splunk>

Le guide Splunk du remplacement de votre SIEM

Sommaire

Splunk Enterprise Security est une solution de gestion des informations et des événements de sécurité (SIEM) de pointe aux fonctionnalités avancées. Splunk dispose d'une organisation de services professionnels dont l'objectif est d'aider les clients à optimiser leur ROI avec Splunk. Après avoir mené à bien des centaines de projets de remplacement de SIEM, nous sommes convaincus que chaque organisation, quelle que soit sa taille et sa maturité, a quelque chose à retirer de ce changement de solution. Dans ce document, nous présenterons :

- les raisons qui pourraient pousser les organisations à vouloir remplacer leur solution SIEM,
- les considérations liées au coût total de possession, au coût total du changement, au délai de rentabilité et la valeur à en retirer,
- les fonctionnalités SIEM avancées de Splunk,
- comment remplacer un SIEM grâce aux bonnes pratiques et à la méthodologie de remplacement de Splunk,
- comment préparer le changement de son SIEM,
- les considérations de design pour le nouveau SIEM,
- les scénarios de remplacement d'un SIEM et les bonnes pratiques spécifiques aux prestataires de services gérés (MSP),
- des témoignages de réussite et les étapes post-changement.

Nous sommes ravis de partager ce que nous avons appris sur le processus et de vous accompagner dans votre démarche de remplacement de solution SIEM.

1. Pourquoi remplacer ma solution SIEM ?

Les opérations de sécurité nécessitent une solution SIEM moderne pour façonner le SOC du futur. Une solution SIEM moderne doit être capable :

- d'offrir une visibilité complète en interprétant le bruit des données,
- d'assurer des détections précises contextualisées,
- d'améliorer l'efficacité opérationnelle grâce à des workflows unifiés de détection, d'investigation et de réponse.

Ces fonctionnalités constituent une base pour réussir à détecter les menaces émergentes et à y répondre. Sans elles, les organisations doivent s'appuyer sur des systèmes de détection ponctuels disparates imposant une quantité de travail manuel intenable.

Si la solution SIEM est si importante, pourquoi la remplacer ?

Il existe de nombreuses raisons pour lesquelles une organisation peut décider de remplacer sa plateforme existante, et la plupart d'entre elles ont trait à la *valeur*. La valeur correspond au rendement de l'utilisation d'une technologie au-delà du montant investi. Si vous dépensez un dollar pour une technologie et obtenez deux dollars en l'utilisant, vous en retirez une valeur d'un dollar. En règle générale, cette décision fondée sur la valeur est le résultat d'une combinaison des facteurs ci-dessous :

- la fonctionnalité du produit,
- le coût total de possession (TCO), en tenant compte du coût total du changement (TCC) et de la concrétisation de valeur,
- la relation avec le fournisseur.

Détaillons chacun de ces facteurs, afin de partir des mêmes définitions.

> *Nous allons réutiliser quelques acronymes à plusieurs reprises tout au long de ce document, mettons-nous donc d'accord sur leur signification avant de continuer :*

- *TCO : coût total de possession*
- *TCC : coût total du changement*
- *ROI : retour sur investissement*
- *TTV : délai de rentabilité*

Fonctionnalité du produit

Ce facteur est relativement explicite. Si votre solution SIEM actuelle est dépassée, son fournisseur n'a probablement pas investi pour garder la technologie à jour, suivre le rythme de l'innovation et l'évolution du paysage des menaces. Elle ne propose peut-être plus les fonctionnalités nécessaires pour atténuer les risques qui pèsent sur votre entreprise. Par ailleurs, une solution maison qui fonctionnait bien lorsque vous étiez une start-up n'est peut-être plus suffisante et vous vous heurtez à ses limites techniques. Quelle que soit la raison, si le produit ne fait plus l'affaire, vous devez commencer à évaluer vos options. Le Magic Quadrant de Gartner, un rapport de recherche annuel sur les fournisseurs de technologie, est un bon point de départ pour la plupart des organisations.

Coût total de possession (TCO)

Le risque est un concept magique. Dans sa forme la plus simple, la théorie du risque métier stipule que si une menace pour votre entreprise présente un dollar de risque matériel, dépenser deux dollars pour atténuer ce risque n'a pas beaucoup de sens. Votre technologie SIEM n'échappe pas à cette logique. Si, sur la base de votre propre analyse des risques, le coût total de possession et d'exploitation d'une solution SIEM est supérieur au prix que vous jugez logique de payer, deux options s'offrent à vous :

- augmenter la valeur (généralement sous la forme d'un montant de risque financier atténué) que votre SIEM fournit, nous aborderons la concrétisation de la valeur plus en détail plus tard ;
- réduire le TCO de votre SIEM.

Vous aurez noté que nous disons « réduire le TCO », et non « réduire le coût de la licence ». En effet, le coût total de possession ne se limite pas au coût de la solution. La manière dont vous calculez le TCO dépend de votre organisation, mais certains facteurs assez courants peuvent entrer en ligne de compte :

- le coût de la technologie,
- le coût humain,
- le coût du traitement.

Attardons-nous brièvement sur ces concepts afin d'avoir une idée de la manière dont il faut envisager le TCO.

Coût de la technologie

Ce facteur est trompeur. Certes, le coût de votre licence SIEM peut sembler élevé, mais il en va de même pour le coût des solutions ponctuelles supplémentaires (pare-feu, protection des endpoints, passerelles de messagerie sécurisées, etc.) dont vous pourriez avoir besoin, en fonction des fonctionnalités manquantes. Il faut également tenir compte du coût des interruptions de service qui surviennent lorsque la technologie ne fonctionne pas comme prévu ou qu'elle est difficile à configurer pour une utilisation efficace des ressources. Il y a aussi le coût humain de l'ingénierie et des intégrations si le ou les produits rendent des tâches telles que l'intégration de sources de données (ou la configuration de nouvelles corrélations) trop longues et fastidieuses – ou pire, si simples qu'elles manquent de fidélité pour apporter une quelconque valeur, ce qui signifie que notre bon vieil ami, le risque, commence à pointer le bout de son nez.

De nombreuses organisations ont l'impression de devoir investir dans différentes technologies afin de réduire le TCO, la consolidation devient donc un élément clé. La consolidation consiste à prendre deux outils, l'outil A et l'outil B, chaque outil couvrant 50 % d'un scénario d'utilisation puis à passer à un outil unique pour couvrir 100 % du scénario d'utilisation en question. Cette solution est presque toujours beaucoup plus rentable et peut être obtenue soit en augmentant la couverture de l'outil A à 100 %, soit en faisant de même avec l'outil B. Il est également possible de passer à un outil complètement nouveau, c'est-à-dire un outil C, qui apporte quelque chose de nouveau. Bien que toutes ces mesures soient susceptibles d'entraîner un certain niveau de coût de changement, cette dépense d'investissement (CapEx) ponctuelle peut souvent être facilement amortie via une réduction à long terme des dépenses d'exploitation (OpEx).

> *Splunk Lantern, le guide de mise en œuvre des scénarios d'utilisation de Splunk est un bon point de départ pour comprendre les scénarios d'utilisation couverts par le portefeuille de sécurité de Splunk grâce à sa fonctionnalité Use Case Explorer. Pour accéder aux corrélations de sécurité, rendez-vous sur le portail de contenu de sécurité* de la Splunk Threat Research Team.

Lorsque vous réfléchissez aux différentes combinaisons de scénarios d'utilisation, tenez compte du fait que les scénarios d'utilisation technologiques existent en dehors du cadre de la sécurité. Si vous pouvez vous procurer un outil capable de soutenir à la fois vos objectifs de sécurité et ceux d'une autre équipe (par exemple ITOps ou observabilité), vous pouvez réaliser des gains substantiels en termes de coût de possession en consolidant les outils et en tirant parti d'une mise en commun efficace des données.

Quelle que soit la manière dont vous calculez le coût de la technologie, les principes suivants peuvent vous aider à prendre une décision :

- considérez les coûts des produits de manière globale, plutôt que de vous concentrer sur le coût d'une seule licence,
- considérez l'impact du coût de la technologie sur le coût humain,
- considérez le potentiel de la consolidation.

Coût humain et de traitement

Les coûts humains et des processus sont étroitement liés, c'est pourquoi nous avons décidé de les regrouper dans une même section. En effet, le coût total du temps d'une personne est étroitement lié au temps qu'il lui faut pour mener à bien un processus, comme le tri des alertes.

Encore une fois, cela peut s'avérer plus compliqué qu'il n'y paraît à première vue. La façon la plus simple d'envisager le coût humain est de considérer le coût du temps d'un analyste SOC. Prenons par exemple le scénario suivant :

- un SIEM émet 1 000 alertes par jour,
- un analyste a besoin de 10 minutes (min) pour trier une alerte,
- un analyste travaille huit heures dans sa journée, soit 480 minutes par jour.

Nous pouvons transposer cela sous forme d'algorithme textuel simplifié :

> *Alertes (1 000) x Temps pour trier une alerte 10 min = 10 000 min*

Si ce qui précède est vrai, cela signifie que dans notre scénario, nous avons besoin de 20,8 analystes pour assurer le tri des alertes pour une seule journée. Par souci de réalisme, disons plutôt 21 analystes.

> *Alertes (1 000) x Temps pour trier une alerte 10 min = 10 000 min*
>
> *10 000 min / 480 (Minutes travaillées par l'analyste) = ~21 analystes par jour*

Si nous avons besoin de 21 équivalents temps plein (FTE) par jour et que le coût journalier d'un analyste est de 500 $, cela signifie que nous devons dépenser 10 500 $ par jour pour assurer le tri des alertes.

