gravité des événements notables, lancer un processus de correction et fournir un audit de l'intégralité du processus entourant l'incident.

Enfin, l'équipe IT doit disposer d'un tableau de bord permettant d'appliquer intuitivement des filtres à n'importe quel champ au cours d'une investigation afin d'élargir ou réduire la portée de l'analyse en quelques clics. L'objectif final doit toujours être de permettre à n'importe quel membre de l'équipe de sécurité de placer des événements, des actions et des annotations sur une chronologie grâce à laquelle les autres membres de l'équipe pourront facilement comprendre la situation. Ces chronologies peuvent ensuite être incluses dans un journal donnant ensuite la possibilité d'étudier l'attaque et de mettre en place une méthodologie de kill chain reproductible, pour prendre en charge les événements de ces types particuliers.

PagerDuty bénéficie d'une visibilité de bout en bout avec Splunk Cloud et Amazon Web Services

Les clients font appel à PagerDuty, une société de services de réponse aux incidents, pour gérer et résoudre leurs incidents IT de façon rapide et efficace. Lorsque cette entreprise entièrement basée sur le cloud a cherché une solution pour ses besoins en analyse et classification opérationnelles, elle a adopté Splunk Cloud, appliqué à AWS. Avec Splunk Cloud et AWS, PagerDuty garantit la haute disponibilité de ses services et leur évolutivité face à la demande des clients. Depuis le déploiement de Splunk Enterprise, PagerDuty a observé plusieurs avantages :

- une satisfaction des clients garantie et des services cloud hautement disponibles ;
- 30 % d'économies par rapport au service précédent ;
- une réduction du délai de résolution des incidents IT et de sécurité, qui passe de plusieurs dizaines de minutes à quelques minutes voire quelques secondes.

Pourquoi Splunk

Arup Chakrabarti est le Directeur de l'ingénierie d'infrastructure de PagerDuty. Ses responsabilités englobent la fiabilité du site, la plateforme interne et l'ingénierie de sécurité. La mission de son organisation est de favoriser la productivité et l'efficacité de toute l'organisation d'ingénierie de l'entreprise, qui regroupe plusieurs équipes d'ingénierie au sein du département de développement produit.

Avant d'adopter Splunk Cloud, PagerDuty utilisait une solution de journalisation qui n'a pas été à la hauteur lorsque l'entreprise a commencé à indexer des centaines de gigaoctets de logs chaque jour. L'équipe avait en outre des difficultés à extraire des informations exploitables de ces données pour prendre des décisions et résoudre rapidement les problèmes. Après avoir utilisé en parallèle son précédent service et Splunk Cloud, l'équipe a conclu que Splunk Cloud offrait la vitesse nécessaire pour résoudre rapidement les problèmes et garantir à ses clients une disponibilité élevée. En quelques jours, les ingénieurs sont passés à Splunk Cloud.

M. Chakrabarti explique : « Avec notre précédente solution, il fallait à certaines requêtes jusqu'à 30 minutes pour analyser les données et produire les informations demandées, ce qui était tout bonnement inacceptable. Du point de vue de l'impact sur le client, nous sommes parvenus à faire passer ce délai de résolution de plusieurs dizaines de minutes à quelques minutes ou même secondes en installant Splunk Cloud. »

M. Chakrabarti souligne également que le coût n'était pas le facteur principal du choix de Splunk Cloud, mais **« Mon équipe de comptabilité était absolument ravie lorsque j'ai annoncé 'Nous allons nous procurer la meilleure solution, et soit dit en passant, elle coûte 30 % moins cher que celle que nous utilisons actuellement.' »** En savoir plus.

Supervision des utilisateurs

Au strict minimum, la supervision de l'activité des utilisateurs doit offrir la possibilité d'analyser les données d'accès et d'authentification, établir le contexte de l'utilisateur et produire des alertes en cas de comportement suspect et d'infraction aux politiques de l'entreprise et aux directives réglementaires.

Il est absolument essentiel que la supervision des utilisateurs soit étendue aux utilisateurs privilégiés qui sont les plus souvent visés par les attaques et peuvent causer le plus de dommages en cas d'usurpation. En effet, en raison de ce risque, la supervision des utilisateurs privilégiés est une exigence courante dans les rapports de conformité.

Pour atteindre ces objectifs, il faut des vues en temps réel et des capacités de rapports exploitant divers mécanismes d'identités capables de couvrir un nombre illimité d'applications et de services tiers.

Travis Perkins PLC adopte un SIEM orienté analyse pour faciliter la migration vers un cloud hybride

Travis Perkins PLC est un fournisseur britannique de matériel pour le bâtiment et détaillant de fournitures de bricolage comptant 2 000 points de vente et 28 000 employés En 2014, l'organisation s'est lancée dans une initiative « priorité au cloud », mais sa solution de gestion des événements et des informations de sécurité n'était pas en mesure de délivrer les informations de sécurité nécessaires sur un environnement hybride. Travis Perkins PLC a examiné les alternatives disponibles et choisi Splunk Cloud, Splunk Enterprise et Splunk Enterprise Security (ES) comme SIEM. Depuis le déploiement de la plateforme Splunk, Travis Perkins PLC a observé plusieurs avantages :

- l'amélioration de la visibilité sur l'infrastructure hybride ;
- la capacité à détecter et à prendre en charge les cybermenaces complexes ;
- une réduction des coûts informatiques grâce à une gestion plus rentable des ressources.

Pourquoi Splunk

Confronté à un marché difficile au cours de la récession, Travis Perkins PLC avait fait passer ses investissements technologiques au second plan. Récemment, avec l'amélioration du contexte économique, la société a procédé à une étude stratégique de son infrastructure technologique et adopté une approche « priorité au cloud » pour réduire ses coûts et gagner en flexibilité. Quand Travis Perkins PLC a déployé plusieurs services cloud comme la G Suite de Google Cloud, Amazon Web Services et Infor CloudSuite, il est rapidement devenu évident que son SIEM n'était pas capable de fournir les informations nécessaires sur les événements de sécurité d'un environnement hybride complexe. Après avoir étudié différentes alternatives, dont les offres d'HP, IBM et LogRhythm, Travis Perkins PLC a choisi Splunk Cloud, Splunk Enterprise et Splunk ES pour bénéficier d'une vue unifiée sur son activité de sécurité.

