Guide d’achat des solutions SIEM

Votre guide des solutions de sécurité orientées données et taillées pour un monde hybride

splunk>
turn data into doing®

Sommaire

Face à l'imprévisibilité sans précédent provoquée par la pandémie et les autres perturbations internationales, les deux dernières années nous ont plongés dans la tourmente et ont bouleversé notre façon de vivre et de travailler. Du côté des entreprises, la transformation numérique est passée du rang de priorité à celui d'impératif. Ainsi, la plupart des organisations ont pris en urgence le virage du numérique, mais par nécessité beaucoup plus que par choix. Pour autant, tout n'est pas noir, puisque les changements majeurs ouvrent souvent la voie à l'innovation. De fait, en ces temps incertains, nous n'avons eu d'autre choix que d'innover à vitesse grand V, ce qui a abouti à des innovations stratégiques portées par l'accélération des technologies cloud et la puissance des données.

Ainsi, pour survivre et même prospérer dans ce monde hybride, les entreprises ont désormais besoin de solutions puissantes, flexibles et rapides, exploitant les données. En misant sur une base solide alliant données et technologie, elles se donnent les moyens de parer rapidement à toute éventualité, de protéger leurs organisations contre des menaces qui se renouvellent sans cesse et d'utiliser leurs données pour innover.

Mais toutes les entreprises n'ont pas réussi à tirer parti de la puissance des données. Un phénomène qui s'explique par trois contraintes majeures.

- **Les silos de données :** la multiplication inutile des outils à l'échelle des équipes se traduit souvent par la fragmentation des données et par un manque de visibilité, ce qui génère des inefficacités et des vulnérabilités.
- **Une visibilité insuffisante à l'échelle des processus :** en l'absence de données contextuelles, il est difficile de suivre les processus métier de bout en bout, et donc d'identifier les causes profondes et de trouver des solutions d'optimisation.
- **Des réglementations de sécurité et de conformité :** avec des réglementations en constante évolution dans les domaines de la sécurité, de la confidentialité et de la conformité, il est toujours plus compliqué d'accéder aux données appropriées au bon moment, avec la bonne gouvernance.

Par conséquent, les organisations ont du mal à extraire des informations et à passer à l'action en s'appuyant sur leurs données car ce processus prend trop de temps et nécessite trop de ressources.

Mais votre entreprise peut relever ces défis, rester en sécurité et exploiter la puissance des données en optant pour une solution de gestion des événements de sécurité (SIEM) adaptée, basée sur le cloud et orientée données.

Qu’est-ce qu’un SIEM ?

Un SIEM s’apparente au radar d’un pilote. Tout comme les pilotes, les analystes aux commandes de votre centre des opérations de sécurité (SOC) ont besoin d’un radar pour naviguer en toute sécurité face à ce qui les entoure, ce qui les attend et ce qui pourrait être hors de leur champ de vision. En pratique, une solution SIEM est une plateforme de sécurité qui aide les analystes du SOC à obtenir une vue d’ensemble de l’IT d’entreprise et à repérer les menaces de sécurité qui se cachent dans les recoins des systèmes qu’ils protègent. Sans elle, ils avancent à l’aveuglette.

Si les applications de sécurité et les logiciels système et de sécurité réseau interceptent et consignent les attaques isolées et les comportements anormaux, les menaces les plus graves sont aujourd’hui distribuées et ne peuvent être neutralisées uniquement avec ces outils. Pourquoi ? Parce que les hackers attaquent simultanément plusieurs systèmes et utilisent des techniques d’évasion avancées pour éviter la détection.

Dans le même esprit, les attaquants profitent également des situations stressantes pour exploiter la moindre faiblesse, comme lors de l’adoption immédiate du télétravail pendant la pandémie. Dans le cadre de cette transition opérée en urgence, les équipes SOC ont été chargées d’assurer la sécurité des systèmes, mais sans pouvoir accéder physiquement aux outils et processus de sécurité sur lesquels elles avaient l’habitude de s’appuyer.

C’est à cause de ce type de situations que les solutions SIEM modernes revêtent une importance plus capitale que jamais. Car sans un SIEM adapté, les cyberattaques peuvent s’amplifier et se transformer en incidents catastrophiques que même les meilleurs analystes du SOC ne peuvent anticiper. Résultat, au moment où ces derniers découvrent une vulnérabilité – que ce soit par le biais d’un ransomware ou d’une attaque visant la chaîne d’approvisionnement –, ils ne peuvent que limiter les dégâts et commencer à chercher un nouveau RSSI.

Dans ce guide d’achat, nous verrons ce qu’est exactement un SIEM, à quoi il sert, en quoi il est différent des autres outils et comment trouver la solution SIEM adaptée à votre entreprise.

À quoi sert un SIEM, exactement ?

Pour Gartner, un SIEM est « une technologie qui prend en charge la détection des menaces et la réponse aux incidents de sécurité grâce à la collecte en temps réel et à l'analyse historique des événements de sécurité à partir d'une grande variété de sources de données contextuelles et d'événements ».

Fondamentalement, une solution SIEM aide les analystes du SOC à mieux faire leur travail. Il s'agit d'une plateforme de sécurité qui ingère les logs d'événements et offre une vue unique de leurs données, avec plus de visibilité.

Avec un SIEM moderne, les analystes peuvent surmonter trois défis de sécurité majeurs :

- manque de visibilité sur le statut en temps réel de la sécurité de l'organisation, ce que l'on appelle souvent la posture de sécurité ;
- efforts visant à limiter le nombre de faux positifs concernant les alertes de sécurité transmises aux analystes, à hiérarchiser ces alertes, puis à accélérer les détections et les investigations ;
- manque de flexibilité ou prise en charge insuffisante des différents types d'environnements de déploiement, d'outils technologiques et de threat intelligence.

Alors comment les entreprises tentent-elles actuellement de relever ces défis sans solution SIEM ? Habituellement, elles optent pour des solutions « héritées », des solutions ponctuelles diverses et des outils tels que la technologie de détection et de réponse étendues (XDR). Mais les résultats sont mitigés. Passons brièvement en revue ces options, avant de nous concentrer sur la solution la plus efficace : le SIEM moderne.

Les SIEM d'ancienne génération sont dépassés

La technologie SIEM d'ancienne génération n'est tout simplement pas conçue pour faire face à l'évolution permanente des défis de sécurité. De fait, compte tenu du cloisonnement de leur environnement et de leurs limites en matière d'ingestion de données, les SIEM traditionnels ne sont pas suffisamment rapides pour traiter les requêtes et les investigations et ne peuvent s'adapter aux besoins de l'entreprise.

De nombreux services IT d'entreprise en ont fait la pénible expérience après avoir investi des sommes importantes dans une plateforme SIEM. Ils ont découvert que l'ingestion de données prenait un temps considérable, et surtout, que le système de données sous-jacent utilisé pour créer le SIEM tendait à être statique. Ainsi, bien que divers logiciels sur le marché permettent de collecter, de stocker et d'analyser uniquement les données de sécurité, seuls quelques-uns sont capables de transformer ces données en informations exploitables, et ce n'est pas le cas des SIEM d'ancienne génération.

Autre point bloquant, la rapidité. En cas d'alerte de sécurité, les analystes de votre SOC ne peuvent pas se permettre de perdre du temps et une solution SIEM héritée ne leur permet pas d'analyser les données aussi rapidement que nécessaire.