Alertes (1 000) x Temps pour trier une alerte 10 min = 10 000 min

10 000 min / 480 (Minutes travaillées par l'analyste) = ~21 analystes par jour

FTE au coût journalier (500 $) x 21 analystes par jour = 10 500 $

Prenons maintenant en compte l'impact des faux positifs ou d'autres facteurs sur ces chiffres. Disons que pour 10 000 alertes, 80 % (8 000) sont des détections basse fidélité. C'est un nombre relativement normal pour une organisation moyenne. Par nature, les détections basse fidélité sont bruyantes et présentent des taux de faux positifs (FP) élevés.
Supposons que le taux de FP pour ces détections basse fidélité soit de 50 % (4 000) des 80 % (8 000) de détections basse fidélité totales, soit 40 % de toutes les alertes quotidiennes totales. Cela signifierait que le calcul ci-dessous est vrai :

40 % de 10 000 = 4 000 FP

4 000 min / 480 (Minutes travaillées par l'analyste) = ~9 analystes par jour

FTE au coût journalier (500 $) x 9 analystes par jour = 4 500 $

Si 40 % de vos alertes sont des faux positifs basse fidélité, vous devriez dépenser 4 500 $ par jour pour trier les faux positifs. La réduction du nombre de faux positifs grâce à des détections d'une fidélité supérieure, ou par exemple via un système d'alertes basées sur les risques (RBA), pourrait donc grandement réduire le coût humain.

Dans le monde réel, le calcul du coût d'un analyste est légèrement plus compliqué que cela. Les analystes n'ont pas tous le même coût, le tri d'une alerte n'est que la première étape d'une chaîne d'investigations possibles et toutes les alertes n'arrivent pas à un rythme régulier, etc. Néanmoins, cela devrait aider à illustrer le concept selon lequel la gestion du coût humain peut jouer un rôle important dans la gestion du TCO.

Vous pouvez appliquer ce même concept de mesure du coût humain aux autres personnes interagissant avec votre SIEM, comme le coût d'ingénierie, qui peut être impacté *négativement* par le coût d'ingestion des données (GDI) – qui est typiquement influencé par la complexité de l'intégration de nouvelles sources de données – ou être impacté *positivement* par la mise en œuvre d'une méthodologie de détection en tant que code (CI/CD) pour gérer efficacement les détections, ou par l'automatisation.

Coût total du changement (TCC)

Le coût total du changement représente tous les coûts encourus lors du passage à une nouvelle technologie telle qu'une solution SIEM. Le coût de la mise en œuvre n'est qu'un des éléments du TCC. La formation et la concrétisation de la valeur sont également des éléments critiques dont il faut tenir compte. Lorsque nous utilisons l'expression « concrétisation de la valeur » dans ce contexte, nous parlons du temps nécessaire pour mettre en œuvre les scénarios d'utilisation qui ont motivé la décision d'achat d'une technologie, comme la mise en place de fonctionnalités de détection et de réponse face à des menaces définies afin d'atténuer les risques métiers.

L'équipe Professional Services de Splunk élabore un plan de mise en place étape par étape couvrant l'implémentation initiale ainsi que la concrétisation de la valeur à long terme. La concrétisation de la valeur est essentielle pour obtenir un retour sur son investissement.

Il est important de comprendre le TCO, car si vous décidez que le meilleur moyen de réduire le TCO est de combiner les scénarios d'utilisation ou de remplacer entièrement une solution SIEM, le processus de migration vers ce nouveau SIEM entraînera un coût. Le temps nécessaire pour que la réduction du TCO soit égale ou supérieure au TCC correspond au temps nécessaire pour obtenir un ROI positif. Par exemple, si votre TCO actuel est de 1 000 000 $ par an, votre TCC pour migrer vers un nouveau SIEM de 300 000 $ et le TCO du nouveau SIEM de 700 000 $, vous récupérerez le coût de la migration au cours de la première année suivant le changement. Vous atteindrez le seuil de rentabilité à la fin de l'année et, à partir de là, votre ROI sera positif. Seule votre entreprise est en mesure de définir le délai nécessaire pour atteindre ce ROI positif.

Vous devez également tenir compte des facteurs ci-dessous :

- Réduire le TCC est une bonne chose, mais seulement dans le contexte du TCO. Il n'est pas logique de réduire le TCC si le TCO ne fait qu'augmenter d'un montant équivalent, puisque le TCO est un coût permanent et le TCC un coût unique.
- Réduire le TCO est une bonne chose, mais si le TCC lié à cette réduction est si élevé qu'il remet en question la migration – *ou* si le délai nécessaire pour atteindre le seuil de rentabilité est si long qu'il n'est pas acceptable pour votre entreprise – alors la migration n'est pas une bonne idée.
- Réduire le TCO tout en conservant un TCC acceptable semble être le juste milieu pour un remplacement de SIEM, notamment lorsque cela s'accompagne d'autres améliorations, telles qu'une meilleure fonctionnalité du produit et une meilleure concrétisation de la valeur.
- Lorsqu'il est question de TCC, tenez compte de la formation et de la concrétisation de la valeur. La mise en œuvre technique d'une technologie sans permettre à vos équipes de l'utiliser, et sans l'appliquer à tout ou partie des scénarios d'utilisation pour lesquels vous avez acheté cette technologie, peut rallonger le délai de rentabilité et entraîner des dépenses supplémentaires. Ne vous focalisez pas sur les coûts, concentrez-vous plutôt sur la valeur créée par vos dépenses.

Relation avec le fournisseur

Lors du choix d'un fournisseur de solutions SIEM, les fonctionnalités du produit et le coût sont des facteurs essentiels. Mais un élément souvent négligé est le type de relation que vous établirez avec le fournisseur avec lequel vous travaillerez. Lors de votre évaluation des différentes solutions SIEM, vérifiez si le fournisseur dispose ou non d'une méthodologie de concrétisation de la valeur basée sur vos besoins organisationnels. Cette méthodologie sera un ingrédient essentiel de la concrétisation de la valeur et de votre ROI.

> *L'équipe Professional Services de Splunk collabore avec les clients pour établir une feuille de route de concrétisation de valeur afin d'accélérer le ROI et d'augmenter la valeur.*

2. Pourquoi Splunk ?

Splunk aide les organisations à devenir plus résilientes. Les plus grandes entreprises utilisent notre plateforme unifiée de sécurité et d'observabilité pour assurer la protection et la fiabilité de leurs systèmes numériques. Les organisations comptent sur Splunk pour éviter que les problèmes de sécurité, d'infrastructure et d'application ne deviennent des incidents majeurs, résister aux effets néfastes des perturbations numériques et accélérer leur transformation numérique. Pour ce faire, Splunk permet aux équipes de sécurité, d'ingénierie et IT de profiter d'une visibilité complète, de processus de détection et d'investigation rapides, ainsi que d'une réponse optimisée, à l'échelle dont ont besoin les plus grandes organisations numériques au monde.

Splunk Enterprise Security

Splunk est un pionnier du SIEM et de l'analyse de sécurité. Nos innovations ont aidé des milliers de clients à prendre une longueur d'avance sur leurs concurrents. En tant que fournisseur de solutions SIEM et d'analyse de sécurité de pointe, seul Splunk a été désigné leader par plusieurs analystes, allant même jusqu'à réaliser un triplé.

Splunk Enterprise Security est la solution de choix pour les SOC du monde entier. Ses fonctionnalités avancées offrent une visibilité complète, permettent des détections précises contextualisées et augmentent l'efficacité opérationnelle. S'appuyant sur une plateforme extensible et des capacités d'assistance basées sur l'IA, Splunk Enterprise Security garantit des analyses à l'échelle nécessaire pour une supervision continue de la sécurité et une optimisation des données rentable. Sur cette base, vous pouvez détecter les problèmes avec précision, mener des investigations complètes et réagir rapidement.

Obtenir une visibilité complète

La plateforme de données de Splunk dotée de capacités d'assistance IA offre une visibilité complète et inégalée en ingérant, en normalisant et en analysant à grande échelle des données provenant de n'importe quelle source en toute fluidité. Elle assure une supervision et une corrélation continues sur l'ensemble des outils de sécurité peu importe le type de déploiement – sur site, cloud ou hybride – pour maximiser la couverture de la surface d'attaque. Détectez les menaces grâce à des recherches exhaustives et utilisez le Splunk AI Assistant pour traduire vos recherches en SPL (Search Processing Language) pour gagner du temps. La fonctionnalité d'actions d'alertes personnalisées de Splunk permet de réagir rapidement en cas d'alerte. Ces alertes personnalisées peuvent être définies à différents niveaux de granularité en fonction de divers facteurs, tels que des seuils de données, des conditions basées sur les tendances et la reconnaissance de modèles comportementaux comme les attaques par force brute et les scénarios de fraude.

Splunk Enterprise Security garantit une optimisation rentable des données en n'ingérant que les données essentielles aux scénarios d'utilisation de sécurité. Les utilisateurs disposent de la flexibilité nécessaire pour stocker et accéder à leurs données, notamment en périphérie du réseau, en fonction du tiering des données. Cela permet de réduire les coûts de stockage liés aux investigations numériques et à la conformité, ce qui se traduit par des économies supplémentaires.

Permettre des détections précises contextualisées

Les alertes basées sur les risques (RBA) au sein de Splunk Enterprise Security réduisent les volumes d'alertes jusqu'à 90 %. La RBA utilise le framework de recherche de corrélation de Splunk Enterprise Security pour collecter et regrouper les événements de risques au sein d'un index de risque unique. Les événements collectés dans cet index créent un seul notable de risque lorsqu'ils répondent à certains critères prédéfinis. Ainsi, vous pouvez vous concentrer sur les menaces imminentes que les solutions SIEM traditionnelles pourraient ne pas détecter. Cela stimule votre productivité et garantit que les menaces que vous détectez sont fidèles.