Bâtir intégralement la sécurité

Travis Perkins PLC a saisi l'opportunité qu'offrait l'implémentation de Splunk ES pour sensibiliser tout le personnel de l'IT aux questions de sécurité, au lieu de se limiter à l'équipe de sécurité. Tous les employés de l'équipe des opérations IT ont maintenant accès à des tableaux de bord et à des alertes spécifiques qui leur permettent de répondre sans délai aux menaces potentielles et de prendre des mesures immédiates avant de transmettre les problèmes à l'équipe de sécurité dédiée si nécessaire. Travis Perkins PLC a ainsi mis sur pied un centre des opérations de sécurité (SOC) hautement efficace et lean, sans avoir à mobiliser les ressources considérables que cela exige normalement.

Automatisation de la défense contre les menaces

Avec 24 000 employés basés dans tout le Royaume-Uni et utilisant une variété d'appareils pour accéder aux données de l'entreprise, il était devenu indispensable pour Travis Perkins PLC d'automatiser une large part de sa cybersécurité. Grâce à Splunk ES, Travis Perkins PLC calcule aujourd'hui les scores de risque de différentes activités menaçantes en s'appuyant sur des données et alertes corrélées précédemment et provenant des solutions de sécurité existantes de l'entreprise. En cas d'attaque par des e-mails d'hameçonnage, par exemple, si un client infecté est identifié par des recherches de corrélation dans la plateforme Splunk, cela produit une alerte automatisée. Les équipes concernées réagissent ensuite en suivant une procédure prédéfinie. Les couloirs d'activité de Splunk ES offrent une vue holistique sur un actif ou un utilisateur, ce qui réduit considérablement le temps nécessaire à l'investigation et à la résolution d'un incident de sécurité. **En savoir plus**.

Threat intelligence

Un SIEM axé sur l'analyse doit proposer deux formes différentes de threat intelligence. La première repose sur l'utilisation de services de threat intelligence qui fournissent des informations actualisées sur les indicateurs de compromission, les tactiques, techniques et procédures adverses, ainsi que du contexte supplémentaire sur différents types d'incidents et d'activités. Ces informations facilitent la reconnaissance des activités anormales comme, entre autres, l'identification de connexions sortantes vers une adresse IP externe connue pour être un serveur de commande et de contrôle actif. Avec ce niveau de threat intelligence, les analystes détiennent les informations nécessaires pour évaluer les risques, l'impact et les objectifs d'une agression, des aspects cruciaux pour hiérarchiser et adapter la réponse.

La deuxième forme d'intelligence consiste à évaluer le caractère critique d'un actif, son utilisation, sa connectivité, ses propriétaires et, en dernier lieu, le rôle, la responsabilité et le statut d'emploi de l'utilisateur. Ce contexte supplémentaire est souvent crucial quand il s'agit d'évaluer et d'analyser le risque et l'impact potentiels d'un incident. Par exemple, un SIEM axé sur l'analyse doit pouvoir incorporer les informations de lecture de badge des employés et corréler ces données avec les logs d'authentification du VPN pour produire du contexte sur l'emplacement d'un employé dans le réseau de l'entreprise. Pour offrir des niveaux d'analyse et d'intelligence opérationnelle plus profonds encore, le SIEM doit aussi utiliser les API REST pour récupérer, via une action de workflow ou un script, ces informations de contexte et les injecter dans le système, ainsi que pour combiner des données structurées issues de bases de données relationnelles avec des données machine.

Les données de threat intelligence doivent idéalement être intégrées avec les données machine générées par divers types d'infrastructures IT et d'application pour créer des listes de supervision, des règles de corrélation et des requêtes, afin d'accroître le taux de réussite de la détection précoce des failles. Ces informations doivent être automatiquement corrélées aux données d'événements et ajoutées aux vues et rapports des tableaux de bord, ou bien transmises à des pare-feux ou autres systèmes de prévention des intrusions capables de résoudre la vulnérabilité en question.

Le tableau de bord fourni par le SIEM doit suivre l'état et l'activité des produits de détection des vulnérabilités déployés dans l'environnement IT, réaliser des contrôles de santé des systèmes de balayage et identifier les systèmes qui ne sont plus supervisés.

Pour résumer, une couche complète de threat intelligence doit prendre en charge n'importe quelle liste de menaces, identifier automatiquement les informations redondantes, identifier et hiérarchiser les menaces figurant dans plusieurs listes et attribuer une pondération aux différentes menaces afin d'évaluer le risque réel qu'elles représentent pour l'entreprise.

La Ville de Los Angeles met en œuvre le partage des informations de sécurité en temps réel sur plus de 40 agences municipales

Pour protéger son infrastructure numérique, la ville de Los Angeles a besoin d'avoir une connaissance précise de sa position de sécurité et de fournir à ses services et ses partenaires des informations sur les menaces. Par le passé, les 40 agences de la ville disposaient de mesures de sécurité disparates, ce qui compliquait la consolidation et l'analyse des données. Los Angeles était en quête d'une solution de gestion des événements et des informations de sécurité qui soit évolutive et fournie sous forme SaaS, afin d'identifier, hiérarchiser et réduire les menaces, acquérir une visibilité sur les activités suspectes et évaluer les risques à l'échelle de la ville. Depuis qu'elle a déployé Splunk Cloud et Splunk Enterprise Security, la ville bénéficie de nombreux avantages :

- la création d'un Centre des opérations de sécurité (SOC) à l'échelle de la ville ;
- la threat intelligence en temps réel ;
- la réduction des coûts d'exploitation.

Connaissance de la situation en temps réel

Splunk Cloud fournit à la ville de Los Angeles des images holistiques de sa position de sécurité. Les forwarders Splunk envoient des logs bruts et autres données provenant des différents services de la ville à Splunk Cloud, où ils sont normalisés et renvoyés au SOC intégré pour être analysés et visualisés dans des tableaux de bord Splunk. Grâce aux tableaux de bord préconfigurés et faciles à personnaliser de Splunk ES, les cadres et les analystes bénéficient en permanence d'une vision en temps réel des événements de sécurité dans toute l'infrastructure réseau de la ville. Depuis que toutes les données de sécurité sont stockées dans une base de données continuellement mise à jour, l'équipe de Timothy Lee affiche et compare tous les types de données machine (logs disparates, données structurées ou non) pour en extraire des informations de sécurité globales et exploitables.