Pire encore, comme les SIEM traditionnels ne fournissent des informations que sur les données de sécurité, il est difficile de corréler les événements de sécurité avec le reste de l'activité de l'environnement IT. Cela aurait pu fonctionner il y a dix ans, mais pas dans notre monde hybride, où certains employés travaillent à distance, tandis que d'autres apportent leurs propres appareils au bureau, ce qui se traduit par une interconnexion de tout l'écosystème et par la génération d'importants volumes de données, autant d'aspects cruciaux pour la sécurité.

Ainsi, à l'heure où l'adoption rapide des services cloud élargit les vecteurs de menaces, les entreprises doivent désormais superviser l'activité des utilisateurs, les comportements et l'accès aux applications sur les solutions cloud et SaaS stratégiques, et pas uniquement sur site, afin de cerner la portée des menaces et attaques potentielles.

Sept raisons de remplacer votre ancien SIEM

Les entreprises dépendent souvent des architectures datées des SIEM traditionnels, qui utilisent généralement une base de données SQL avec un schéma fixe. Ce type de base de données peut constituer un point de défaillance unique ou présenter des limites en termes de portée et de performances.

1. **TYPES DE SÉCURITÉ LIMITÉS**	Les limites concernant le type de données ingérées génèrent des contraintes au niveau des délais de détection, d'investigation et de réponse.
2. **IMPOSSIBILITÉ D'INGÉRER EFFICACEMENT DES DONNÉES**	Avec les SIEM traditionnels, l'ingestion de données peut être un processus extrêmement laborieux et très coûteux.
3. **INVESTIGATIONS LENTES**	Avec les SIEM traditionnels, les actions de base, telles que les recherches de logs bruts, peuvent prendre plusieurs heures, voire plusieurs jours.
4. **INSTABILITÉ ET ÉVOLUTIVITÉ**	Plus les bases de données SQL sont volumineuses, plus elles sont instables. Les clients sont souvent confrontés à des performances médiocres ou à un grand nombre de défaillances, car les pics d'événements entraînent des défaillances de serveur.
5. **FIN DE VIE OU FEUILLE DE ROUTE INCERTAINE**	À mesure que les fournisseurs de SIEM traditionnels changent de propriétaire, la R&D ralentit considérablement. Ainsi, en l'absence d'investissement et d'innovation continus, les solutions de sécurité ne peuvent suivre l'évolution des menaces.
6. **ÉCOSYSTÈME CLOISONNÉ**	Les fournisseurs de SIEM traditionnels permettent rarement d'intégrer d'autres outils. Les clients sont donc contraints d'utiliser ce qui est inclus dans le SIEM ou d'opter pour des développements sur mesure ou des services professionnels synonymes de dépenses supplémentaires.
7. **DÉPLOIEMENT UNIQUEMENT SUR SITE**	La plupart du temps, les SIEM traditionnels ne peuvent être déployés que sur site, alors même que les professionnels de la sécurité doivent être en mesure d'utiliser les charges de travail cloud, multicloud, hybrides et sur site.

Existe-t-il des solutions alternatives ?

Commençons par comparer les solutions ponctuelles aux plateformes. Les fournisseurs de solutions ponctuelles mentent s'ils vous garantissent des résultats équivalents à ceux obtenus avec une solution SIEM moderne. Généralement, les solutions ponctuelles sont très efficaces pour une ou deux tâches. Mais elles peuvent aussi générer une complexité supplémentaire dans le SOC. De plus, elles exigent une configuration et une gestion supplémentaires, et nécessitent habituellement de s'intégrer à votre pile technologique existante. Ainsi, en l'absence de système centralisé pour interpréter les données de l'entreprise, les analystes de votre SOC avancent à l'aveuglette.

Prenons ensuite le cas du XDR, une solution émergente qui fait beaucoup parler d'elle, mais dont les performances ne sont pas à la hauteur de l'engouement qu'elle suscite. Le XDR est une évolution de la détection et de la réponse sur les points de terminaison (EDR), qui faisait traditionnellement office de source de données supplémentaire pour les solutions SIEM, sans pour autant les remplacer. Bien que le XDR puisse être combiné à un SIEM moderne, seul, il ne suffit pas.

Sans visibilité sur la posture de sécurité de votre organisation, les analystes de votre SOC ont les mains liées. Et étant donné que les analystes SOC compétents sont difficiles à trouver, leur compliquer la tâche est la pire chose à faire. Car le constat est sans appel : la pénurie générale de professionnels de la sécurité n'a fait qu'empirer depuis le début de la pandémie.

Mais revenons-en à notre radar : en l'absence de visibilité, les investigations de sécurité ne peuvent véritablement résoudre les incidents, ce qui provoque au bout du compte une augmentation des vulnérabilités. Ainsi, moins votre entreprise a de visibilité, plus elle est vulnérable à une violation de grande envergure qui peut lui coûter des millions de dollars et entacher durablement sa réputation. Or, aucun PDG ne veut voir le nom de sa société cité par Bloomberg, et aucun RSSI ne veut devoir expliquer comment une telle situation a pu se produire.

D'où vient le SIEM orienté données ?

L'évolution du SIEM illustre la loi du plus fort. Les SIEM hérités étant dépassés et les solutions dernier cri ne permettant de résoudre qu'une partie du problème, le SIEM moderne a dû évoluer vers une solution robuste et analytique pour suivre la sophistication et la rapidité des attaques actuelles.

Aujourd'hui, les analystes du SOC ont besoin d'un moyen simple de corréler l'ensemble des données de sécurité. C'est-à-dire d'une solution qui permet au service IT de gérer facilement sa posture de sécurité. Les analystes du SOC doivent être en mesure d'anticiper les menaces qui pourraient planer et de mettre en place des mesures pour limiter la vulnérabilité de leur organisation en temps réel. Pour ce faire, les entreprises ont besoin de solutions SIEM modernes et orientées données, qui offrent aux analystes une visibilité totale sur les données générées et qui ne fonctionnent pas uniquement avec des données de log et de simples règles de corrélation pour l'analyse des données. Dans ce contexte, les solutions SIEM de référence associent désormais le stockage à long terme des logs d'événements à une supervision en temps réel pour fournir une vue globale de la sécurité de l'organisation.

Les bases du SIEM moderne

Le Magic Quadrant de Gartner sur la gestion des événements et des informations de sécurité s'impose comme une lecture indispensable pour les organisations qui veulent se pencher sur le marché du SIEM. Au fur et à mesure de son évolution, le rapport a élargi la catégorie pour inclure les fournisseurs de SIEM open source et d'autres nouveaux entrants. Dans ces conditions, comment déterminer si une solution sera à la hauteur ou non ?

Dans le rapport « Critical Capabilities for Security Information and Event Management », Gartner met en avant les cinq caractéristiques que seuls les SIEM modernes possèdent.