La Splunk Threat Research Team travaille d'arrache-pied pour créer des techniques de détection, vous offrant plus de 1 700 détections prêtes à l'emploi afin que vous puissiez détecter les menaces et y remédier plus rapidement. Ces détections sont conformes aux frameworks du secteur tels que MITRE ATT&CK, NIST CSF 2.0 et Cyber Kill Chain®. Splunk propose également le Machine Learning Toolkit pour détecter les menaces plus rapidement grâce à la détection des anomalies.
Avec Splunk Enterprise Security, vous pouvez améliorer votre programme de sécurité avec des tableaux de bord, des visualisations et des rapports personnalisables. Vous pouvez par exemple opérationnaliser le

framework MITRE ATT&CK avec une matrice de visualisation qui met en évidence les tactiques et les techniques observées dans les événements de risques afin de gagner du temps lors de vos investigations. De plus, vous pouvez évaluer l'ampleur d'un incident et y répondre avec précision grâce à la visualisation de la topologie des menaces (Threat Topology). Grâce au tableau de bord d'analyse des risques amélioré, les analystes de sécurité peuvent superviser les événements de risque pour l'entité utilisateur à partir des détections effectuées dans le cadre de la RBA et de l'analyse comportementale.

Augmenter l'efficacité opérationnelle

Centralisez les workflows et unifiez les processus de détection, d'investigation et de réponse pour améliorer l'efficacité opérationnelle et empêcher des failles avec Mission Control, une fonctionnalité essentielle de Splunk Enterprise Security. Mission Control unifie vos workflows, renforcés par des playbooks automatisés agrémentés de threat intelligence qui permet de rassemble et de normaliser l'évaluation des sources de données. Cela vous permet de rationaliser les processus SOC dans le respect des modèles prédéfinis afin de réduire les efforts manuels et le besoin de jongler entre des outils disparates.
La plateforme unifiée de Splunk pour l'agrégation, l'analyse et l'automatisation des données vous permet d'augmenter sensiblement votre efficacité opérationnelle. De plus, Splunk est indépendant de tout fournisseur et peut donc prendre en charge un nombre illimité de scénarios d'utilisation, ce qui vous permet de construire ce dont vous avez besoin. Vous pouvez tirer parti d'un réseau de plus de 2 200 partenaires pour créer des applications personnalisées et les intégrer à vos outils existants. Vous pouvez également accroître l'efficacité de votre SOC en collaborant avec la communauté Splunk Answers et en exploitant les plus de 2 800 applications développées par les partenaires et la communauté Splunkbase.

Garantir le respect des risques réglementaires

Les exigences de conformité devenant de plus en plus complexes, Splunk vous permet de collecter, interroger, superviser et analyser les données à l'aide d'une solution centralisée. Vous pouvez rapidement répondre aux exigences en matière de gestion et de stockage à long terme des logs et utiliser les applications de conformité Splunk – PCI, GDPR, Essentials for Industrial Control Systems et bien d'autres – pour connaître l'état de conformité de votre organisation.

Notre suite de produits respecte les différentes exigences du SOC du futur, y compris celles indiquées ci-dessus. Ces produits incluent :

- Splunk Enterprise : notre plateforme d'analyse des données et d'investigation
    - Plateforme évolutive d'analyse des données ; prend en charge les scénarios d'utilisation IT, de sécurité et de fraude dans le cadre d'architectures Zero Trust.
    - Capacité à ingérer un large éventail de données structurées et non structurées.
    - Écosystème de partenaires complet, comprenant des solutions Zero Trust pour soutenir l'intégration et la normalisation rapides des sources de données.
- Splunk Enterprise Security : gestion des événements et des informations de sécurité (SIEM)
    - Bibliothèque étendue de scénarios d'utilisation pour la supervision et la détection de la sécurité, prise en charge par Splunk Security Essentials (SSE) et Enterprise Security Content Update (ESCU).
    - Frameworks clés pour soutenir l'enrichissement et la contextualisation des données d'actifs et d'identités, l'évaluation des risques et la posture de sécurité pour soutenir les objectifs de Zero Trust.
    - Les alertes basées sur les risques (RBA) permettent une évaluation avancée des risques et des détections multi-indicateurs conformes au framework MITRE ATT&CK. Elles recherchent

dans les contrôles Zero Trust une séquence d'activités susceptible d'indiquer un comportement malveillant.

- Splunk User and Entity Behavior Analytics (UEBA)
    - Machine learning autonome prêt à l'emploi pour la détection comportementale avancée et la résolution automatique des problèmes d'identité
- Splunk SOAR : orchestration, automatisation et réponse de sécurité (SOAR)
    - Gestion complète des cas, investigation des incidents, orchestration et automatisation pour répondre aux incidents de sécurité et de service dans le cadre d'une architecture Zero Trust.

3. Remplacer une solution SIEM traditionnelle par Splunk

Il n'y a jamais eu de meilleur moment pour troquer votre SIEM traditionnel contre un SOC du futur. Splunk Enterprise Security, la solution SIEM phare de Splunk, est au cœur de la suite de sécurité de Splunk. Elle offre des fonctionnalités et des capacités puissantes permettant de réduire délai de rentabilité.

Scénarios d'utilisation prêts à l'emploi

Splunk Enterprise Security est livré avec plus d'un millier de scénarios d'utilisation prêts à l'emploi (OOTB), associés à des détections de menaces et des mises à jour de contenu de Splunk Security Essentials, conformes aux frameworks de détection modernes tels que MITRE ATT&CK. Splunk Enterprise Security, associé à Splunk Professional Services, facilite le mappage des scénarios d'utilisation SIEM existants avec ces scénarios d'utilisation prêts à l'emploi et permet une rentabilisation extrêmement rapide.

Alertes basées sur les risques

Les alertes basées sur les risques (RBA) permettent aux équipes de passer de fonctions traditionnellement réactives à des fonctions proactives dans le SOC. À mesure que la fidélité des alertes et les taux de vrais positifs augmentent, les ressources des analystes peuvent être transférées vers des tâches à plus forte valeur ajoutée comme la chasse aux menaces ou la simulation d'adversaires, ce qui permet aux SOC de renforcer les compétences de leurs analystes et de les préparer à toutes les menaces qu'ils pourraient rencontrer.

La méthodologie de la RBA est très similaire à votre mode opératoire actuel dans Splunk Enterprise Security. Elle utilise pratiquement tous les frameworks existants dans Splunk Enterprise Security, mais elle inclut quelques optimisations qui augmentent drastiquement l'efficacité et la maturité de votre posture de sécurité au sein du SOC.

Voici les principaux avantages de la RBA :

- gain de temps pour se consacrer à des activités à forte valeur ajoutée au sein de votre organisation de sécurité telles que la chasse aux menaces, la simulation d'adversaires et le développement de contenu de sécurité,
- conformité aux frameworks de cybersécurité tels que MITRE ATT&CK, la Lockheed Martin Kill Chain et CIS2,
- respect et dépassement des exigences des audits de sécurité, ce qui se traduit par une période d'audit beaucoup plus sereine,
- réduction du volume d'alertes basse fidélité et chronophages de 50 à 90 %.

Gestion du TCC et du TCO avec la RBA

La RBA peut aider les équipes SOC à réduire le nombre d'alertes qu'elles ont à traiter et à reprendre le contrôle. Si vous avez suivi les exemples que nous avons donnés dans la première section pour calculer le coût d'une alerte, vous pouvez probablement deviner que l'utilisation de la RBA pour gérer et consolider les alertes basse fidélité en détections haute fidélité contribuera à réduire rapidement et considérablement les dépenses d'exploitation du SOC, ce qui entraînera une baisse du TCO.

En revanche, ce que vous n'avez peut-être pas envisagé, c'est que la mise en œuvre d'un système d'alertes tel que la RBA peut également faire baisser le TCC. En effet, elle offre un framework permettant de tester et de promouvoir rapidement de nouvelles recherches de corrélations avec des enjeux beaucoup plus faibles.

Exemple de RBA

Prenons l'exemple suivant. Dans un cadre de corrélation standard où une détection équivaut à une alerte, une valeur spécifique sera appliquée à un événement de sécurité pour créer un déclencheur. Cela signifie que si vous créez une détection pour les échecs de connexion, vous pouvez configurer le seuil de déclenchement A pour déclencher une alerte après cinq échecs et le seuil de déclenchement B pour déclencher une alerte après dix échecs. Si un utilisateur ou un ordinateur ne parvient pas à se connecter six fois avec le seuil A, une alerte sera créée pour cet événement. En revanche, si le seuil B est appliqué, aucune alerte n'est générée, même en cas d'attaque probable.

Les enjeux sont élevés : si le seuil d'alerte est trop élevé, les faux négatifs seront fréquents, mais si le seuil est trop bas, les analystes seront submergés de faux positifs.

Heureusement, avec la RBA, vous pouvez rapidement itérer sur les alertes en fonction du risque correspondant. Par exemple, si un score de risque faible est attribué à une alerte via le framework F de Splunk, la plupart des événements associés aux faux positifs n'iront pas dans la file d'attente de votre analyste. Plus vous gagnerez en confiance dans la fidélité et la pertinence de l'alerte et dans la précision de la configuration du seuil, vous pourrez augmenter le score de risque en fonction de vos besoins. Une fois que vous aurez compris les risques métiers et le modèle de menace, vous pourrez commencer à utiliser des modificateurs de risque pour appliquer un multiplicateur à votre génération de risque en fonction de l'importance de l'utilisateur ou de l'ordinateur ciblé.

Résumé de la RBA

La RBA vous permet de réduire le TCO et le TCC lors du remplacement d'un SIEM en vous permettant de transformer les alertes basse fidélité en méta-alertes agrégées haute fidélité. Vous réduisez ainsi le nombre d'alertes à trier pour vos analystes et permettez à votre équipe d'ingénierie de sécurité de mettre en œuvre les scénarios d'utilisation dont votre entreprise a besoin pour générer de la valeur plus rapidement.