La threat intelligence au bon moment

Le SOC intégré de la ville ne se contente pas de recueillir des informations, il en fournit également. Il traduit les données provenant de Splunk Cloud en threat intelligence opportune. La ville communique ses observations à ses propres agences ainsi qu'aux acteurs externes comme le FBI, le département de Sécurité intérieure, les Services secrets et autres autorités. Forte de ces informations, la ville collabore avec les agences fédérales pour identifier les risques et mettre au point des stratégies afin de décourager de futures intrusions sur le réseau.

M. Lee explique : « Grâce à la connaissance de la situation, nous savons où nous en sommes. Mais avec la threat intelligence, nous savons aussi qui est notre ennemi. Nous administrons désormais un programme intégré de threat intelligence et notre SIEM Splunk fait partie des éléments clés de la plateforme centralisée de gestion de l'information que nous déployons dans notre centre intégré des opérations de sécurité (ISOC). » **En savoir plus**.

Analyses avancées

L'analyse avancée peut mettre en œuvre des méthodes quantitatives sophistiquées telles que les statistiques, l'exploration de données descriptive et prédictive, la simulation et l'optimisation pour produire de nouvelles informations cruciales. Les méthodes d'analyse avancée incluent la détection des anomalies, le profilage des groupes de pairs et la modélisation des relations des entités.

Tout aussi important, un SIEM orienté analyse doit comprendre des outils permettant de visualiser et de corréler les données, par exemple en cartographiant des événements catégorisés sur une kill chain ou en créant des cartes de chaleur pour mieux appuyer les investigations.

Pour rendre tout cela possible, il faut accéder à une plateforme SIEM employant des algorithmes de machine learning capables d'apprendre par eux-mêmes ce qui distingue un comportement normal d'une véritable anomalie.

Ce niveau d'analyse des comportements doit ensuite être utilisé pour élaborer, valider et déployer des modèles prédictifs. Il doit même être possible d'exploiter un modèle créé à partir d'outils tiers.

Le déploiement d'un SIEM en cloud innovant dote Equinix d'informations de sécurité exploitables

Equinix, Inc. connecte les plus grandes entreprises du monde à leurs clients, leurs employés et leurs partenaires dans 33 marchés répartis sur cinq continents. La sécurité est d'une importance cruciale pour Equinix ; en effet, des milliers d'entreprises dans le monde s'appuient sur ses datacenters et ses services d'interconnexion. Pour obtenir une image unifiée de son infrastructure de sécurité, Equinix avait besoin d'une solution cloud offrant une visibilité centralisée et des fonctions (SIEM). Il fallait en outre que cette solution puisse être déployée facilement et rapidement, sans engager d'importants efforts opérationnels. Depuis qu'elle a déployé Splunk Cloud et Splunk Enterprise Security (ES), Equinix bénéficie de nombreux avantages :

- une visibilité opérationnelle totale ;
- le renforcement de sa position de sécurité ;
- des gains de temps et d'argent.

Visibilité globale sur l'infrastructure avec Splunk Cloud et Splunk Enterprise Security

Avant d'utiliser Splunk Cloud, Equinix était submergée par plus de 30 milliards d'événements de sécurité bruts chaque mois. Avec Splunk ES et Splunk Cloud, l'équipe de sécurité réduit désormais les 30 milliards d'événements de sécurité bruts à environ 12 000 événements corrélés, puis à 20 alertes exploitables : elle bénéficie ainsi d'informations de sécurité utilisables et s'est dotée des fondements d'un SOC dédié.

Maintenant que toutes les données sont agrégées dans la plateforme Splunk, l'équipe de sécurité peut croiser les informations issues de différents systèmes et ainsi investiguer, comprendre et prendre en charge les incidents jusqu'à 30 % plus rapidement qu'avant. « Notre objectif ultime est de protéger nos clients, nos employés et nos données. Avec ES et Splunk Cloud comme plateforme SIEM, les informations dont nous avons besoin sont toujours à portée de main, » explique George Do, Responsable de la sécurité des systèmes d'information d'Equinix.

« À chaque fois que nous avons besoin d'investiguer un incident, il nous suffit d'afficher les données correspondantes dans des tableaux de bord Splunk, ce qui permet à tous les membres de notre équipe de sécurité, comme à l'équipe dirigeante, d'accéder aux informations. Les gains de temps et d'efforts sont considérables, tout comme l'économie de 50 % réalisée sur le coût total de possession (TCO) du système comparé au déploiement d'un SIEM local conventionnel. »

Grâce à Splunk ES, Equinix est désormais armée d'une capacité exhaustive d'analyse de sécurité. Par exemple, lorsqu'un compte utilisateur montre des signes d'activité suspecte, comme la connexion d'un employé local depuis un autre continent, des alertes de haute priorité sont immédiatement déclenchées et envoyées à l'équipe de sécurité. De plus, en utilisant Splunk Cloud, Equinix parvient à empêcher la fuite d'informations commerciales sensibles. En particulier, les administrateurs utilisent des corrélations pour déterminer si un employé sur le départ est susceptible de chercher à voler des données confidentielles. **En savoir plus**.

Détection des menaces avancées

Les menaces de sécurité évoluent constamment. Un SIEM axé sur l'analyse s'adapte aux nouvelles menaces avancées grâce à la mise en œuvre de la supervision de la sécurité du réseau, la détection des points de terminaison, l'isolement des problèmes et l'analyse des comportements, en combinaison les uns avec les autres, pour identifier les nouvelles menaces potentielles et les mettre en quarantaine. La plupart des pare-feux et des systèmes de protection contre les intrusions ne suffisent pas à remplir ces fonctions.

L'objectif n'est pas seulement de détecter les menaces, mais aussi d'en déterminer la portée en localisant la destination possible d'une menace avancée après sa détection initiale, en déterminant comment la contenir et en choisissant les informations à partager.

Bibliothèque de cas d'usage

Non seulement les événements de sécurité évoluent constamment, mais les analystes doivent aussi détecter et prendre en charge les menaces à vitesse réelle. Une solution SIEM axée sur l'analyse renforce la position de sécurité d'une entreprise en proposant du contenu prêt à l'emploi et pertinent. Une bibliothèque de cas d'usage peut également aider les analystes à découvrir automatiquement de nouveaux scénarios d'utilisation et identifier ceux qui s'appliquent à leur environnement en fonction des données assimilées. Cela permet, à terme, de réduire les risques en accélérant la détection et la prise en charge des menaces continues ou récemment découvertes.