Les cinq capacités essentielles d'un SIEM moderne

1. **Collecte des logs d'événements de sécurité et de la télémétrie en temps réel pour les scénarios d'utilisation de détection des menaces et de conformité.**
   Une solution SIEM moderne peut collecter, utiliser et analyser des données de log provenant d'un écosystème d'équipes, d'outils, de pairs et de partenaires, conformément aux exigences sectorielles en matière de conformité et de reporting réglementaires, ainsi qu'aux besoins les plus récents en matière de détection des menaces.
2. **Analyse de la télémétrie en temps réel, au fil du temps, pour détecter les attaques et autres activités pertinentes.**
   Un SIEM moderne peut collecter, utiliser et analyser tous les logs d'événements et offrir une vue unifiée de ce qui se passe dans la pile de sécurité en temps réel. Cela permet aux équipes IT et de sécurité de gérer les logs d'événements de façon centralisée, de mettre en corrélation différents événements sur plusieurs machines ou plusieurs jours, et de lier d'autres sources de données, comme les modifications de registre et les logs de proxy ISA, pour obtenir une vue d'ensemble exhaustive. Les professionnels de la sécurité peuvent également effectuer des audits et assurer le reporting sur tous les logs d'événements à partir d'un seul emplacement.
3. **Investigation des incidents afin de déterminer leur gravité et leur impact potentiels sur l'entreprise.**
   Un SIEM peut aussi déterminer la gravité et la probabilité d'incidents potentiels pour chaque problème identifié, et utiliser ces informations pour hiérarchiser et orienter les actions correctives.
4. **Reporting sur ces activités.**
   Un SIEM moderne peut également générer des rapports contenant des informations de sécurité sur n'importe quelle partie de l'infrastructure d'une organisation, ce qui permet de satisfaire les exigences de documentation et de conformité.
5. **Stockage des événements et logs pertinents.**
   Enfin, une solution SIEM moderne peut stocker les données historiques des logs à long terme, ce qui aide les analystes à respecter les exigences de conformité et à mettre en corrélation les données au fil du temps.

Les sept stratégies SIEM incontournables

Voici une nouvelle liste qui a pour but de faciliter votre travail.

Elle présente les sept stratégies clés pour sécuriser votre organisation (et vous explique comment utiliser un SIEM moderne pour les mettre en œuvre) :

1. **Supervision et analyse de la sécurité en temps réel :** détectez et neutralisez les menaces rapidement
2. **Sécurité dans le cloud :** détectez et contrez les menaces dans les environnements hybrides, cloud et multicloud
3. **Réponse aux incidents :** identifiez les incidents lorsqu'ils se produisent, puis suivez, routez et annotez les événements
4. **Threat intelligence :** accédez à des recherches sur la sécurité intégrée au produit concernant les menaces existantes et émergentes
5. **Investigation et analyse des incidents :** optimisez la traque des menaces, limitez le nombre d'alertes et éliminez les faux positifs
6. **Détection des menaces avancées et internes :** améliorez significativement les performances de détection, ce qui libère du temps et des ressources pour cibler les menaces complexes et haute-fidélité
7. **Conformité :** unifiez les trois piliers de la conformité (les processus, la technologie et le personnel) grâce à une meilleure visibilité sur l'ensemble des systèmes et des processus

1. Supervision et analyse de la sécurité en temps réel

Les entreprises doivent pouvoir détecter et neutraliser les menaces en un temps record, indépendamment de la nature et de la gravité de l'attaque. Pour cela, elles ne peuvent faire l'impasse sur la supervision de la sécurité en temps réel qui fait partie des fonctionnalités des SIEM modernes.

Comment est-ce que ça fonctionne ? Pour identifier et repérer différents types de comportement malveillant et/ou anormal, un SIEM récupère et gère des données contextuelles relatives aux utilisateurs, aux dispositifs et aux applications (par exemple, données d'identité et d'actif) à partir d'environnements sur site, cloud, multicloud et hybrides. Toutes les données pertinentes sont ensuite transmises dans un workflow pour évaluer les risques potentiels.

En supervisant et en ingérant des données machine à partir d'un ensemble divers de sources sur différents types de déploiements, les équipes de sécurité disposent d'une vue complète des événements de sécurité potentiels, ce qui facilite la détection et le ciblage des acteurs malveillants. Pour cela, un SIEM de pointe doit inclure une bibliothèque de règles de corrélation personnalisables et prédéfinies, une console d'événements de sécurité qui présente en temps réel les incidents de sécurité, et des tableaux de bord montrant des visualisations en direct des activités menaçantes.

La supervision de la sécurité peut aussi s'enrichir de recherches de corrélation prêtes à l'emploi pouvant être invoquées en temps réel ou selon un planning défini. Ces recherches doivent être accessibles à l'aide d'une interface intuitive qui n'exige pas que les analystes ou administrateurs maîtrisent un langage de recherche. Enfin, un SIEM moderne doit disposer d'une fonction de recherche locale et historique pour faciliter la recherche des données de log et réduire la quantité de trafic réseau accédant aux données de recherche.

2. Sécurité dans le cloud

Au fur et à mesure que votre entreprise se lance dans des initiatives numériques, vous devez porter une attention particulière aux exigences de sécurité générales ainsi qu'aux complexités techniques de la migration dans le cloud. Inévitablement, le passage à une approche cloud-native s'accompagne d'une augmentation considérable des risques pour l'entreprise, en particulier si cette dernière n'est pas à jour sur les contrôles réseau, les systèmes de gestion des accès ou les options de configuration du cloud. À cela s'ajoutent l'expansion de la surface d'attaque et un manque de visibilité qui accroît la probabilité d'une violation de sécurité. Dans ces conditions, la supervision traditionnelle ne suffit pas. Les équipes de sécurité ont besoin des capacités d'un SIEM moderne pour analyser et ingérer des données provenant d'un large éventail de sources, dans tous les types d'environnements, afin d'identifier la localisation et la cause des événements de sécurité.

Comment est-ce que ça fonctionne ? Avec une solution SIEM de pointe, vous bénéficiez d'une fonctionnalité prête à l'emploi de supervision de la sécurité du cloud qui facilite la détection et la neutralisation des menaces dans les environnements hybrides, cloud et multicloud. Elle inclut des règles de détection sophistiquées pour les attaques dans le cloud, ainsi que des outils pour vous aider à tester et à améliorer les détections dans le cloud via des simulations d'attaque.

À l'ère du télétravail, il est impératif de pouvoir capturer et analyser toutes les données du cloud et des points de terminaison, indépendamment de leur volume, de leur variété et de leur vitesse. Au bout du compte, en supervisant la disponibilité et l'activité de plusieurs déploiements cloud avec un SIEM moderne, vous profitez d'une visibilité totale sur les services cloud, tels qu'Amazon Web Services (AWS), Azure et Google Cloud Platform, ainsi que sur toutes les informations exploitables qui en découlent.

Slack libère les données pour renforcer la collaboration

Lorsque la pandémie de COVID-19 frappe, Slack doit faire passer plus de 1 600 employés en télétravail, en continuant à fournir un service sûr et performant à sa base d'utilisateurs en plein essor. Grâce à Splunk, Slack peut migrer en toute transparence ses effectifs dans le cloud, renforcer la sécurité au sein d'un framework Zero Trust et obtenir une visibilité sur toutes les activités de ses services cloud. Slack se sert également de Splunk pour :

- obtenir des informations sur les modèles comportementaux à l'échelle des applications critiques ;
- autoriser et authentifier les utilisateurs au sein d'un réseau Zero Trust ;
- innover et rester en phase avec ses clients tout en garantissant la sécurité.

Un écosystème sécurisé

Face à l'explosion de la demande provoquée par la pandémie, Slack doit s'assurer que son programme de sécurité fonctionne efficacement. Avec l'aide bienvenue de Splunk, l'entreprise lance ainsi une nouvelle interface de programmation (API) et un réseau Zero Trust consolidé.

L'intégration d'une API d'analyse à Splunk se révèle avantageuse à différents niveaux : les utilisateurs peuvent plus facilement suivre l'évolution de l'entreprise, les clients obtiennent les informations dont ils ont besoin et la direction peut rester connectée. Et comme toutes les applications critiques de Slack envoient du contenu de journalisation à Splunk, les données sont centralisées ce qui permet d'obtenir des informations sur divers modèles comportementaux.