> *Pour en savoir plus sur la RBA, lisez notre e-book Le Guide essentiel des alertes basées sur les risques (en anglais).*

Gestion des incidents

La gestion des incidents fait référence à la capacité à gérer les alertes dans un système de tickets. Cela permet aux analystes et aux autres parties prenantes de collaborer facilement sur les investigations, d'assigner les tickets, d'établir des rapports et de documenter les résultats des investigations.

En termes de fonctionnalités, un tableau de bord de gestion des incidents détaillé permet aux analystes de travailler à partir d'une vue unifiée sans avoir à passer d'un écran et d'un outil à l'autre. Il existe également un haut degré de cohésion avec les autres outils utilisés dans le SOC, notamment Splunk SOAR et UBA.

En termes de coût, la gestion des incidents permet à un analyste d'utiliser une plateforme unique, plutôt que des systèmes de tickets externes, ce qui contribue à réduire le TCO d'une plateforme SIEM. Cela est dû à la fois à la réduction des coûts de licence grâce à l'utilisation d'un seul outil et à la réduction des coûts d'ingénierie liés à l'intégration continue entre plusieurs systèmes.

Splunk Security propose des options de gestion des incidents qui peuvent aboutir à de meilleurs résultats et permettre d'utiliser un outil unique en fonction de votre workflow de gestion des incidents préféré.

Splunk Enterprise Security et Splunk SOAR

Splunk Enterprise Security intègre le tableau de bord Incident Review pour la gestion des incidents. Splunk SOAR fournit également son propre tableau de bord de gestion des cas. Ces deux tableaux offrent de nombreuses fonctionnalités et peuvent ajouter une valeur significative en fonction du modèle d'exploitation de SOC préféré de votre organisation. Splunk SOAR peut exister dans le back-end pour assurer uniquement des fonctions d'automatisation (« mode headless ») ou devenir le système de gestion des incidents de prédilection d'un SOC orienté SOAR, en ingérant directement les alertes de Splunk Enterprise Security.

Mission Control est une fonctionnalité de Splunk Enterprise Security pour les utilisateurs cloud du monde entier et offre une expérience unifiée, simplifiée et modernisée des opérations de sécurité pour votre SOC. Mission Control offre le meilleur compromis entre les deux solutions grâce à une vue centralisée sur un même écran de Splunk Enterprise Security et Splunk SOAR. Cette intégration fluide réduit le temps que les analystes passent à obtenir les informations dont ils ont besoin en proposant un environnement de travail unique pour détecter les problèmes avec précision, mener des investigations complètes et réagir judicieusement, et en contextualisant les événements afin de réduire le temps de suivi des investigations. Comme le portefeuille de sécurité de Splunk s'appuie sur l'automatisation pour enrichir les événements et automatiser les actions, l'utilisation de Splunk pour la gestion des cas peut réduire le TCO en diminuant le temps passé à réaliser des tâches d'analyse manuelles et rébarbatives à faible valeur ajoutée.

> *Splunk Professional Services peut vous aider à créer l'approche de gestion des cas la plus adaptée à votre organisation et vous assister dans la documentation des workflows et des runbooks des analystes nécessaires à l'utilisation de votre nouvelle plateforme SIEM. Cela permet de gérer le TCC lié au passage à un nouveau workflow de gestion des cas.*

Automatisation

Intégration native à Splunk SOAR

Splunk SOAR est la solution d'orchestration, d'automatisation et de réponse de sécurité de Splunk. Splunk Enterprise Security s'intègre nativement à Splunk SOAR. Cela signifie que la configuration et la mise en œuvre de Splunk Enterprise Security et de Splunk SOAR sont rapides et faciles.

Actifs et identités

Splunk Enterprise Security comprend plusieurs frameworks, dont le framework Asset and Identity (A&I).

Splunk Enterprise Security utilise un système d'actifs et d'identités pour corréler les informations sur les actifs et les identités avec les événements afin d'enrichir et de contextualiser vos données. Ce système utilise des informations provenant de sources de données externes pour renseigner des lookups, c'est-à-dire des ensembles de données de référence stockées dans Splunk, qu'Enterprise Security met en corrélation avec les événements au moment de la recherche. Cette capacité à utiliser des informations

contextuelles au moment de la recherche améliore drastiquement la contextualisation et la fidélité des alertes.

Threat Intelligence

Un autre framework de Splunk Enterprise Security est le framework Threat Intelligence (TI).

En tant qu'administrateur de Splunk Enterprise Security, vous pouvez corréler des indicateurs d'activité suspecte, des menaces connues ou des menaces potentielles avec vos événements en ajoutant de la threat intelligence à Splunk Enterprise Security. L'ajout de threat intelligence améliore les capacités de supervision de vos analystes et contextualise leurs investigations.

Splunk Enterprise Security intègre une sélection de sources de threat intelligence. Il prend également en charge plusieurs types de threat intelligence afin que vous puissiez ajouter votre propre threat intelligence.

Cette capacité à ingérer nativement un ensemble de sources de threat intelligence signifie que vous pouvez intégrer vos abonnements existants de threat intelligence et facilement importer des données open source pour adapter vos corrélations au modèle de menace de votre organisation, garantissant ainsi une rentabilisation rapide de vos flux de threat intelligence.

Splunk Machine Learning Toolkit

Splunk Enterprise Security utilise l'application Splunk Machine Learning Toolkit pour aider vos data scientists et vos ingénieurs en sécurité à développer et à rapidement mettre en œuvre un machine learning de pointe. Le Splunk Machine Learning Toolkit est disponible pour les utilisateurs de Splunk Enterprise et de Splunk Cloud Platform via Splunkbase. Il agit comme une extension de la plateforme Splunk et inclut des commandes de recherche SPL de machine learning, des macros et des visualisations.

Splunk Security Essentials

Pour garantir un retour sur investissement rapide de votre solution SIEM avec Splunk, Splunk propose une application gratuite. Splunk Security Essentials vous permet d'associer vos besoins métiers et vos sources de données à la bibliothèque de plus de 1 700 détections de sécurité prêtes à l'emploi de Splunk en toute simplicité.

L'équipe Professional Services de Splunk utilise Splunk Security Essentials dans ses ateliers de scénarios d'utilisation. La fonctionnalité de l'application vous permet de vous approprier et d'itérer sur ces résultats ou d'utiliser vos propres scénarios comme base d'analyse.

4. Que puis-je faire aujourd'hui pour préparer le remplacement de mon SIEM ?

Vous avez donc décidé de remplacer votre SIEM. Parfait ! Si vous hésitez encore sur le choix du fournisseur et que vous attendez le bon moment dans le cycle budgétaire de votre organisation, il y a encore de nombreuses étapes que vous pouvez et devez même entreprendre avant de vous lancer dans le remplacement de votre SIEM. Dans cette section, nous aborderons des éléments clés à prendre en compte pour le remplacement de votre SIEM.

Faire le point sur vos besoins

C'est le moment idéal pour réfléchir à vos besoins. Que ce soit dans votre appel d'offres SIEM ou pendant vos conversations avec les fournisseurs, vous devrez préciser ce que votre future solution doit être capable de réaliser pour atteindre vos objectifs métiers.

Voici une liste pour vous aider à commencer à réfléchir à vos besoins en matière de SIEM.

- Quels sont vos besoins fonctionnels ? Quels problèmes métiers cherchez-vous à résoudre et quelles sont les fonctions du SIEM de remplacement que votre SIEM actuel n'assure pas ?
- Quels sont vos besoins non fonctionnels ? La disponibilité, la fiabilité, l'évolutivité, etc. dont vous avez besoin afin d'avoir une solution résiliente conforme aux limites de risques acceptées par votre entreprise ?
- Quelles sont vos échéances ? À quelle date votre nouveau SIEM doit-il être opérationnel ? Votre licence actuelle arrive-t-elle à échéance ou souhaitez-vous vous séparer d'un MSP ?
- Quels sont les scénarios d'utilisation métiers que vous souhaitez prendre en charge ? Les scénarios d'utilisation techniques proviendront-ils de votre ancien SIEM ou ferez-vous table rase du passé ? La création d'un inventaire des scénarios d'utilisation que vous prenez actuellement en charge servira de base à vos futurs exercices de mappage de vos scénarios d'utilisation.
- Aurez-vous besoin d'autres technologies de sécurité à l'avenir, telles que le SOAR ? Envisagez les besoins futurs potentiels de votre entreprise, plutôt que de vous limiter à vos besoins actuels.
- Quelles sont vos principales sources de données ? Si vous vous associez à Splunk Professional Services pour planifier votre mise en œuvre, ils devront connaître vos principales sources de données ainsi que les scénarios d'utilisation métiers afin d'optimiser votre stratégie d'intégration.
- Quels sont vos volumes de données ? Le fait de pouvoir partager ces informations avec les fournisseurs de la manière la plus précise possible vous permettra d'obtenir rapidement des estimations précises concernant les coûts de licence.
- Quelles sont les exigences réglementaires que vous devrez respecter avec votre nouvelle solution ? L'une d'entre elles impose-t-elle de conserver les données pendant une certaine période ?
- Quelles sont les intégrations nécessaires avec vos autres technologies ? Si vous vous associez à Splunk Professional Services, ils devront comprendre vos intégrations pour planifier avec précision votre mise en œuvre.

Identifier les parties prenantes

À mesure que vous évaluez vos besoins, vous identifierez inexorablement d'autres parties prenantes. Il s'agit de toutes les personnes et équipes qui ont un intérêt à utiliser votre solution SIEM. Certaines de ces parties prenantes sont évidentes, comme votre décideur en matière de budget et votre responsable de la sécurité. Certaines le sont un peu moins, comme les équipes qui peuvent vouloir utiliser votre nouvelle solution SIEM dans le cadre d'autres scénarios d'utilisation, dans le but de réduire le TCO et de l'optimisation des dépenses. Si d'autres parties prenantes seront amenées à utiliser conjointement la plateforme, commencez à réfléchir à la manière dont l'utilisation sera partagée ou priorisée.