SAIC gagne en visibilité et détecte les menaces

Science Applications International Corp. (SAIC) est un leader des services d'intégration technologique spécialisé dans les marchés des techniques, de l'ingénierie et de l'informatique d'entreprise. Forte d'une expertise dans des domaines tels que la recherche scientifique, la gestion de programme et les services IT, SAIC tire la majorité de ses revenus de ses contrats avec le gouvernement américain. La société devait mettre sur pied un centre des opérations de sécurité (SOC) robuste ainsi qu'une équipe de réponse aux incidents informatiques (CIRT) pour se protéger des cyberattaques. Depuis le déploiement de la plateforme Splunk, la société a observé plusieurs avantages :

- l'amélioration de la position de sécurité et de la maturité opérationnelle ;
- plus de 80 % de réduction des délais de détection et de correction des incidents ;
- une visibilité complète sur tout l'environnement de l'entreprise.

Pourquoi Splunk

Après que la société SAIC d'origine s'est divisée en deux entreprises en 2013 pour éviter des conflits d'intérêts organisationnels, la nouvelle SAIC souhaitait mettre un SOC sur pied dans le cadre de son nouveau programme de sécurité. Si elle possédait tous les outils de sécurité dont elle avait besoin, il lui manquait une solution de gestion des événements et des informations de sécurité pour ancrer ses défenses. Le SIEM traditionnel utilisé par l'ancienne société comme outil principal pour les investigations de sécurité souffrait de limitations. SAIC a complété son SIEM avec Splunk Enterprise, en utilisant la plateforme pour la détection des incidents au moyen de recherches de corrélation, ainsi que pour ses investigations. Le personnel des opérations IT de SAIC utilise désormais aussi la solution Splunk pour ses activités de supervision du réseau, de gestion des performances, d'analyse des applications et de rapports.

Quand SAIC a commencé à bâtir son nouveau SOC, la société a décidé de s'appuyer sur Splunk comme plateforme de sécurité unique pour tous ses besoins de type SIEM : détection des incidents, investigations et rapports de supervision continue, alertes et analyses.

Visibilité complète et détection des menaces sur tout l'environnement

SAIC utilise désormais le logiciel Splunk pour superviser son environnement pour toutes les menaces. Dans le SOC, les analystes supervisent des tableaux de bord Splunk personnalisés pour être informés en cas d'alerte ou de signe de comportement anormal ou non autorisé. Ils sont maintenant immédiatement informés des menaces connues avec signature (comme celles qui sont enregistrées par l'IDS ou une solution de détection de malware) et des menaces inconnues (par exemple, une activité atypique provenant d'un compte privilégié).

Les SIEM traditionnels utilisent habituellement des recherches prédéfinies et rigides qui ne parviennent pas à capturer les menaces avancées et génèrent un grand nombre de faux positifs. Avec la plateforme Splunk, les analystes SAIC ont élaboré de nouvelles recherches de corrélation de haute précision pour détecter des menaces et des indicateurs de compromission propres à SAIC, ce qui permet à l'équipe de mesurer et de gérer le risque à haut niveau. Les dirigeants, RSSI inclus, peuvent maintenant consulter des métriques clés en lien avec les activités menaçantes : tendances, emplacement agrégé des sources et indicateurs de compromission apparus récemment. **En savoir plus**.

Architecture

Les menaces d'aujourd'hui exigent une solution souple et évolutive. Une solution SIEM orientée analyse doit pouvoir être déployée localement, dans le cloud ou dans le cadre d'un déploiement hybride. Ce SIEM moderne doit également s'adapter à une entreprise quelle que soit sa taille, et être suffisamment flexible pour évoluer au fil de sa croissance et de la maturation de ses besoins en sécurité.

Aflac adopte la plateforme Splunk pour mettre en place une sécurité axée sur l'analyse

Aflac est la plus grande compagnie d'assurance optionnelle des États-Unis. Face à une augmentation du volume et de la rapidité des menaces de sécurité, Aflac avait besoin d'une approche de la sécurité axée sur l'analyse pour protéger ses clients, ses presque 10 000 collaborateurs et la réputation de sa marque. La société a mis la plateforme Splunk au cœur de son système de threat intelligence (ITS) interne. Depuis le déploiement de Splunk Enterprise Security (ES) et Splunk User Behavior Analytics (UBA), Aflac a observé de nombreux avantages :

- une implémentation complète de niveau entreprise en deux semaines ;
- plus de deux millions de menaces de sécurité bloquées en six mois ;
- 40 heures de gagnées chaque mois par l'élimination d'activités manuelles de collecte des données et de production de rapports, ce qui permet aux équipes de se concentrer sur la supervision proactive et l'analyse de sécurité.

Pourquoi Splunk

À l'heure où Aflac entre sur de nouveaux marchés et propose de nouveaux services, l'entreprise a besoin d'adapter son programme de sécurité en continu pour faire face à l'évolution rapide du paysage des menaces, qui englobe aussi bien l'hameçonnage que des malwares en pleine prolifération. Avant d'adopter la plateforme Splunk, Aflac utilisait une solution conventionnelle de gestion des événements et des informations de sécurité (SIEM), mais l'entreprise avait besoin d'une plateforme de threat intelligence plus robuste pour détecter les pirates et les contrer.

Selon D.J. Goldsworthy, Directeur des opérations de sécurité et de la gestion des menaces pour Aflac, « avec notre précédent SIEM, il fallait avoir une excellente connaissance des données avant de pouvoir passer à l'action, tandis que Splunk permet d'y parvenir très rapidement. Splunk nous a rendus bien plus agiles et nous permet de donner des preuves de valeur à toutes les parties prenantes très rapidement. »

Au départ, Aflac a mis en place Splunk ES pour traquer les menaces. M. Goldsworthy raconte : « Concrètement, notre preuve de concept a été l'utilisation de Splunk pour nos activités de recherche des menaces, et le délai de rentabilité a largement dépassé nos espérances. Nous sommes parvenus à faire des choses extraordinaires dans un délai très court en termes de détection des menaces avancées. Finalement, c'est ce qui nous a décidés à réaliser un investissement bien plus important dans Splunk ES et UBA pour nos différents scénarios de sécurité. »