Dans le même temps, l'exploitation d'un réseau Zero Trust, où les utilisateurs sont authentifiés et autorisés, renforce la posture de sécurité de Slack. Larkin Ryder explique : « Splunk joue un rôle essentiel dans la capacité de Slack à exploiter un réseau Zero Trust. En effet, Splunk nous apporte une visibilité sur toutes les activités qui se produisent à l'échelle de nos services cloud. »

« C'est avec Splunk que nous vérifions que, sur l'ensemble de notre parc et de nos applications d'entreprise, notre programme de sécurité fonctionne conformément à nos attentes et comme il le faut pour assurer l'intégrité de notre entreprise. »
En savoir plus.

3. Réponse aux incidents

Les entreprises d'aujourd'hui ont également besoin d'une stratégie de réponse aux incidents à jour. Dans cette optique, un SIEM moderne peut vous aider à identifier les incidents lorsqu'ils se produisent et vous fournir un moyen de suivre, de router et d'annoter les événements.

Comment est-ce que ça fonctionne ? Un SIEM peut agréger manuellement ou automatiquement des événements, prendre en charge des systèmes et des fournisseurs tiers (ce qui facilite l'ingestion de données à destination et en provenance de diverses sources) et fournir une threat intelligence à jour ainsi que des capacités de réponse automatique (telles que des procédures) qui évitent ou interrompent les cyberattaques juste avant ou juste après leur apparition.

Pour ce faire, il faut qu'un workflow de réponse aux incidents soit personnalisé et conçu autour du SIEM. Les événements de sécurité étant associés à différents niveaux d'urgence, les menaces potentielles peuvent être identifiées, classées et triées via des tableaux de bord, avant d'être attribuées aux analystes pour examen. De plus, en identifiant, en triant et en auditant les événements notables en fonction de la fidélité de la menace, un SIEM moderne renforce la fiabilité du début du processus de remédiation, ce qui offre à vos équipes la visibilité contextuelle dont elles ont besoin pour déterminer les prochaines étapes.

Afin d'étendre ou de réduire la portée de leur analyse (qui peut être vaste), les analystes de votre SOC peuvent utiliser un SIEM pour appliquer des filtres aux données de log, puis placer des événements, des actions et des annotations dans une chronologie en vue de cerner la situation. Ils peuvent ensuite vérifier et codifier ces chronologies via une méthodologie de kill chain reproductible, pour prendre en charge des types d'événement spécifiques.

4. Threat intelligence

La threat intelligence constitue une autre stratégie indispensable. Mais son interprétation est souvent difficile, car les analystes de sécurité doivent gérer manuellement les données en vue de les utiliser. Et la saisie manuelle s'accompagne de contraintes de taille : le contexte est perdu pendant le processus d'investigation ou les données deviennent trop disparates, tandis que l'enrichissement dans les procédures est trop fastidieux. Pour compliquer encore un peu plus la tâche des analystes, les données de sécurité les plus précieuses se retrouvent souvent dans des silos intra- et inter-entreprises. Et face à la multiplication des intégrations générant davantage de données à sécuriser et à stocker, le problème n'est pas près de disparaître.

Heureusement, grâce à la croissance rapide du marché de l'intelligence, les solutions SIEM modernes peuvent intégrer la threat intelligence à chaque étape du flux de réponse aux incidents, ainsi qu'à un écosystème d'équipes, d'outils, de pairs et de partenaires.

Comment est-ce que ça fonctionne ? La threat intelligence transforme les sources internes et externes de security intelligence afin de mettre en place une automatisation éclairée et exploitable au sein d'écosystèmes d'équipes et d'outils. Cela facilite le partage d'informations avec les parties prenantes internes et externes. Votre équipe peut ainsi éviter les attaques et créer des pipelines complexes sans avoir à écrire ou à gérer des scripts dans le back-end. En pratique, la threat intelligence est intégrée à la plupart des solutions SIEM modernes ou se présente sous la forme d'un SaaS cloud-native qui s'intègre de manière transparente à une plateforme SIEM moderne.

Les informations fournies incluent souvent les indicateurs de compromission (IOC), les tactiques, techniques et procédures adverses, ainsi que du contexte supplémentaire sur différents types d'incidents et d'activité. Il est ainsi beaucoup plus facile de repérer les activités anormales, puisque vos analystes détiennent toutes les informations nécessaires pour évaluer les risques, l'impact et les objectifs d'une attaque, aussi sophistiquée soit-elle, et intervenir en conséquence.

Les données de threat intelligence peuvent être intégrées aux données machine pour créer des listes de supervision, des règles de corrélation et des requêtes, afin d'améliorer la détection et la neutralisation des attaques. Ces informations peuvent être automatiquement corrélées aux données d'événements et ajoutées aux vues et rapports des tableaux de bord, ou bien transmises à des dispositifs capables de résoudre la vulnérabilité en question.

5. Investigation et analyse des incidents

Il est probable que votre équipe de sécurité passe trop de temps à analyser des alertes de faible valeur avec trop peu de contexte. De fait, les incidents basés sur des détections étroitement définies peuvent conduire à un volume élevé de faux positifs qui submerge rapidement les équipes en première ligne. D'où la nécessité d'une solide stratégie d'investigation et d'analyse des incidents, basée sur un SIEM moderne.

Comment est-ce que ça fonctionne ? Un SIEM moderne visualise et met en corrélation les données en mappant les événements classés par catégorie sur une kill chain, ou en créant des heat maps pour mieux appuyer les investigations via la fourniture d'informations importantes sur les tactiques utilisées par un attaquant et alignées sur un framework sectoriel particulier.

L'attribution des risques peut également aider à optimiser la traque des menaces et à réduire le volume des alertes, ce qui augmente les vrais positifs, tout en mettant au jour des menaces plus sophistiquées, comme les attaques discrètes et de longue haleine qui échappent à la plupart des recherches de corrélation. Cela libère du temps et des ressources pour cibler les menaces réelles (souvent complexes), en alignant les opérations sur des frameworks de cybersécurité standardisés.

Résultat, vos analystes peuvent se concentrer sur des tâches de grande valeur et sont donc plus à même d'intervenir rapidement et efficacement en cas de violation de sécurité, ce qui est idéal.

Pour ne rien gâcher, votre équipe peut prendre des décisions plus éclairées et recueillir des preuves d'analyse grâce aux capacités complètes de collaboration et de reporting intégrées à un workflow d'investigation SIEM moderne.

6. Détection des menaces avancées et internes

Les menaces de sécurité continuent d'évoluer, de muter et de trouver des moyens d'échapper aux procédures de sécurité standards. Et plus l'attaque est sophistiquée, plus il est difficile pour votre équipe de la détecter et de la neutraliser. Ainsi, face à l'évolution du paysage des menaces et à la complexité des menaces nouvelles et émergentes, il n'a jamais été aussi crucial de s'appuyer sur une stratégie de détection des menaces avancées et internes.

Mais la plupart des outils de sécurité traditionnels ne sont pas à la hauteur. Ils reposent sur des règles et des signatures existantes et ne peuvent détecter que les menaces simples et bien connues. Ils sont donc dépassés par la sophistication des menaces de sécurité avancées, telles que les menaces internes, les attaques zero-day, le déplacement latéral de malwares et les compromissions de comptes.

Comment est-ce que ça fonctionne ? Heureusement, un SIEM moderne peut s'adapter à ces menaces en reliant les anomalies et en les corrélant dans le cadre du workflow de réponse aux incidents, ainsi qu'en mettant en œuvre des capacités telles que la détection sur les points de terminaison et l'analyse comportementale.