Définir votre budget

Après avoir fini d'évaluer vos besoins et identifié vos parties prenantes, vous devez définir votre budget. Cela vous aidera à définir une stratégie appropriée de tiering, de routage et de filtrage des données, et aidera votre fournisseur à déterminer la solution la plus rentable pour votre entreprise.

Impliquer l'équipe Splunk

Il n'est jamais trop tôt pour commencer à discuter avec les fournisseurs. En impliquant Splunk dès le début, vous pouvez vous assurer d'avoir une bonne compréhension des technologies disponibles et de pouvoir prévoir avec précision le coût potentiel de votre nouvelle solution.

5. Business case : gérer les coûts de la transition

Introduction

Le coût total du changement, ou TCC, correspond au coût de toute transformation. Lors du calcul de l'investissement dans une nouvelle technologie, le coût du changement est pris en compte dans le TCO sur une durée pertinente, généralement de trois ou cinq ans. Si la mise en place d'une technologie coûte 100 000 $ la première année, mais qu'elle permet d'économiser 70 000 $ par an sur cinq ans, il est logique que l'entreprise accepte ce TCC.

Coût du changement par rapport au nouveau coût d'exploitation

Le TCC correspond au coût total pour effectuer un changement. Le coût d'exploitation de votre nouvelle solution correspond au coût que vous prévoyez d'engager une fois le changement effectué – ici, une migration vers un nouveau SIEM. Lors de l'analyse de rentabilité d'un coût de changement potentiel, vous devez le comparer au nouveau coût d'exploitation de la solution envisagée.

En règle générale, les projets de transformation tels que la mise en œuvre d'un nouveau SIEM sont considérés comme des dépenses d'investissement, tandis que la licence d'abonnement et les coûts de maintenance du SIEM, une fois mis en œuvre, seront considérés comme des dépenses d'exploitation.

Votre organisation peut considérer le coût du changement comme une dépense d'investissement ou une dépense d'exploitation. Travaillez avec votre fournisseur pour comprendre comment les coûts des licences ou des services peuvent être intégrés dans le budget de votre organisation.

Calculer le coût de changement potentiel

Pour définir avec précision le coût du changement, vous devez d'abord avoir une idée claire de vos besoins.

Les éléments faisant partie du coût de changement peuvent inclure :

- le coût de la reformation de vos analystes et ingénieurs de sécurité afin qu'ils puissent travailler avec votre nouveau SIEM,
- le coût de tout service professionnel nécessaire à la conception, à la mise en œuvre et à la personnalisation de votre nouveau SIEM,
- le coût de toute migration de données ou de dual forwarding,
- le coût effectif en euros de tout risque métier supplémentaire encouru pendant la transition, car vous réorientez des ressources pour qu'elles se concentrent sur ce projet plutôt que sur le travail d'ingénierie opérationnelle standard,
- tout transfert de licence entre votre SIEM traditionnel et votre nouveau SIEM,
- les frais liés au travail de vos équipes d'achats, juridiques et autres avec le fournisseur de votre nouveau SIEM.

Gérer le coût du changement

Maintenant que vous connaissez le coût du changement, vous comprenez pourquoi il est important de le maintenir aussi bas que possible.

Enfin, ce n'est pas tout à fait exact. Vous voulez que le coût du changement soit aussi bas que possible, tout en maximisant le retour sur investissement de votre nouvelle solution. Si votre nouvelle solution vous permet de réaliser des économies importantes chaque jour, ne serait-il pas judicieux de dépenser un peu plus pour réaliser ces économies plus rapidement ? Nous vous expliquerons plus en détail comment trouver ce juste milieu dans cette section consacrée à la gestion du coût du changement.

Diminuer le coût du changement

Comment réduire le coût initial du changement ? Examinons chaque option :

- Une planification efficace : la meilleure façon de gérer le coût du changement est de vous préparer. Toutes les données que vous recueillez et documentez en amont vous permettront de gagner du temps lors des entretiens et de l'identification de vos besoins par l'équipe Professional Services. Plus vous ferez preuve d'anticipation et de précision, moins le coût des services sera élevé.
- Réussir votre migration du premier coup, rapidement : il peut être tentant d'essayer de remplacer votre SIEM vous-même. Notre équipe Professional Services a pu constater à maintes reprises que travailler directement avec Splunk pour la migration est l'un des moyens les plus rapides et les plus fiables de migrer votre SIEM. Rater sa migration SIEM parce que vous avez tenté de la réaliser sans supervision ou aux côtés d'une organisation non accréditée est le meilleur moyen pour décupler le coût du changement.
- Renforcer vos compétences : en vous formant, vous et vos équipes, à l'utilisation du nouveau SIEM, vous vous familiariserez rapidement avec le système et accélérez sa mise en œuvre. Cela peut faciliter la tâche de l'équipe Professional Services et ainsi réduire le coût global. Chez Splunk, nous proposons des cours et des formations par le biais de Splunk Education pour vous aider à développer vos compétences avec Splunk.
- Adapter la migration à vos besoins : si vous n'avez pas besoin de migrer vos données, d'utiliser vos scénarios d'utilisation SIEM traditionnels et de conserver l'intégralité de vos données dans des systèmes de stockage de pointe, alors Splunk peut vous aider à réduire l'échelle de la migration.

Augmenter le ROI

Il est important de réduire le coût du changement, mais en fin de compte, votre projet de remplacement de SIEM doit à la fois réduire les coûts *et* créer de la valeur. Seule votre organisation peut juger des dépenses les plus judicieuses. Assurez-vous qu'au lieu de fixer des limites arbitraires aux coûts de ce changement, vous l'envisagez plutôt dans le contexte de votre TCO sur une période pertinente. Si le fait de dépenser plus aujourd'hui permet d'économiser davantage sur une période de trois ans grâce à un meilleur ROI et à une meilleure concrétisation de valeur, l'investissement initial en vaut probablement la peine.

6. Scénarios de remplacement du SIEM d'un fournisseur de services gérés

Introduction

Aujourd'hui, les fournisseurs de services gérés (MSP) sont omniprésents dans le monde de la sécurité. Parfois appelés fournisseurs de services de sécurité gérés (MSSP) dans ce contexte, ils proposent des services SOC couvrant un ou plusieurs des domaines suivants, entre autres :

- la détection et la supervision des menaces,
- l'ingénierie SIEM,
- la réponse aux incidents,
- la gestion des vulnérabilités,
- la supervision et les rapports de conformité.

Les scénarios d'utilisation typiques pour les MSP dans le domaine du SIEM peuvent être :

- la réduction du TCO en externalisant une ou plusieurs fonctions du SOC,
- la mise en place d'une nouvelle fonctionnalité dans le SOC.

Pour comprendre comment les MSP peuvent réduire le TCO, il convient d'analyser leur modèle commercial. Un MSP a rarement un seul client. Au contraire, les MSP tirent parti des économies d'échelle, en formant des équipes et en concevant des plateformes de sécurité basées sur une méthodologie cohérente. Les MSP gèrent le service de chaque client en utilisant ce système complet pour un coût inférieur à celui que le client devrait dépenser en interne pour le même service. Cela signifie que le recours à un MSP peut s'avérer gagnant pour le fournisseur et le client. La plupart des organisations qui ne sont pas actives dans le domaine de la sécurité ou qui ne gèrent pas un service de sécurité devraient consentir des investissements conséquents pour créer leur propre SOC. Pourquoi se donner tout ce mal alors que vous pouvez profiter de l'expertise d'une organisation dont c'est la spécialité ?

En revanche, en comprenant comment un MSP peut créer de la valeur en fonction de l'échelle du déploiement, vous pouvez également voir qu'un MSP a tout intérêt à adopter une approche évolutive. Cela signifie que le niveau de personnalisation en fonction de vos besoins spécifiques peut varier. Lorsque vous atteindrez un niveau de maturité supérieur, vous pourriez constater que vous avez du mal à obtenir le niveau de spécificité nécessaire pour répondre à vos nouveaux besoins, bien que cela dépende grandement de la nature du MSP.

La décision de recourir ou non à un MSP se base généralement sur une échelle mobile entre le coût et le niveau de personnalisation, ainsi que sur les relations de votre organisation avec les MSP actuels et potentiels. Ces facteurs peuvent évoluer avec le temps ; cependant, la bonne nouvelle est que, que vous soyez une organisation envisageant de confier des fonctionnalités à un MSP, ou que vous souhaitiez ramener tout ou partie des fonctionnalités de votre MSP en interne, Splunk dispose des produits, des services professionnels et de l'expérience nécessaires pour vous accompagner tout au long de votre transition, le tout en conservant un TCC raisonnable.

Splunk Professional Services a travaillé avec de nombreux clients pour soutenir l'internalisation des fonctionnalités MSSP existantes en tirant parti de notre processus éprouvé de remplacement de solution, des fonctionnalités de nos produits et de notre expertise dans le domaine du SIEM.

Que vous mettiez en place un tout nouveau SOC ou que vous souhaitiez développer des capacités existantes, Splunk Professional Services peut vous aider à concevoir et à mettre en œuvre la RBA de Splunk afin d'optimiser l'efficacité et de faciliter le travail de vos analystes, tout en contrôlant le TCO.

L'équipe Splunk Professional Services a l'expérience nécessaire pour découvrir et traduire les métriques courantes des MSP avec les solutions Splunk grâce au mappage et à la rationalisation des scénarios d'utilisation :

- compatibilité et respect des frameworks (par ex. MITRE ATT&CK, réglementations),
- risques atténués,
- scénarios d'utilisation mis en place,
- alertes traitées.