Retour sur investissement immédiat

D'après M. Goldsworthy, le temps nécessaire pour installer la plateforme Splunk et la rendre opérationnelle pour l'entreprise a été très court : deux semaines seulement. « Nous avons été très surpris, étant donné le volume de sources de données à importer et le nombre de scénarios d'utilisation à mettre en place. Avec Splunk, nous avons vu un retour sur investissement immédiat. »

Aujourd'hui, avec Splunk ES au cœur du centre des opérations de sécurité (SOC) d'Aflac, la société fait gagner du temps à de nombreux employés. M. Goldsworthy indique : « Nous avons calculé que nous gagnons plus de 40 heures par mois grâce à l'automatisation de rapports précédemment manuels. Avec Splunk, il est très facile d'importer les données de différentes sources et de les présenter sous une forme intelligible pour nos interlocuteurs du comité ou les autres responsables. »

Six équipes, composées d'environ 40 personnes, utilisent la plateforme Splunk pour gérer un large éventail de scénarios de sécurité : recherche des menaces, threat intelligence, opérations de sécurité, réponse aux incidents, sécurité des applications, administration de la sécurité et fraude.

« Nous avons d'abord implémenté Splunk pour la threat intelligence puis pour les opérations de sécurité, et quand nous avons vu à quel point la solution était polyvalente, il nous a paru logique de l'appliquer à la fraude, » explique M. Goldsworthy.

Déploiement, opérations et assistance

Il existe une croyance répandue selon laquelle les solutions SIEM peuvent être difficiles à mettre en place, et qu'une fois opérationnelles, elles requièrent une maintenance constante. Un SIEM axé sur l'analyse doit tenir compte du faible nombre d'ingénieurs possédant des connaissances dans le domaine et prévoir, à la place, des fonctions et des tableaux de bord prédéfinis, ainsi qu'une assistance telle que des services professionnels, pour faire face aux problèmes susceptibles de se présenter.

Gestion des logs et des données

Les données de log représentent une archive définitive des activités de toutes les entreprises, organisations et agences, et elles sont rarement exploitées à des fins de dépannage ou pour appuyer les objectifs plus généraux de l'entreprise.

Et face au paysage actuel des menaces, où une attaque peut survenir de partout, toutes les données sont utiles à la sécurité. Les logs d'événements sont souvent le point de départ pour détecter les menaces, automatiser la conformité et prendre une longueur d'avance sur les menaces avancées. Et plus souvent encore, les solutions SIEM ont besoin d'un lieu où stocker des données brutes non structurées qu'elles peuvent ensuite enrichir pour accomplir des tâches comme la recherche de menaces, les analyses avancées et l'investigation des incidents.

3. Les 9 capacités techniques d'un SIEM moderne

Maintenant que vous comprenez les neuf fonctionnalités essentielles d'un SIEM orienté analyse, nous allons plonger au cœur de la technologie sur laquelle il repose, afin de vous aider à bien faire la différence entre SIEM moderne et SIEM traditionnel, SIEM open-source et nouveaux venus sur le marché du SIEM, comme l'UBA.

Le Magic Quadrant annuel de Gartner sur la gestion des événements et des informations de sécurité est une lecture indispensable pour quiconque explore le marché du SIEM. Ce rapport a évolué au fil des ans et englobe désormais les fournisseurs de SIEM open source et de nouvelles technologies comme l'UBA.

Le cabinet d'analyse produit également d'autres rapports sur le SIEM et, dans un mémo d'étude, met en lumière neuf capacités techniques qui différencient un SIEM moderne, comme Splunk peut l'être, de ces autres catégories.

Les neuf capacités techniques qui différencient une solution SIEM moderne des autres catégories plus vastes sont les suivantes :

	SPLUNK	SIEM TRADITIONNEL	OPEN SOURCE	NOUVEAUX VENUS
1. Collecte des logs et des événements	Oui	Oui	Oui	Oui
2. Application en temps réel de règles de corrélation	Oui	Oui	Manuelle	Oui
3. Application en temps réel d'analyses avancées et de machine learning	Oui	Limitée	Manuelle	Oui
4. Analyses historiques à long terme et machine learning	Oui	Limitée	Manuelle	Limitée
5. Stockage des événements à long terme	Oui	Limitée	Oui	Limitée
6. Recherche et rapports sur des données normalisées	Oui	Oui	Oui	Oui
7. Recherche et rapports sur des données brutes	Oui	Complexe	Oui	Complexe
8. Assimilation de données contextuelles à des fins de corrélation et d'analyse supplémentaires	Oui	Limitée	Oui	Limitée
9 Prise en charge de cas d'usage hors du domaine de la sécurité	Oui	Non	Manuelle	Non

1. Collecte des logs et des événements

Une solution SIEM axée sur l'analyse doit pouvoir collecter, utiliser et analyser tous les logs d'événements et en offrir une vue unifiée en temps réel. Cela donne aux équipes IT et de sécurité la possibilité de gérer les logs d'événements depuis un emplacement centralisé, de corréler différents événements survenus sur différentes machines ou plusieurs jours, et d'associer d'autres sources de données comme les modifications de registre et les logs d'événements ISA pour produire une image complète. Les praticiens de la sécurité peuvent également contrôler et produire des rapports sur tous les logs d'événements depuis un même point.

2. Application en temps réel de règles de corrélation

La corrélation des événements est une manière de produire du sens à partir d'un grand nombre d'événements de sécurité puis d'approfondir et de se concentrer sur ceux qui comptent vraiment en établissant des liens entre différents événements.

3. Application en temps réel d'analyses avancées et de machine learning, et 4. analyses historiques à long terme et machine learning

Il existe une forme simple d'analyse qui, dans le contexte d'un SIEM, permet de révéler les motifs remarquables qui se cachent dans les données. Pour les analystes de sécurité, c'est un moyen de rechercher et détecter les menaces avant qu'elles ne se concrétisent ou de mener des investigations.

Selon **une récente étude de Forrester**, 74 % « … des décideurs en technologie de sécurité de l'entreprise font de la supervision de sécurité une priorité élevée ou critique » et « les fournisseurs ajoutent des fonctions d'analyse de sécurité à leurs solutions existantes et les nouveaux éditeurs élaborent des solutions (d'analyse de sécurité) qui exploitent des technologies plus récentes sans s'encombrer des solutions traditionnelles. »

Avec le machine learning, l'analyse des données va encore plus loin. Le ML donne aux entreprises dotées d'un SIEM orienté analyse la possibilité d'utiliser l'analyse prédictive pour produire des informations intelligentes à partir des données historiques. C'est très intéressant pour les professionnels de la sécurité, notamment pour détecter les incidents, prédire et même prévenir les attaques, entre autres.