En établissant des références comportementales multidimensionnelles et des analyses de groupes de pairs dynamiques, idéalement en tandem avec du machine learning non supervisé, il est possible de détecter les comptes compromis ou mal utilisés.

L'objectif est non seulement de détecter les menaces dissimulées, mais aussi de déterminer la portée de l'attaque et la meilleure façon de la contenir. Pour cela, votre équipe a besoin de vues en temps réel et de capacités de reporting qui peuvent être étendues pour inclure un nombre illimité d'applications et de services tiers.

Au sein d'un SIEM, ce type d'analyse et de profilage comportemental peut améliorer de façon exponentielle les performances de détection, libérant ainsi du temps et des ressources pour votre équipe, qui peut alors se concentrer sur les menaces complexes et haute-fidélité, avant qu'il ne soit trop tard.

L'événement mondial Expo 2020 Dubaï assure sa sécurité avec Splunk

Garantir la sécurité d'un événement comme l'Expo 2020 est un défi de taille, surtout face aux menaces internes. C'est pourquoi la cybersécurité est depuis toujours une priorité pour l'Expo Dubaï. Mais à l'approche de son prochain événement devant durer six mois, l'organisation décide d'aller plus loin.

Pour dissiper ses inquiétudes croissantes, l'Expo 2020 a besoin d'une plateforme de sécurité capable d'évoluer rapidement, de gérer la sécurité opérationnelle de centaines de sources de données et solutions technologiques différentes, et d'être suffisamment flexible pour s'adapter à l'évolution des besoins de cybersécurité de l'événement. La plateforme Splunk s'avère la meilleure pour satisfaire ces exigences.

Grâce à Splunk, l'Expo 2020 peut :

- superviser, signaler et classer les activités/comportements anormaux ou suspects ;
- répondre immédiatement aux menaces potentielles et mettre en place des mesures correctives ;

faire face aux menaces internes potentielles.

Les événements et les organisations de grande envergure font régulièrement face à un grand nombre d'incidents de sécurité, le principal danger étant désormais les menaces internes. Pour protéger ses écosystèmes technologiques contre des attaquants potentiels, l'Expo s'appuie sur la supervision en temps réel afin d'identifier les comportements suspects.

Splunk aide également l'équipe de l'Expo à prendre des décisions plus rapides et mieux orientées données, à renforcer la cyber-résilience globale et à réagir immédiatement aux menaces à l'aide de mesures correctives.

« Grâce à la flexibilité de Splunk, nous avons pu facilement élargir le déploiement pour répondre à l'évolution des besoins de l'Expo pendant la pandémie, et notamment au report d'un an de l'événement. » En savoir plus.

7. Conformité

Que ce soit pour la cybersécurité, les analyses, la confidentialité, la lutte contre la fraude ou la gestion des risques, différentes équipes ont besoin de vues et de processus différents autour des données afin de garantir la conformité. Dans ce contexte, un SIEM moderne peut unifier les trois piliers de la conformité (les processus, la technologie et le personnel), en fournissant une meilleure visibilité à tous les niveaux.

Comment est-ce que ça fonctionne ? Une solution SIEM moderne adopte une approche globale et fondamentale de la conformité qui relie les équipes de conformité, les silos et les services technologiques, tout en rationalisant également l'efficacité globale des opérations liées à la conformité. Cela signifie qu'on peut tirer un trait sur le fardeau de l'examen des logs. Dans ces conditions, vos analystes peuvent être plus productifs et assurer une approche documentée et stricte de la gestion des risques, conformément à ce que l'on attend d'eux.

Avec un SIEM moderne, les organisations ont accès à l'ensemble de la pile de sécurité pour les évaluations, les classements, les investigations et les audits, et ne dépendent plus d'un seul service ou d'une seule unité fonctionnelle pour obtenir des informations. Vos analystes peuvent ainsi rechercher des données machine et générer des alertes et des rapports à ce sujet à partir d'une multitude de sources. Résultat, ils sont en mesure de répondre aux exigences de conformité liées à la collecte des pistes d'audit et au reporting, tout en produisant des rapports de conformité spécifiques à un secteur en quelques secondes.

Découvrez l'offre de Splunk

Splunk propose une solution SIEM orientée données sur une plateforme de données flexible. Avec Splunk, les organisations peuvent bénéficier d'une visibilité à l'échelle de toutes leurs données, obtenir des informations rapidement et réagir de façon précise et fiable en toute simplicité, le tout grâce à une solution unifiée et intégrée. En un mot, Splunk est le radar indispensable aux analystes pour piloter les activités du SOC.

Splunk peut superviser et analyser les données de n'importe quelle source, à l'échelle de l'entreprise. Cette plateforme offre des solutions intégrées qui garantissent une observabilité cohérente sur toute la pile et une sécurité unifiée, tout en fournissant diverses applications personnalisées. Pour vous, c'est la certitude de pouvoir obtenir des informations exploitables à partir de vos données.

En pratique, une plateforme d'opérations de sécurité orientée données, comme Splunk, conjugue les performances et la flexibilité nécessaires pour relever les défis complexes de conformité et répondre aux menaces afin que votre entreprise puisse se développer et innover en toute sécurité.

En opérant dans des environnements multicloud et hybrides et en fournissant des outils robustes d'investigation, d'analyse et d'orchestration, Splunk aide les organisations à détecter et à corriger les menaces rapidement et avec précision.

Splunk Enterprise supervise et analyse les données machine pour améliorer les performances IT, métier et de sécurité. Grâce à ses fonctions d'analyse intuitives, au machine learning, à ses applications prêtes à l'emploi et à ses API ouvertes, cette plateforme flexible est tout autant capable de traiter des scénarios d'utilisation spécifiques que d'être la colonne vertébrale des analyses de toute l'entreprise.

La plateforme Splunk Cloud est une plateforme de données flexible, sécurisée et rentable, qui aide les organisations à rechercher, analyser, visualiser et exploiter leurs données. En déployant Splunk en tant que service géré de manière sécurisée, fiable et évolutive, vous bénéficiez d'un service rapide et flexible, d'un streaming puissant et intégré, de fonctionnalités de recherche et de machine learning, ainsi que d'une tarification prévisible en phase avec la valeur.

Pour votre SIEM, faites confiance à Splunk

Les écosystèmes technologiques complexes d'aujourd'hui et les menaces de sécurité en constante évolution exigent des opérations de sécurité modernes qui équilibrent efficacement le risque métier avec le risque de sécurité, tout en permettant aux entreprises de s'adapter rapidement.

Dans ce contexte, les solutions de sécurité de Splunk répondent aux besoins SIEM d'aujourd'hui et de demain. Splunk offre une plateforme d'opérations de sécurité qui ingère des données provenant de n'importe quelle source pour une détection précise des menaces, une investigation approfondie et une réponse automatisée dans les environnements cloud, sur site et hybrides. Et comme Splunk s'appuie sur un écosystème ouvert, vous avez la liberté de choisir les meilleurs outils et de capitaliser sur votre infrastructure existante.

La plateforme Splunk est conçue pour ingérer, normaliser et fournir des informations sur l'ensemble de vos données, afin que vous puissiez obtenir des détections précises et exploitables, mener des investigations plus rapides et réduire le temps nécessaire à la remédiation. Ces analyses de sécurité avancées apportent le contexte et les informations visuelles dont votre équipe de sécurité a besoin pour prendre des décisions de sécurité plus rapides et plus éclairées.