Facilitez la gestion de plusieurs business units grâce à l'architecture mutualisée, la RBAC, une conception basée sur les niveaux de service, l'automatisation, le tiering des données, le processus CI/CD, etc.

Internalisation

L'internalisation de tout ou partie du parc SIEM de votre MSP peut représenter un changement important. L'ampleur de ce changement dépend du niveau d'internalisation :

- vous souhaitez internaliser l'ensemble des capacités SOC et créer un tout nouveau SOC interne, ou
- vous souhaitez internaliser une partie des capacités SOC, par exemple les processus de détection et de supervision de niveau 2.

Il est évident que l'internalisation de l'ensemble des capacités d'un SOC et la création d'un tout nouveau SOC représentent un projet plus important que l'intégration d'une partie des fonctionnalités MSP dans un SOC existant. Considérons donc qu'il s'agit de deux scénarios différents et voyons comment Splunk Professional Services peut vous aider.

A. Tout internaliser

Internaliser l'ensemble de vos capacités de sécurité est une décision importante, mais que de nombreuses organisations prennent lorsqu'elles atteignent une certaine taille ou un certain niveau de maturité. Bien que le TCO puisse être une bonne raison d'internaliser sa sécurité, la plupart des organisations avec lesquelles nous travaillons choisissent d'internaliser l'ensemble de leurs opérations de sécurité parce qu'elles veulent un niveau de qualité et de pertinence qu'elles ont du mal à obtenir sur le marché des MSP.

Pendant votre transition, vous devrez prendre plusieurs décisions majeures :

- Allez-vous conserver les KPI et OKR (Objectives and Key Results) que vous utilisiez avec votre MSP ou allez-vous en définir de nouveaux ? Par exemple, le nombre d'alertes traitées est un SLA courant pour un MSP, mais il peut s'avérer moins pertinent en interne.
- Allez-vous essayer de migrer les scénarios d'utilisation de votre MSP dans votre plateforme SIEM interne ? Tout dépend si vous possédiez votre ancien SIEM ou si votre MSP le gérait comme une boîte noire, sans que vous ayez la moindre idée de sa configuration. Si vous le possédiez, vous pouvez exporter et mapper les scénarios d'utilisation dans votre nouveau SIEM. Si vous ne le possédiez pas, votre MSP ne souhaitera peut-être pas partager sa propriété intellectuelle, d'autant plus que votre relation commerciale prend fin, vous devrez donc peut-être repartir de zéro.
- Allez-vous devoir migrer des données de la solution de votre MSP ? En fonction du contrat établi avec votre MSP, cela pourrait être impossible ou entraîner un coût supplémentaire.

L'approche de Splunk Professional Services

Splunk Professional Services a de l'expérience dans la conception, la mise en œuvre et la documentation de ces transformations et peut vous aider à planifier l'internalisation à partir d'un environnement MSP.

En optant pour un SOC interne, vous avez la possibilité de créer une plateforme entièrement basée sur vos propres besoins. Cela signifie que Splunk peut travailler avec vous pour mettre en place une approche optimale entièrement adaptée à vos besoins organisationnels.

B. Hybride : internaliser une partie des fonctionnalités

La bonne nouvelle est que si vous internalisez une partie des fonctionnalités dans un SOC existant, vous n'avez qu'à ajouter les capacités nécessaires pour mettre en œuvre ces fonctionnalités, ce qui engendrera naturellement un TCC inférieur que si vous deviez tout internaliser. La difficulté réside dans le fait que vous devrez continuer à travailler avec votre MSP dans votre nouvel environnement hybride, ce qui signifie que vos systèmes et runbooks doivent être capables de gérer une approche multi-équipes.

Lorsque vous migrez un sous-ensemble des fonctionnalités de votre MSP en interne, comme la détection et la supervision avancées ou l'ingénierie SOC, vous devez également tenir compte du fait que les rapports et les métriques que votre MSP vous fournit pour prouver sa valeur ne sont probablement pas les mêmes que les résultats que votre entreprise attendra de votre équipe SOC interne. Là où un MSP peut s'appuyer sur des métriques telles que le MTTR, le MTTA et le nombre d'alertes triées, vos parties prenantes internes seront peut-être davantage intéressées par les résultats de vos investigations internes personnalisées et par des informations sur l'avancée de l'atténuation des risques et la couverture des détections.

L’approche de Splunk Professional Services

Splunk Professional Services peut aider à configurer un environnement MSP hybride. L’équipe a de l’expérience dans la conception, la mise en œuvre et la documentation de ce type d’activités et travaille très souvent dans ce type d’environnements.

Mettre toutes les chances de son côté

- **Évaluation de la situation actuelle – Contrôles d’optimisation :** si vous assumez une partie de la responsabilité de votre service de sécurité, vous devrez tout d’abord vous assurer que vous comprenez l’état actuel de la configuration de la plateforme SIEM, puis établir une feuille de route pour réaliser toutes les optimisations nécessaires afin d’augmenter la valeur de votre future configuration. Si votre SIEM était précédemment géré par un MSP, vous pouvez vérifier qu’il est configuré selon les bonnes pratiques en vigueur et identifier d’éventuelles lacunes. Splunk Professional Services peut réaliser cette analyse des écarts et vérifier si les configurations SIEM existantes respectent les bonnes pratiques du marché.
- **Conception du système :** lorsque vous passez à un SOC hybride, vous devrez probablement aussi hybrider votre SIEM. Même si vous continuez à utiliser la même plateforme SIEM que votre MSP en tant que colocataires, vous devrez toujours prendre en compte les nouvelles intégrations et configurations dont votre équipe a besoin pour assurer votre part du service de sécurité. Splunk Professional Services peut aider à concevoir une nouvelle approche qui décrit les nouveaux éléments de cette solution et les communiquer à vos parties prenantes internes et externes, y compris votre MSP. Si vous prévoyez d’utiliser deux solutions SIEM distinctes, l’une interne et l’autre externe, Splunk Professional Services peut vous aider à concevoir une approche qui décrit l’intégration entre vos deux systèmes, ainsi qu’à réaliser l’intégration à proprement parler.
- **RBAC :** pour que plusieurs équipes puissent utiliser la même plateforme, vous devez prévoir un index et un système RBAC résilients et évolutifs. Splunk gère l’accès au niveau des données via ces index et un modèle RBAC.
- **Workflows :** vous devrez concevoir une plateforme de gestion des investigations qui réponde à vos besoins. Si votre équipe interne a besoin d’un accès différent à votre MSP, vous devrez peut-être créer un modèle RBAC multilocataires non seulement pour vos données, comme indiqué ci-dessus, mais aussi pour vos alertes. Pour ce faire, vous pouvez utiliser Splunk Mission Control, et Splunk Professional Services peut vous aider à créer une architecture de bonnes pratiques pour atteindre cet objectif, et la documenter en même temps que vos workflows planifiés de gestion des investigations.

Scénarios d’utilisation et rapports

Scénarios d’utilisation : Splunk peut vous aider à établir une feuille de route au cours de notre atelier sur les scénarios d’utilisation. Ainsi, vous pouvez définir une approche collaborative avec votre MSP. Splunk Professional Services peut solliciter la contribution de vos équipes internes, ou d’une combinaison de votre organisation et du MSP, pour s’assurer que toute feuille de route est consensuelle et respecte les bonnes pratiques. Splunk Professional Services peut également aider votre équipe SOC à mettre en œuvre un sous-ensemble de nouveaux scénarios d’utilisation, afin de vous permettre d’acquérir les compétences nécessaires pour assumer vos nouvelles responsabilités dans le cadre du projet d’internalisation.

Rapports : lorsque vous internalisez un sous-ensemble de vos fonctionnalités SOC, vous devez fournir vos propres rapports sur les activités de vos équipes internes et ne plus vous contenter des rapports fournis par votre MSP. Splunk peut aider à configurer des rapports et des tableaux de bord permettant de communiquer les résultats de votre nouveau SOC interne aux principales parties prenantes.

Externalisation

A. Service entièrement géré : tout externaliser

L'objectif d'un MSP 100 % externe est d'affranchir votre équipe du fardeau des opérations de sécurité. Cela signifie que vous ne devriez pas avoir trop d'éléments à prendre en compte lors de la conception de la solution. Vous devrez établir vos exigences, les partager avec votre MSP et réfléchir aux modalités du contrat, en déterminant les KPI et les SLA appropriés pour répondre aux besoins de votre entreprise. Veuillez noter que plus les SLA sont stricts, plus les coûts risquent d'être élevés.

Splunk travaille avec un éventail de partenaires agréés pour proposer des services de sécurité gérés à ses clients. Si votre organisation est elle-même un MSP, Splunk Professional Services peut vous aider à mettre en place une solution performante et évolutive pour gérer plusieurs clients utilisant Splunk. Essayez la Splunk Content Manager App pour voir comment vous pouvez gérer le contenu sur plusieurs plateformes Splunk dès aujourd'hui.

B. Hybride : externaliser une partie des fonctionnalités

Vous devez suivre le même processus que pour tout externaliser, mais avec l'exigence supplémentaire de déterminer les points d'interaction et d'intégration entre votre SIEM sur site et votre nouveau MSP.

7. Concevoir une solution SIEM

Remplacer son SIEM ne revient pas seulement à reprendre ce que vous faisiez auparavant et à le reproduire avec une nouvelle technologie. La migration vers un nouveau SIEM est un virage dont vous pouvez profiter pour optimiser votre plateforme SIEM et l'expérience de vos analystes, et au final, obtenir de meilleurs résultats avec un TCO inférieur.

Dans cette section, nous présentons quelques-uns des nombreux sujets et concepts que vous devrez comprendre et aborder afin de dresser les contours de votre futur modèle SIEM.

Pour en discuter plus en détail, veuillez contacter l'équipe Splunk Professional Services. Nous pouvons vous conseiller et vous proposer des solutions de pointe adaptées à vos besoins.