5. Stockage des événements à long terme

Une solution SIEM axée sur l'analyse est en mesure de conserver les données de log historiques à long terme. Cela permet de corréler les données au fil du temps et de remplir certaines obligations de conformité.

En quoi est-ce important en termes de sécurité ?
La conservation à long terme des données machine permet aux analystes de sécurité d'investiguer et de retracer le parcours d'une intrusion sur le réseau, par exemple.

6. Recherche et rapports sur des données normalisées

La recherche et les rapports de type SIEM permettent aux utilisateurs d'interroger leurs données, de créer des modèles de données et des pivots, d'enregistrer des recherches et des pivots sous forme de rapports, de configurer des alertes et de créer des tableaux de bord faciles à partager.

7. Recherche et rapports sur des données brutes

La recherche et la lecture de données brutes, en termes de SIEM, consiste à recueillir les données de sources variées et à les centraliser au sein d'une solution orientée analyse. Une solution SIEM orientée analyse, contrairement à un système traditionnel, peut assimiler les données brutes de pratiquement toutes les sources. Ces données peuvent ensuite être transformées en informations exploitables, puis en rapports intelligibles qui peuvent être distribués aux personnes concernées directement.

8. Assimilation de données contextuelles à des fins de corrélation et d'analyse supplémentaires

Une fois qu'une solution SIEM orientée analyse a collecté les données, l'utilisateur a besoin de contexte supplémentaire pour savoir quoi en faire et ce qu'elles signifient. Il est impératif de pouvoir faire la différence entre menaces réelles et fausses alertes, et de détecter et de contrer efficacement les véritables problèmes.

Une solution SIEM orientée analyse sait ajouter du contexte provenant de threat intelligence externe, des opérations IT internes et des schémas d'événements. Ces fonctionnalités permettent d'étudier l'environnement en profondeur et de répondre aux menaces en temps réel.

9. Prise en charge de cas d'usage hors du domaine de la sécurité

Autre distinction entre une solution SIEM orientée analyse et un SIEM traditionnel, la possibilité d'exploiter la première pour plusieurs scénarios d'utilisation en dehors de la sécurité, comme les opérations IT.

4. Splunk entre en jeu

Les données sont au cœur de notre monde en évolution constante, et elles sont source d'autant de défis que d'opportunités. Ces défis ne vont que croître avec les changements induits dans nos habitudes de travail par la pandémie de COVID-19 et 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 y a bien une ressource essentielle dans laquelle les entreprises peuvent puiser pour résoudre ces problèmes, ce sont les données. Les entreprises capables de tirer parti de la puissance des données qu'elles créent seront plus efficaces, rentables, innovantes et, au final, mieux protégées.

Chez Splunk, nous avons mis au point la première plateforme Data-to-Everything au monde pour supprimer les obstacles entre les données et l'action. Nous permettons aux entreprises de compter sur les données pour l'ensemble de leurs questions, décisions et actions.

Splunk Enterprise supervise et analyse les données machine de tous les types de sources pour fournir l'intelligence opérationnelle nécessaire pour optimiser les performances de l'IT, de la sécurité et des fonctions de l'entreprise. Grâce à des fonctions d'analyse intuitives, au machine learning, à des applications prêtes à l'emploi et à des API ouvertes, Splunk Enterprise est une plateforme flexible capable aussi bien de traiter des cas d'usage spécifiques qu'être la colonne vertébrale des analyses de toute l'entreprise. Splunk Enterprise :

- collecte et indexe les logs et les données machine de toutes les sources ;
- dispose de de puissantes capacités de recherche, d'analyse et de visualisation accessibles à toute l'organisation ;
- propose un large écosystème d'applications, Splunkbase, qui offre des solutions pour la sécurité, les opérations IT, l'analyse commerciale et bien plus encore ;
- est disponible sous forme de logiciel pour installation locale ou en tant que service cloud.

Splunk comme SIEM

Les solutions de sécurité Splunk ne répondent pas seulement aux critères actuels des SIEM, elles offrent en outre des capacités d'analyse de sécurité qui délivrent le contexte et les informations visuelles à même d'aider les équipes à prendre des décisions plus rapides et plus intelligentes.

Splunk offre plusieurs options pour les entreprises qui cherchent à déployer un SIEM ou à en changer, avec des options d'installation locale, cloud ou hybride.

Les clients peuvent traiter leurs scénarios d'utilisation SIEM de base avec Splunk Enterprise ou Splunk Cloud. Splunk Enterprise et Splunk Cloud sont les plateformes Splunk fondamentales, qui assurent la collecte, l'indexation, la recherche et les rapports (fonctions CLM). Dans le domaine de la sécurité, de nombreux clients de Splunk utilisent Splunk Enterprise ou Splunk Cloud pour bâtir leurs propres recherches de corrélation en temps réel et tableaux de bord pour obtenir une expérience SIEM de base.

Splunk propose également une solution premium, Splunk Enterprise Security (ES), qui prend en charge des scénarios d'utilisation SIEM avancés, avec des tableaux de bord, des recherches de corrélation et des rapports prêts à l'emploi. Splunk ES fonctionne avec Splunk Enterprise, Splunk Cloud ou les deux. En plus de règles de corrélation et d'alerte prédéfinies, Splunk ES contient des fonctionnalités d'examen des incidents et de workflow, ainsi que des flux de threat intelligence tiers qui soutiennent vos investigations. De plus, il existe plus de 300 autres applications de sécurité sur Splunkbase, avec des recherches, des visualisations et des rapports prédéfinis conçus pour des solutions de sécurité tierces spécifiques. Ces applications, utilitaires et extensions prêts à l'emploi offrent des possibilités variées, parmi lesquelles la supervision de sécurité, des pare-feux de nouvelle génération, des fonctions de gestion des menaces avancées et bien d'autres. Et outre l'abondance de contenus prêts à l'emploi et axés sur des scénarios de sécurité spécifiques, les clients peuvent s'appuyer sur l'expertise de l'équipe de recherche en sécurité de Splunk pour faire face à toutes les nouvelles menaces avancées. Elles élargissent la couverture de sécurité et sont fournies par Splunk, les partenaires de Splunk et d'autres éditeurs tiers.