Outre une visibilité de bout en bout sur la sécurité, Splunk intègre des capacités d'indexation distribuée et de schéma à la lecture qui permettent de collecter et d'analyser les données de n'importe quelle source de façon simple et rapide. Splunk est également flexible et offre plusieurs options aux organisations qui souhaitent déployer leur SIEM ou migrer à partir de leur SIEM existant, en leur permettant de choisir entre un déploiement sur site, dans le cloud ou hybride.

Pour répondre à vos besoins essentiels, vous pouvez utiliser Splunk Enterprise ou la plateforme Splunk Cloud. Ces deux solutions de base offrent des capacités de collecte, d'indexation, de recherche et de reporting. Parmi les clients de Splunk, nombreux sont ceux qui utilisent l'une des deux plateformes pour créer leurs propres recherches et tableaux de bord en temps réel pour des scénarios d'utilisation basiques dans le domaine de la sécurité. Vous pouvez également tirer parti des solutions de recherche et de reporting, de sécurité et d'observabilité développées par Splunk, ainsi que de l'écosystème Splunkbase qui inclut des milliers d'applications.

Optimisez votre SIEM

Vous avez besoin d'aller encore plus loin ? La solution SIEM nouvelle génération de Splunk, Splunk Enterprise Security (ES), est à la fois rapide, puissante et flexible. Elle fournit des informations basées sur les données pour garantir une visibilité complète sur la sécurité de votre entreprise, protéger vos activités et limiter les risques – et ce, à grande échelle. Et il ne s'agit là que de quelques-uns des atouts grâce auxquels Splunk ES domine le marché du SIEM depuis plusieurs années selon IDC.

Grâce à des capacités inégalées de recherche et de reporting, à des analyses avancées, à une intelligence intégrée et à des fonctionnalités de sécurité prédéfinies, Splunk ES accélère la détection des menaces et les investigations, ce qui vous permet d'évaluer rapidement la portée des menaces prioritaires et d'agir en conséquence. De plus, Splunk ES combine le machine learning, la détection des anomalies et les corrélations basées sur des critères au sein d'une même solution d'analyse de la sécurité et s'exécute sur Splunk Enterprise, Splunk Cloud ou les deux.

Autre avantage, Splunk ES garantit flexibilité et interopérabilité. Basée sur une plateforme de données ouverte et évolutive, cette solution permet aux organisations de rester agiles face à l'évolution des menaces et des besoins métier. De plus, l'écosystème étendu de Splunk et les options de déploiement flexibles garantissent que vos investissements technologiques fonctionnent en tandem avec votre SIEM, tout en vous accompagnant à votre rythme dans votre transition vers le cloud ou vers un modèle hybride.

Avec Splunk ES, vous pouvez établir visuellement des corrélations entre les événements au fil du temps et communiquer des informations sur des attaques multi-étapes. Vous pouvez également facilement détecter, superviser et signaler en temps réel les menaces, attaques et autres activités anormales à l'échelle de toutes vos données de sécurité. En outre, Splunk ES propose désormais de nouvelles fonctionnalités natives d'alerte basée sur les risques et de sécurité dans le cloud, pour vous permettre d'analyser les menaces réelles encore plus rapidement, avec davantage d'informations.

Dans le même esprit, Splunk ES évite à votre équipe de sécurité de perdre son temps à étudier des alertes peu fiables grâce aux alertes basées sur les risques. Cette option permet de réduire le nombre d'alertes reçues, afin que votre équipe puisse se concentrer sur celles qui comptent en vue de détecter les menaces complexes qui seraient autrement passées inaperçues.

Cette fonctionnalité attribue le risque aux utilisateurs et aux systèmes et génère uniquement des alertes lorsque les seuils de risque et de comportement sont dépassés, ce qui limite les faux positifs. Et contrairement à d'autres solutions, les alertes basées sur les risques de Splunk ont également été conçues pour améliorer l'efficacité du SOC et aider les équipes à s'aligner sur les frameworks de cybersécurité standardisés de leur choix.

Pour des scénarios d'utilisation plus avancés, Splunk ES propose des tableaux de bord, des recherches et des rapports prêts à l'emploi et personnalisables. La solution inclut aussi l'examen des incidents, des fonctionnalités de workflow et des flux de threat intelligence tiers afin d'accélérer la détection et l'investigation des menaces.

Cinq problèmes complexes que vous pouvez résoudre avec Splunk Enterprise Security

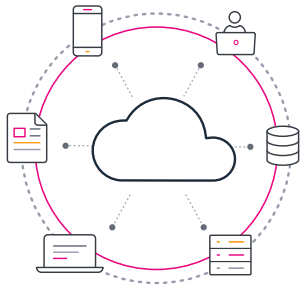
Problème	Solution	Fonctionnement	Avantage pour vous
1. Impossibilité de voir toutes vos données provenant de différentes sources (audit, pare-feu, Windows, Unix, Linux, point de terminaison ou autres logs).	**Supervision et analyse de la sécurité en temps réel**	Place toutes vos données au sein d'une seule plateforme centralisée pour vous permettre de rechercher et d'interpréter ce qui se passe dans votre environnement.	Bénéficiez d'une visibilité en temps réel sur votre posture de sécurité, tout en ayant la possibilité de rechercher, d'analyser et de hiérarchiser les problèmes éventuels.
2. Menaces avancées et internes qui passent inaperçues et compromettent l'équilibre financier et la réputation de votre organisation.	**Détection des menaces avancées et internes**	Les analyses avancées vous aident à détecter les menaces sophistiquées et internes qui échappent aux méthodes de détection traditionnelles.	Évitez les incidents de sécurité de façon rapide et anticipée, avant qu'ils ne provoquent des dommages irrémédiables.
3. Impossibilité d'effectuer des recherches dans les données pendant l'exécution d'une investigation, ce qui est fastidieux.	**Investigation et analyse des incidents**	Vous fournit le contexte complet d'un événement, identifie la cause profonde et assure un reporting et des recherches rapides et flexibles.	Analysez rapidement et facilement les événements de sécurité, trouvez et analysez des données pour obtenir des preuves et évaluez les dommages potentiels.
4. Manque de données centralisées pour l'analyse et les recherches, et manque d'analyses prédictives ou de machine learning qui peut ralentir et compliquer la traque des menaces.	**Traque des menaces**	Assure une traque et une analyse approfondies grâce à des recherches flexibles, au machine learning et à la threat intelligence.	Recherchez de manière proactive les cybermenaces susceptibles d'échapper à la détection.
5. Manque de visibilité et impossibilité d'analyser les contrôles IT et de sécurité, ce qui peut entraîner des violations de la conformité (ainsi que des sanctions et des amendes sévères).	**Conformité**	Effectue une évaluation continue des risques, centralise et analyse les données à l'échelle de l'organisation et fournit des rapports solides pour garantir le respect des normes de conformité.	Confirmez et démontrez le respect effectif des exigences de conformité et des cadres réglementaires.

Un SIEM dans le cloud, pour le cloud

Aujourd'hui, la plupart des organisations ont entamé leur transition vers le cloud. Mais compte tenu du nombre d'outils à gérer sur différents portails et des contraintes liées à la conformité, à la migration et aux offres de services, la supervision de la sécurité dans le cloud peut s'avérer difficile. Pour cela, les équipes de sécurité ont besoin d'outils qui s'intègrent facilement aux fournisseurs cloud. C'est pourquoi Splunk ES inclut des fonctionnalités de supervision de la sécurité du cloud conçues pour simplifier la supervision, où que se trouvent vos données.