Migration des données, dual forwarding et transferts

Introduction

Changer de SIEM signifie qu'il y aura forcément une période de transfert pendant la migration de l'ancienne vers la nouvelle plateforme. Ces périodes de transfert peuvent se présenter sous de nombreuses formes, mais deux se détachent clairement : le dual forwarding et le « big bang ».

Les organisations doivent également décider si elles souhaitent migrer les données hors de leur SIEM traditionnel ou repartir de zéro dans leur nouveau SIEM (scénario « greenfield »).

Il n'y a pas de meilleure approche et l'alternative la plus judicieuse pour votre transition dépendra des priorités et des objectifs de votre entreprise.

Migration des données

La migration des données consiste à transférer tout ou partie des données stockées dans votre ancien SIEM vers votre nouveau SIEM. En règle générale, cela se fait en transférant les données de votre ancien SIEM vers votre nouveau SIEM.

Avantages

Cette approche peut aider à réduire la durée du dual forwarding, ce qui entraîne une réduction des coûts car vous pouvez ainsi répondre plus rapidement aux exigences de conservation des données dans votre nouveau SIEM. Par exemple, si votre régulateur indique que vous devez conserver les données des appareils critiques pendant 100 jours dans votre outil SIEM, votre processus de dual forwarding devra durer 100 jours. Si vous migrez vos données de votre ancien vers votre nouveau SIEM, vous pouvez réduire le temps nécessaire pour répondre à cette exigence réglementaire. De plus, cela peut permettre à votre nouveau SIEM d'utiliser une plus grande plage de données historiques dans les corrélations, améliorant ainsi la fidélité des alertes.

Défis

Bien que la migration des données semble être le choix le plus évident, elle présente également des défis importants :

- Si votre ancien SIEM contient une quantité importante de données, leur transfert vers votre nouveau SIEM peut entraîner des coûts de réseau considérables. Dans le cas d'une migration vers un SIEM hébergé en IaaS, vérifiez les coûts d'importation des données de votre fournisseur cloud, car ils peuvent être importants lors de la migration de grandes quantités de données SIEM historiques.
- Il est peu probable que le format des données stockées dans votre ancien SIEM soit le même que celui des données stockées dans votre nouveau SIEM. Cela signifie que, bien que vous puissiez souvent envoyer les données de votre ancien SIEM vers votre nouveau SIEM et les stocker, des efforts supplémentaires seront peut-être nécessaires pour rendre ces données utilisables en même temps que les données envoyées directement dans votre nouveau SIEM.

Veillez à bien réfléchir lorsque vous souhaitez utiliser une longue période de données historiques pour réaliser des corrélations. Il est assez rare que les corrélations couvrent des périodes supérieures à 30 jours, bien qu'il puisse y avoir des exceptions pour certaines corrélations couvrant des attaques low and slow telles que le beaconing, l'exfiltration de données ou le déni de service (DoS) à long terme.

Dual forwarding

Le dual forwarding consiste pour une organisation à passer de son ancien SIEM à un nouveau SIEM sur une durée définie afin d'éviter toute interruption des activités. Pour ce faire, il faut configurer des sources de données ou des forwarders de sources de données pour envoyer des données à deux endroits ou plus.

Le dual forwarding peut être utile si une politique d'entreprise ou un organisme de réglementation exige la conservation des données pendant une certaine durée, et que vous ne prévoyez pas de tenter une migration des données.

Dans le contexte d'un remplacement de SIEM impliquant un passage à Splunk, le dual forwarding signifie généralement que vous configurez vos sources de données pour qu'elles soient envoyées à la fois vers votre ancien SIEM et vers Splunk pendant un certain temps. Une fois que vous avez importé suffisamment de données dans votre solution Splunk pour répondre aux exigences de conservation des données ou pour assurer la fonctionnalité des contrôles de sécurité à un niveau acceptable, vous pouvez interrompre le forwarding des données vers votre ancien SIEM et le mettre hors service.

Avantages

L'avantage de cette approche est qu'elle garantit à votre entreprise de ne pas perdre sa couverture de sécurité et de respecter toutes les exigences de conservation des données, les risques pour l'entreprise sont donc atténués.

Défis

L'inconvénient est qu'elle peut nécessiter beaucoup de temps et de ressources, et nécessiter le paiement simultané du coût des licences de deux solutions pendant un certain temps.

Pour décider de choisir cette approche, il faut comparer la valeur du risque pour votre entreprise par rapport à d'autres approches et le coût plus élevé d'une approche dual forwarding.

Le dual forwarding est l'approche la plus courante observée par Splunk Professional Services sur le marché, car la plupart des organisations privilégient la résilience aux économies lors du remplacement de leur SIEM.

Mode différé (Store-and-forward)

Lors de la migration depuis un SIEM traditionnel, une alternative au dual forwarding est la configuration « store-and-forward » ou mode différé. Dans un scénario de store-and-forward, au lieu de configurer vos sources de données pour qu'elles soient envoyées simultanément vers votre ancien et votre nouveau SIEM, vous configurez votre ancien SIEM pour qu'il stocke les données et les transmette à Splunk.

Avantages

L'avantage de cette approche est qu'elle est relativement simple à configurer, ce qui réduit les efforts d'ingénierie et les coûts associés.

Défis

L'inconvénient de cette approche est qu'une fois les données traitées par un SIEM traditionnel, elles ne sont généralement plus dans leur format d'origine. Splunk met à disposition sa base de données d'applications, Splunkbase, utilisée par une communauté de développeurs et de fournisseurs afin de garantir que les données peuvent être facilement ingérées et utilisées dans leur format standard. L'envoi de données à partir d'un SIEM traditionnel signifie généralement que ces parsers ne peuvent pas être utilisés et qu'un parsing personnalisé doit être créé. Bien que Splunk Professional Services ou l'équipe d'administrateurs Splunk de votre organisation puisse réaliser ce parsing rapidement et facilement, vous pourriez économiser ce temps en choisissant un autre processus de migration.

Deuxièmement, bien que la configuration d'un système de stockage et de transfert soit relativement facile, elle n'élimine pas la nécessité de couper les sources de données à un certain moment. Étant donné qu'une source de données transférée depuis un autre SIEM n'utilisera probablement pas le même format, des étapes supplémentaires pourraient être nécessaires une fois la source coupée afin de s'assurer que les données sont bien envoyées.

Bien que le store-and-forward ait été une stratégie de migration courante, il est de plus en plus rare de voir des organisations l'utiliser pour obtenir un ROI rapide avec leurs nouvelles solutions SIEM, elles l'utilisent maintenant plutôt comme un outil de stockage des données de sécurité.

Transferts directs big bang

Un transfert big bang consiste à migrer directement toutes vos sources de données, plutôt que de configurer un dual forwarding vers votre ancien et votre nouveau SIEM. Ce type de transfert est généralement effectué dans un délai très court afin de réduire au minimum la période pendant laquelle votre organisation ne dispose d'aucune couverture de sécurité.

Avantages

Les transferts big bang présentent un avantage considérable : ils vous permettent de vous appuyer sur votre nouveau SIEM dès que possible. Cela peut s'avérer particulièrement utile dans les scénarios

d'internalisation de MSSP, évoqués plus haut, ou lorsque vous devez migrer depuis votre SIEM traditionnel avant un dépassement ou une expiration de licence.

De plus, si votre ancien SIEM n'est plus fonctionnel et qu'aucun organisme de réglementation ne vous impose une couverture de sécurité permanente ou une certaine période de conservation des données, il n'y a pas beaucoup d'inconvénients à l'abandonner et à passer à autre chose.

Défis

Le problème potentiel d'une approche big bang est qu'elle entraînera, par nature, une période pendant laquelle une partie de vos sources de données sera importée dans votre ancien SIEM et une autre partie dans votre nouveau SIEM.

Les implications sont nombreuses :

- Si un incident survient pendant la migration big bang, vous ne pourrez pas vous tourner vers un SIEM unique contenant toutes les données associées à cet incident.
- Les analystes n'auront pas accès à une vue unique de vos systèmes. Ils seront contraints d'alterner entre deux outils jusqu'à la fin de la migration, ce qui rallonge drastiquement leur travail et augmente les risques métiers.
- Vous n'aurez pas le temps de bien tester et confirmer la fonctionnalité des scénarios d'utilisation et des données pendant le transfert des sources de données. Le temps nécessaire pour tester correctement chaque source de données pendant la migration prolongera la période de transfert et augmentera les risques.

Toute décision concernant l'adoption d'une approche big bang doit se baser sur une analyse rationnelle de la situation de votre organisation. Vous devrez quoi qu'il arrive accepter un certain niveau de risque, mais la situation peut être telle que le big bang reste l'approche la plus adaptée, surtout si vous repartez de zéro après une mise en œuvre ratée de votre ancien SIEM.

Splunk peut faciliter les migrations big bang car nous utilisons une méthodologie de traitement des données de schéma de lecture (schema-on-read). Cela signifie que les données ne doivent pas nécessairement respecter un schéma spécifique au moment de l'ingestion, et que des recherches et des analyses peuvent être créées sur les données historiques après coup pour s'assurer qu'elles sont toujours utilisables. De nombreux SIEM traditionnels utilisent plutôt une méthodologie de traitement des données de schéma d'écriture (schema-on-write), ce qui signifie que toute source de données transférée pendant le processus de migration ne correspondant pas au schéma attendu serait rendue inutilisable pour toute corrélation de sécurité.

Classification et stockage des données

Introduction

Dans son article de blog sur le sujet, Splunk décrit la classification des données comme « le processus d'organisation des données en groupes sur la base de leurs attributs et caractéristiques, puis l'attribution d'étiquettes de classe décrivant un ensemble d'attributs qui s'appliquent aux ensembles de données correspondants. Nous pouvons considérer qu'il s'agit d'une partie d'une pratique globale de gestion des données ».