Splunk ES est également un SIEM axé sur l'analyse composé de cinq frameworks différents qui peuvent être exploités indépendamment pour traiter un large éventail de scénarios de sécurité, concernant par exemple la conformité, la sécurité des applications, la gestion des incidents, la détection des menaces avancées et la supervision en temps réel. Une plateforme SIEM pilotée par l'analyse combine le machine learning, la détection des anomalies et les corrélations basées sur des critères, au sein d'une même solution d'analyse de sécurité.

Splunk ES vous permet d'établir visuellement des corrélations entre les événements au fil du temps, et de communiquer des informations sur des attaques multi-étapes. La plateforme permet également aux entreprises de découvrir, de superviser et d'analyser en temps réel les menaces, les attaques et autres activités anormales à partir de toutes les données de sécurité, en les replaçant dans leur contexte métier. Grâce aux analyses avancées, les clients parviennent à accélérer la détection des menaces et la réponse aux incidents sur tout l'écosystème de sécurité.

Splunk Mission Control est une nouvelle solution du vaste portefeuille de sécurité qui augmente et renforce les puissantes capacités de Splunk ES. Cette solution cloud SaaS à l'épreuve de l'avenir vous permet de détecter, gérer, investiguer, traquer, isoler et corriger les menaces et autres problèmes de sécurité de haute priorité sur l'intégralité du cycle de vie de l'événement, le tout à partir d'une même surface de travail.

En intégrant les fonctionnalités de SIEM axé sur l'analyse à une surface de travail commune et unique dans l'industrie, Splunk ES et Splunk Mission Control offrent ensemble à votre équipe les outils fondamentaux pour mieux gérer votre SOC, mener des investigations efficaces et harmoniser les processus, afin de détecter, investiguer et prendre en charge plus rapidement les menaces de sécurité.

Splunk ES fait partie d'un portefeuille de sécurité plus large qui inclut Splunk Enterprise ou Splunk Cloud (plateforme de données centrale), Splunk User Behavior Analytics (fonctionnalités UBA avancées), Splunk Phantom (orchestration, automatisation et réponse de sécurité, ou SOAR), et Splunk Mission Control (surface de travail commune pour la détection, l'investigation et la réponse).

Comment Splunk fonctionne-t-il comme SIEM ?

- Le logiciel Splunk peut être employé pour administrer les SOC (centres d'opérations de sécurité) de toutes tailles.
- Prise en charge d'une gamme complète d'opérations de sécurité informatique : évaluation de la position de sécurité, supervision, gestion des alertes et des incidents, CSIRT, analyse et prise en charge des failles, et corrélation des événements.
- Prise en charge directe des cas d'utilisation du SIEM et des scénarios de sécurité.
- Détectez les menaces connues et inconnues, investiguez les risques, établissez votre conformité et utilisez des analyses de sécurité avancées pour obtenir des informations détaillées.
- Plateforme éprouvée et intégrée d'information de sécurité basée sur le big data.
- Utilisez des recherches ad hoc à des fins d'analyse de faille avancée.
- Possibilités de déploiement en local, dans le cloud et en hybride local et cloud.
- Contenu prédéfini de détection et d'investigation pour les grands fournisseurs de cloud.

Un SIEM pour les gouverner tous

Choisir la bonne solution SIEM peut donner à votre entreprise toutes les chances de réussir à gérer la maturation progressive de ses besoins en sécurité. Splunk ES peut poser les fondations de la refonte intégrale du SOC et de sa préparation pour l'avenir.

Splunk ES devient la pièce centrale de la suite Splunk pour les opérations de sécurité, et réunit les meilleures technologies SIEM, UEBA et SOAR au sein d'une même plateforme, pour armer le SOC nouvelle génération.

Splunk n'offre pas seulement nativement les capacités ci-dessus, il prend également en charge les cas d'usage suivants :

- **supervision :** Splunk Enterprise, Splunk Cloud ou Splunk Enterprise Security
- **investigation :** Splunk Enterprise, Splunk Cloud ou Splunk Enterprise Security
- **automatisation et orchestration :** Splunk Phantom
- **détection des menaces avancées et internes :** Splunk User Behavior Analytics et Splunk Enterprise Security
- **réponse aux incidents :** Splunk Phantom ou Splunk Enterprise Security
- **conformité :** Splunk Enterprise, Splunk Cloud ou Splunk Enterprise Security

InfoTeK et Splunk mettent en place une plateforme d'informations de sécurité pour le secteur public

De nombreuses organisations utilisent un logiciel de SIEM pour superviser, investiguer et prendre en charge les menaces de sécurité. Mais une agence du gouvernement américain était déçue de son système SIEM HP ArcSight. L'agence a fait appel à InfoTeK, un leader de la cybersécurité, des logiciels et de l'ingénierie système, pour remplacer son outil SIEM. Depuis le déploiement de la plateforme Splunk, le client a observé plusieurs avantages :

- le déploiement en un week-end et l'arrêt d'une attaque le jour suivant ;
- la réduction des coûts de support de 75 % ;
- la réduction du nombre total d'outils requis (agrégateurs de logs et solutions de points de terminaison).

Avec Splunk Enterprise et Splunk ES, l'agence est dotée d'un SIEM axé sur l'analyse qui fournit à l'équipe IT des informations de sécurité exploitables à un coût abordable. InfoTeK a déployé Splunk en un week-end pour le client.

La plateforme a donné des résultats dès le jour suivant. L'équipe IT a pu explorer les événements de sécurité et a immédiatement repoussé un vecteur d'attaque.

Jonathan Fair, Responsable senior de la réponse aux incidents et ingénieur en sécurité chez InfoTeK explique : « Ce qui pouvait prendre des heures, des jours voire des semaines avec d'autres produits ou nécessitait de jongler avec différents outils, se fait maintenant en quelques secondes, minutes ou heures avec Splunk. Nous avons pu obtenir un retour sur investissement avant même la finalisation de l'achat du produit parce que le client est parvenu à arrêter une menace qui aurait nécessité une refonte complète du réseau. »
En savoir plus.

Cliquez ici pour découvrir comment InfoTeK a réduit ses coûts de SIEM de 75 %.