Splunk ES intègre des détections et des investigations prédéfinies, spécifiques aux principaux fournisseurs cloud comme Amazon Web Services, Google Cloud Platform (GCP) et Microsoft Azure. Ces fonctionnalités vous aident à superviser les données dans le cloud et sur site, en intégrant de manière transparente les données du cloud à vos workflows existants de détection et d'investigation. De plus, Splunk ES est une solution indépendante qui peut superviser vos données, quel que soit votre fournisseur cloud. Ainsi, vous pouvez choisir le fournisseur d'applications et d'infrastructure IT le mieux adapté à votre entreprise.

Et à l'heure où la plupart des solutions sont proposées « en tant que service », pourquoi votre SIEM ne devrait-il pas lui aussi prendre le virage du SaaS ? Lorsqu'elle est déployée en tant que SIEM cloud via Splunk Cloud, la solution Splunk Enterprise Security permet à votre équipe de se concentrer sur des activités à valeur ajoutée, au lieu de se focaliser sur la maintenance du back-end. Dans le même esprit, Splunk ES sur Splunk Cloud peut évoluer pour superviser des To de données par jour, depuis n'importe quelle source, dans n'importe quelle structure et sur n'importe quelle échelle de temps. Pour vous, c'est la promesse de pouvoir combiner la rentabilité d'un service cloud aux puissantes capacités de pointe dont une entreprise a besoin.



Appuyez-vous sur des bases solides

Splunk ES fait partie d'un portefeuille de sécurité étendu qui utilise Splunk Enterprise ou Splunk Cloud comme plateforme de données de base et offre une gamme de solutions de sécurité pour aider votre équipe à réduire son temps moyen de détection et de réponse aux incidents :

- **Splunk UBA (User Behavior Analytics)** utilise le machine learning pour étendre la détection des menaces avancées et internes ;
- **Splunk SOAR (Security Operation, Automation And Response)** accélère les workflows de sécurité en automatisant et en orchestrant le processus de réponse aux incidents ;
- **Splunk Intelligence Management (intelligence des menaces)** automatise l'orchestration des données pour centraliser, normaliser et hiérarchiser les informations à toutes les étapes des opérations de sécurité.

Une sécurité plus intelligente grâce au machine learning et à l'automatisation

Avec Splunk UBA, l'outil d'analyse du comportement des utilisateurs de Splunk, vous pouvez détecter les menaces inconnues et les comportements anormaux à l'aide du machine learning. La détection des menaces avancées permet de repérer les anomalies et les menaces inconnues qui échappent aux outils de sécurité traditionnels. Le regroupement automatique de centaines d'anomalies sous une seule et même menace permet à vos analystes de sécurité d'être plus productifs. Enfin, des capacités d'investigation approfondies et de puissantes références comportementales sur n'importe quelle entité, anomalie ou menace accélèrent votre traque de menaces.

Spunk SOAR, l'outil de Splunk dédié aux opérations de sécurité, à l'automatisation et à la réponse, permet à votre équipe de travailler plus intelligemment, de réagir plus rapidement et de renforcer les défenses de sécurité de votre entreprise. Il automatise les tâches répétitives afin que votre personnel puisse consacrer son temps et son attention aux actions et incidents les plus importants. Splunk SOAR réduit la durée d'implantation grâce à des investigations automatisées et limite les temps de réponse grâce à des procédures qui s'exécutent à la vitesse de la machine. Cette solution intègre également votre infrastructure de sécurité existante afin que chaque partie participe activement à la stratégie de défense et que toutes les parties fonctionnent ensemble.

Splunk Intelligence Management, l'outil de threat intelligence de Splunk, automatise l'orchestration des données pour centraliser, normaliser et hiérarchiser les informations à toutes les étapes des opérations de sécurité. Il supprime les silos de données pour coordonner l'efficacité de la sécurité par rapport aux objectifs commerciaux, améliorant ainsi la cyber-résilience et l'efficacité opérationnelle. Grâce à Splunk Intelligence Management, votre équipe peut facilement sélectionner des sources d'informations, par exemple, sources open source et premium et collections d'événements historiques et d'alertes. Elle peut ensuite appliquer des scores de priorité, des listes fiables et des filtres basés sur des attributs ou des types d'indicateurs et soumettre des données préparées dans les référentiels de données ou l'application de son choix.

Plus de solutions pour sécuriser et intégrer

Pour Splunk Enterprise Security, il existe également l'application Unified App for Splunk Enterprise and Splunk ES, qui aide les professionnels de la sécurité à analyser les événements notables et à tirer parti des informations pour cerner rapidement le contexte des menaces et hiérarchiser et accélérer le triage. Les analystes peuvent ainsi exploiter les données de Splunk et les enrichir avec les flux de threat intelligence et les données de gestion des cas, afin de décrypter les tendances en matière d'attaque.

Pour plus de moyens d'intégration, Splunkbase propose des milliers d'applications en lien avec la sécurité (ainsi que des milliers d'applications sans lien avec la sécurité), avec des recherches, des rapports et des visualisations prédéfinis pour des fournisseurs de sécurité tiers spécifiques. Ces applications, utilitaires et extensions prêts à l'emploi peuvent aider votre équipe pour la supervision de la sécurité, les pare-feu nouvelle génération, la gestion des menaces avancées et bien plus encore.

Et en plus des nombreuses fonctionnalités prêtes à l'emploi pour des scénarios d'utilisation de sécurité spécifiques, vous pouvez compter sur Splunk SURGe, une équipe dédiée d'experts en sécurité, de chercheurs et de conseillers Splunk spécialistes des menaces, pour vous fournir des recherches, des conseils techniques et des recommandations tactiques sur l'approche à adopter en vue de détecter, d'analyser et de contrer les dernières menaces émergentes.

Enfin, en utilisant la plateforme de données Splunk comme base pour Splunk ES, vous pouvez obtenir des informations et résoudre des problèmes dans d'autres domaines que celui de la sécurité, ces mêmes données pouvant être exploitées pour tous les types d'initiatives IT, DevSecOps et métier.

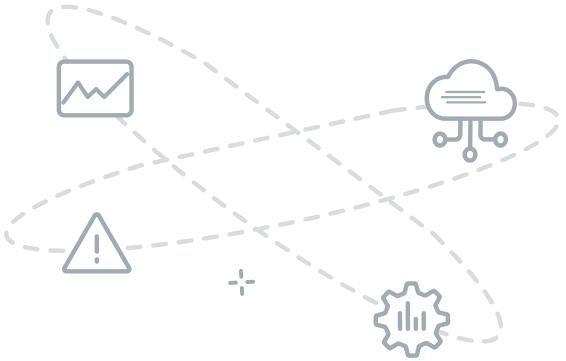
Profitez d'un ROI significatif

Vous vous dites sans doute qu'une solution SIEM moderne et orientée données doit être particulièrement onéreuse. C'est une question de point de vue. Lorsque votre entreprise est victime d'une menace interne, d'une attaque par ransomware ou d'une violation de données, les conséquences financières et réputationnelles sont catastrophiques – ce qui occasionne des dépenses réelles. Si l'on prend en compte le risque associé à ces coûts, il semble plutôt judicieux d'investir dans une solution de sécurité orientée données.

De fait, un SIEM moderne offre un retour sur investissement immédiat en vous aidant à éviter les violations de sécurité et protège de manière proactive votre entreprise des attaquants internes et externes. Mais le ROI ne s'arrête pas là.

Un SIEM orienté données répond à vos besoins de sécurité, tout en prenant également en charge les problèmes IT tels que la conformité, la fraude, le vol et la détection des abus. Il est également utile pour les opérations IT, l'intelligence des services, la livraison d'applications et les analyses métier. Et en se servant de Splunk pour son SIEM, votre équipe de sécurité peut travailler de concert avec d'autres fonctions IT et gagner en visibilité à l'échelle de l'entreprise, favorisant ainsi une meilleure collaboration entre les services et un meilleur retour sur investissement global.

Cependant, pour évaluer le véritable ROI d'un SIEM orienté données, l'idéal reste d'interroger les organisations qui ont adopté une telle solution.



L'université d'État de l'Arizona lutte contre la fraude, protège les salaires et économise 780 000 $ par an

Plus grand établissement d'enseignement aux États-Unis, l'université d'État de l'Arizona (ASU) s'impose comme une référence mondiale de la sécurité dans l'enseignement supérieur. Souhaitant protéger les étudiants et les enseignants contre les menaces telles que la fraude, elle fait confiance à Splunk pour assurer la défense de ses systèmes.

Depuis le déploiement de Splunk, le client observe plusieurs avantages :

- réduction de la fraude à la paie et au virement bancaire pour les plus de 14 600 employés auxquels l'université d'État de l'Arizona verse chaque année 889 millions de dollars de salaires ;
- économies annuelles s'élevant à 780 000 dollars ;
- centralisation des données stratégiques pour améliorer l'expérience des étudiants et des employés.

Si elle exploite Splunk pour la sécurité, l'université d'État de l'Arizona vise également à atteindre un autre objectif crucial : améliorer l'expérience des étudiants et des employés. En se servant de Splunk pour centraliser les données stratégiques à l'échelle du campus, elle bénéficie d'une visibilité sur des systèmes auparavant disparates et peut résoudre les problèmes plus rapidement, optimisant ainsi de façon globale l'expérience offerte aux étudiants.

Regardez la vidéo pour découvrir comment les universités publiques gagnent en efficacité avec Splunk.

ASU Arizona State University

> **« Grâce à Splunk, nous avons désormais de la visibilité sur l'expérience des étudiants et nous pouvons collecter et agréger des données, notamment à des fins de reporting. Nous pouvons ainsi prendre des décisions à un rythme inédit. »**
>
> — Nate Plamondon, Architecte Splunk, Université d'État de l'Arizona

InfoTeK et Splunk mettent en place une plateforme de security intelligence pour le secteur public

De nombreuses organisations utilisent un logiciel SIEM pour superviser, analyser et prendre en charge les menaces de sécurité. Lorsqu'une agence gouvernementale américaine éprouve des difficultés à accomplir sa mission en raison des lacunes de son logiciel SIEM hérité de HP ArcSight, elle se tourne vers InfoTeK, une société leader de la cybersécurité, des logiciels et de l'ingénierie système, pour remplacer son outil SIEM.

Depuis le déploiement de Splunk Enterprise avec Splunk ES, le client observe plusieurs avantages :

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

Avec Splunk Enterprise et Splunk ES, l'agence dispose d'un SIEM orienté données qui fournit à l'équipe IT une security intelligence exploitable à un coût abordable. Il suffit d'un week-end à InfoTeK pour déployer Splunk pour le client.

La plateforme donne des résultats dès le jour suivant, puisque l'équipe IT peut analyser les événements de sécurité et repousser immédiatement un vecteur d'attaque.

Cliquez ici pour découvrir comment InfoTek a réduit ses dépenses SIEM de 75 %.

> **« 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 ROI 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. »**

— Jonathan Fair, Responsable senior de la gestion des incidents et ingénieur en sécurité, InfoTeK

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 le leader américain des centres de services de lubrification rapide. L'entreprise a 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 en tant que plateforme SIEM intégrée, Heartland Automotive bénéficie de nombreux avantages, notamment :

- 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 coût total de possession (TCO) inférieur de 25 % ;
- des investigations de sécurité en temps réel et une protection contre les menaces internes.

Les implémentations SIEM sont souvent complexes, car les grandes entreprises disposent de nombreuses sources de données et la configuration des alertes peut prendre plusieurs semaines. Selon Chidi Alams, grâce à l'équipe de services professionnels de Splunk, Heartland Automotive Services bénéficie aujourd'hui d'un processus plus fluide pour identifier les sources de données de l'entreprise, étoffer la conception SIEM et configurer les alertes.

Cliquez ici pour découvrir comment Heartland Automotive a dopé l'innovation avec Splunk tout en réduisant son TCO de 25 %.

jiffy lube®

« Il est essentiel d'atteindre rapidement la rentabilité. Nous avons pu mettre en œuvre une solution SIEM et de détection des menaces en trois semaines, alors que ce processus nous aurait normalement pris trois mois. »

« Le directeur financier et d'autres membres de l'équipe de direction ont été impressionnés par la rapidité de la rentabilité et par la mise en œuvre de la solution en à peine une journée. Ainsi, ils ont eu d'autant plus confiance en nous pour obtenir des résultats rapidement. »

— Chidi Alams, Chef du service IT et de la sécurité de l'information,
Heartland Automotive Services

Faites le choix d'un SIEM évolutif

Les menaces de sécurité ne vont faire que progresser et le paysage et les systèmes technologiques vont continuer à gagner en complexité. Alors, pourquoi choisir un SIEM qui répond à vos besoins actuels quand vous pourriez opter pour un SIEM taillé pour les défis de demain ?

Une solution SIEM orientée données constitue une base solide pour l'avenir avec des capacités robustes telles que la supervision en temps réel, la réponse aux incidents, la supervision des utilisateurs, les analyses avancées et bien plus encore. Et en combinant dans une seule plateforme un SIEM orienté données avec une détection des menaces avancées et des technologies SOAR, votre SOC est encore mieux armé pour protéger votre entreprise aujourd'hui et demain.

Dans ce contexte, pour contenir et neutraliser rapidement les cyberattaques, il est essentiel de disposer d'une plateforme d'opérations de sécurité évolutive qui permet à votre équipe de gérer les événements de sécurité tout au long de leur cycle de vie, le tout à partir d'une surface de travail commune. Pour votre équipe, c'est la possibilité de répondre rapidement à des menaces en constante évolution et de protéger votre entreprise en optimisant et en modernisant vos solutions de données, d'analyse et d'exploitation.

Splunk développe encore plus de nouvelles capacités de sécurité et d'intégrations pour vous aider à vous préparer à l'avenir – avec notamment une threat intelligence intégrée, des analyses comportementales rationalisées et basées sur le cloud et des alertes avancées basées sur les risques.

Exploitez toute la puissance des données

Votre travail n'a jamais été facile et il est devenu encore plus difficile ces dernières années. Aujourd'hui, il est temps de valoriser vos données grâce à des solutions puissantes, flexibles et rapides.

En s'appuyant sur une base solide alliant données et technologie, votre entreprise se donne les moyens de parer rapidement à toute éventualité. Splunk est la plateforme de données taillée pour les enjeux du monde hybride, qui vous permet de libérer l'innovation, d'améliorer la sécurité et de renforcer la résilience.

Et avec Splunk comme système SIEM orienté données et basé sur le cloud, votre organisation peut bénéficier d'une visibilité sur les sources de données et les processus, suivre les réglementations de sécurité et de conformité et garder une longueur d'avance sur les menaces de sécurité.

Vous êtes prêt à miser sur Splunk pour votre solution SIEM ? En savoir plus.

Lancez-vous.

Vous voulez en savoir plus sur la solution SIEM de Splunk basée sur l'analyse et sur ses avantages pour la sécurité de votre entreprise ? Échangez dès maintenant avec un expert Splunk.

22-23827-Splunk-SIEM Buyers Guide-EB-102

splunk> turn data into doing