SUPERVISION ET SIGNALEMENT	DÉTECTION ET ALERTES	ANALYSES ET INVESTIGATIONS	RÉPONSE ET COLLABORATION	SIEM
Vues et règles prédéfinies	Règles de corrélation, seuils	Analyses, investigations et enrichissement contextuel	Coordination et réponse à l'échelle de l'entreprise	Alertes de gestion SecOps, gestion des incidents, règles basées sur des politiques, règles et analyses de sécurité prêtes à l'emploi

Un département stratégique du gouvernement américain économise 900 000 $ en maintenance de logiciels hérités

Les citoyens n'attendent pas seulement des agences gouvernementales qu'elles dépensent avec sagesse l'argent de leurs impôts : ils veulent qu'elles mettent tout en œuvre pour assurer la résilience de leurs opérations et l'efficacité de leurs services. Un grand département stratégique américain utilisait auparavant HP ArcSight, un outil de gestion des événements et des informations de sécurité qui n'était pas à la hauteur des besoins de l'agence. Depuis que le département l'a remplacé par Splunk Enterprise pour ses activités de sécurité et de conformité, il a observé plusieurs avantages :

- l'économie de 900 000 $ en maintenance de logiciels ;
- l'amélioration de la détection, de la prise en charge et de la correction des incidents de sécurité ;
- les enquêtes de sécurité prennent maintenant quelques minutes et non plusieurs heures.

Approche proactive de la sécurité

M. Margulies et son équipe administrent le SOC du département, composé de 40 analystes qui utilisent Splunk Enterprise pour investiguer les incidents de sécurité, ainsi qu'une vaste équipe IT qui exploite le logiciel à des fins de résolution des problèmes et de rapport. Le reste de leur clientèle se compose des personnes chargées de veiller à la conformité du service aux réglementations de sécurité.

Heartland Automotive protège la réputation de sa marque et sécurise ses données avec la plateforme Splunk

Connue pour ses services de vidange, Heartland Automotive Services, Inc., couramment appelée Jiffy Lube, est la plus grande chaîne de services de lubrification rapide des États-Unis. Heartland Automotive avait besoin d'une plateforme de cybersécurité pour protéger sa marque et sa ressource la plus importante : ses données. Depuis le déploiement de Splunk ES et Splunk UBA comme plateforme SIEM intégrée, Heartland Automotive a observé de nombreux avantages :

- un délai de rentabilité de trois semaines seulement avec la mise en œuvre d'un SIEM et d'une solution de protection contre les menaces internes ;
- la mise en place d'une plateforme d'innovation affichant un TCO inférieur de 25 % ;
- des investigations de sécurité en temps réel et une protection contre les menaces internes.

Les implémentations de SIEM sont souvent complexes, car les grandes entreprises possèdent de nombreuses sources de données et il peut falloir parfois des semaines pour configurer les alertes. Selon Alams, l'équipe de services professionnels de Splunk a entièrement fluidifié tout le processus d'identification des sources de données de l'entreprise, d'élaboration de la conception du SIEM et de configuration des alertes.

Chidi Alams, Responsable de l'IT et de la sécurité de l'information chez Heartland Automotive Services déclare : « Un délai de rentabilité aussi court est un atout majeur : nous avons pu mettre en place une solution de SIEM et de détection des menaces internes en trois semaines seulement, alors que cela prend normalement trois mois. Le Directeur financier et les autres membres de notre équipe dirigeante ont été très impressionnés par cette rapidité : voir cette solution être implémentée quasiment du jour au lendemain leur a donné confiance dans notre capacité à obtenir des résultats rapides. » En savoir plus.

Cliquez ici pour découvrir comment Heartland Automotive a donné un coup d'accélérateur à son innovation en réduisant son TCO de 25 %.

Étude de ROI avec Splunk

On critique souvent les solutions SIEM orientées analyse pour le gros investissement qu'elles représentent. En réalité, cette dépense est une question de point de vue.

Comment évaluerez-vous le coût d'une solution de sécurité axée sur l'analyse après que votre organisation a été victime d'une attaque interne ? Ou du prochain ransomware à faire la une des journaux ?

Il y a un retour sur investissement (ROI) immédiat, qui consiste à éviter les failles et à protéger proactivement votre entreprise contre les acteurs malveillants de l'intérieur et de l'extérieur.

Mais le retour sur investissement du SIEM ne s'arrête pas là.

Un SIEM axé sur l'analyse prend en charge des cas d'usage IT courants comme la conformité, la détection de la fraude, des vols et des compromissions de compte, les opérations IT, l'intelligence des services, la gestion des applications et l'analyse commerciale.

Quand les équipes de sécurité travaillent de concert avec d'autres fonctions IT, la visibilité provenant des autres scénarios d'utilisation vient composer une vue centralisée de toute l'organisation, facilitant la collaboration interdépartementale et renforçant encore le ROI.

La meilleure façon de comprendre le ROI d'une solution SIEM orientée analyse est d'écouter ceux qui en ont déjà une.

L'avenir du SIEM, de l'UBA et du SOAR au sein d'une même plateforme

Tous les SIEM ne sont pas égaux, comme le souligne ce guide d'achat. Une solution SIEM axée sur l'analyse offre des fondations solides pour un avenir sûr avec ses capacités robustes de supervision en temps réel, de réponse aux incidents, de supervision des utilisateurs, d'analyse avancée et plus encore. Mais en réunissant un SIEM axé sur l'analyse aux technologies d'UBA, de détection des menaces avancées et SOAR au sein d'une même plateforme, les SOC sont mieux équipés pour protéger leur entreprise.

Les menaces de sécurité vont continuer de progresser et nous devons être prêts à réagir rapidement. Protégez votre entreprise et renforcez vos cyberdéfenses en optimisant et en modernisant vos données, vos analyses et vos solutions opérationnelles. En dotant vos opérations de sécurité d'une plateforme prête pour l'avenir, vous pourrez gérer les événements de sécurité sur l'intégralité de leur cycle de vie depuis une surface de travail commune, un atout essentiel pour contenir et contrer rapidement les cyberattaques.

Vous voulez en savoir plus sur la solution SIEM orientée analyse de Splunk et découvrir comment elle peut améliorer la position de sécurité de votre entreprise ? **Discutez avec un expert Splunk dès maintenant**.

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

21-13318-Splunk-SIEM Buyers Guide for 2022-WP-108