Dans le contexte d'un SIEM, nous utilisons la classification des données pour gérer le TCO sans affecter la convivialité de la solution. Pour ce faire, il faut diviser les données en plusieurs niveaux et choisir un profil de stockage et de workload adapté à chaque niveau.

Par exemple, si vous prévoyez d'importer des données relatives à la sécurité utilisées pour les alertes, celles-ci seront probablement considérées comme des données de haut niveau, c'est-à-dire des données

que vous devez pouvoir interroger rapidement et de manière fiable. D'un autre côté, il se peut que vous importiez des données dont l'utilité est purement réglementaire et qui n'ont pas besoin d'être interrogées, sauf dans de rares scénarios d'incidents. Dans cette situation, ces données seraient affectées à un niveau inférieur.

Les données SIEM de niveau élevé sont généralement stockées dans un système de données à accès rapide. Les données SIEM de niveau moins élevé sont stockées dans un système de données à accès plus lent. Elles peuvent même être entièrement archivées.

Splunk propose des options pour tous les niveaux de stockage et d'archivage des données, y compris l'utilisation de systèmes de stockage d'objets distants avec SmartStore.

Recherche fédérée S3

En plus de SmartStore, Splunk offre la possibilité d'interroger des données S3 à l'aide de la recherche fédérée. Outre la recherche au sein des environnements Splunk, Splunk Federated Search for Amazon S3 vous permet d'interroger les données de vos buckets Amazon S3 à partir de votre déploiement Splunk Cloud Platform.

Gestion des workloads

La gestion des workloads de Splunk vous permet de séparer les ressources de recherche et d'importation en pools afin de les classer par ordre de priorité. Cela peut s'avérer essentiel dans les environnements où les ressources sont limitées, afin de garantir qu'une expansion des sources de données et des scénarios d'utilisation les moins importants n'a pas d'impact sur la résilience de l'entreprise.

L'exemple le plus courant d'architecture autour de la gestion des workloads consiste à proposer un modèle d'importation et de recherche dans lequel les scénarios d'utilisation critiques tels que le SIEM, qui peuvent coexister avec d'autres workloads moins prioritaires tels que l'analyse métier, sont toujours priorisés par le système. Cela signifie que dans un scénario où vous ne pouvez pas nécessairement contrôler l'utilisation de la plateforme – par exemple, lorsque vous partagez une plateforme Splunk avec l'équipe d'analyse métier, en l'utilisant à la fois comme SIEM et comme moteur d'analyse métier – vous voulez vous assurer que si l'équipe d'analyse métier décide d'augmenter son niveau d'ingestion ou d'utilisation de la plateforme, vous avez la garantie que votre propre ingestion de sécurité et vos workloads ne seront pas affectés.

La planification de la gestion des workloads transversaux peut s'avérer complexe, mais elle est essentielle pour garantir que votre résilience n'est pas affectée et que vous n'aurez pas à étendre votre licence SIEM en raison de facteurs indépendants de votre volonté.

Splunk Professional Services peut vous aider à élaborer une architecture autour de la gestion des workloads.

Data lakes et flux de données intermédiaires

Une tendance que nous voyons émerger dernièrement pour l'évaluation et la préparation des migrations de SIEM consiste à mettre en œuvre une couche intermédiaire entre les sources de données et le SIEM. Il peut s'agir de data lakes, de services de flux de données, ou des deux.

Analysons les raisons les plus souvent citées et voyons si elles sont valables.

- **Résilience :** améliorer la résilience en ajoutant un dépôt de données secondaire. Si pour une quelconque raison, des données n'atteignent pas le SIEM et s'il y a un incident ou une interruption de service, cela permet de stocker ces données à un autre endroit.
- **Dépendance vis-à-vis des fournisseurs :** être indépendant de ses fournisseurs en ajoutant une couche intermédiaire. Cette couche intermédiaire peut facilement être remplacée si une migration du SIEM s'avère nécessaire.

- **Évolutivité :** ajouter une couche intermédiaire permettra à une solution de mieux s'adapter à des destinations multiples.
- **Simplicité :** gérer une couche intermédiaire est plus simple à long terme car vos équipes n'auront besoin que d'un seul ensemble de compétences en cas de changement de fournisseur SIEM.
- **Économies :** utiliser une couche intermédiaire permet de filtrer le bruit et de n'importer que les données dont vous avez vraiment besoin dans votre SIEM, ce qui vous permet d'économiser sur les coûts de licence.

Nous allons maintenant analyser chacun de ces arguments.

- **Résilience :** ajouter une couche supplémentaire ajoute des composants qui doivent être entretenus et configurés, ce qui se traduit par un TCO plus élevé et un risque potentiellement accru. En cas de défaillance de la couche intermédiaire, la résilience de la solution s'en retrouve diminuée au lieu d'être améliorée.
- **Dépendance vis-à-vis des fournisseurs :** ajouter une couche intermédiaire augmente le nombre de fournisseurs avec lesquels vous travaillez, ce qui augmente donc le nombre de points de contact d'approvisionnement. Cela ne permet pas d'éliminer la dépendance vis-à-vis des fournisseurs. Si la couche intermédiaire est un logiciel gratuit open source, vous n'aurez accès à aucun service d'assistance professionnel en cas de problème, ce qui augmente le risque métier.
- **Évolutivité :** de nombreux SIEM modernes, dont Splunk, peuvent ingérer plusieurs pétaoctets de données sans avoir besoin d'une couche intermédiaire.
- **Simplicité :** ajouter une couche intermédiaire augmente le nombre de technologies sous la responsabilité de votre équipe. Cela signifie des effectifs supplémentaires ou la dilution des profils de compétences de vos équipes d'ingénierie.
- **Économies :** bien que les couches intermédiaires puissent filtrer les données, la charge supplémentaire liée à leur gestion peut être importante. De plus, comme de nombreuses couches intermédiaires s'écartent des processus d'ingestion de données SIEM standards, le coût supplémentaire lié à la reconstruction de ces couches plutôt qu'à l'utilisation d'un contenu prêt à l'emploi peut être conséquent. Splunk fournit ses propres technologies pour acheminer et filtrer les données, ainsi que des mécanismes de tiering des données qui vous permettent d'optimiser le coût de vos données en fonction de leur utilisation. Enfin, lorsque vous ajoutez un dépôt de données intermédiaire, vous stockez en fait une partie ou la totalité de vos données en double ; il est peu probable que cela soit moins coûteux que de les envoyer à des dépôts de données correctement hiérarchisés.

Pour préparer une migration efficace vers Splunk, essayez de tenir compte des éléments suivants lorsque vous envisagez d'utiliser une couche intermédiaire :

- La couche intermédiaire réduit-elle ou augmente-t-elle la résilience ? Est-ce au détriment du TCO ?
- Interrompra-t-elle le processus d'ingestion de données prêt à l'emploi de votre nouveau SIEM, vous obligeant donc à recréer les parsers et les détections à vos propres frais ?
- La couche intermédiaire offre-t-elle une évolutivité supérieure à celle que permet votre nouveau SIEM ?
- La couche intermédiaire simplifie-t-elle réellement votre paysage logiciel ou implique-t-elle davantage de compétences et de points de contact administratifs pour vos ingénieurs ?
- Après avoir pris en compte les compétences supplémentaires, le temps de configuration, le coût du double stockage des données, l'impact supplémentaire sur le réseau, les coûts supplémentaires du matériel, des logiciels et de l'assistance, etc., le TCO de votre projet est-il réellement inférieur ?

Bien que le souhait d'utiliser une couche intermédiaire repose sur une logique métier tout à fait valable, les considérations ci-dessus mettent en évidence la manière dont cette couche peut en réalité augmenter les coûts et réduire la fonctionnalité, à moins qu'elle ne soit envisagée dans un contexte métier plus large.

Splunk Professional Services peut vous aider à planifier une migration de SIEM qui atteigne vos objectifs métiers et recommander des solutions intermédiaires répondant à vos exigences le cas échéant. De plus, Splunk propose un outil de traitement des flux, Splunk Edge Processor, décrit dans la prochaine section.

Splunk Edge Processor

Splunk Edge Processor est une solution de traitement des données qui fonctionne à la périphérie de votre réseau. Utilisez Splunk Edge Processor pour filtrer, masquer et transformer vos données à proximité de leur source avant d'acheminer les données traitées vers des environnements externes. Cette solution vous permet d'envoyer les données aux niveaux de données appropriés, ce qui optimise vos coûts de déploiement.

En résumé

Dans cette section, nous avons étudié l'impact de la classification des données et de leur stockage, ainsi que les mécanismes potentiellement impliqués. Pour un guide beaucoup plus approfondi sur les données et le tiering des données, consultez le Guide essentiel des données de Splunk et le Playbook de la hiérarchisation des données de Splunk.

Multi-tenancy

La RBAC pour la multi-tenancy de la couche de données

La RBAC est le mécanisme par lequel Splunk gère les droits d'accès aux données.

Nous pouvons utiliser la RBAC pour fournir les droits d'accès adaptés aux données à un éventail d'équipes de votre organisation, par exemple les utilisateurs métiers et les analystes de sécurité ayant besoin d'accéder à des ensembles de données différents.

La RBAC peut être utilisée lorsque votre organisation et votre MSP ont besoin de différents niveaux d'accès. La RBAC peut également être utilisée pour prendre en charge la multi-tenancy si vous avez besoin de configurer une plateforme de telle sorte que plusieurs unités métiers ou organisations puissent partager un environnement unique sans voir les données des autres.

Si vous êtes un MSP, la RBAC vous permet de gérer un service d'opérations de sécurité pour plusieurs clients à partir d'une seule plateforme Splunk partagée, en donnant un accès basé sur les rôles à leurs données uniquement.

Catalogage des services de sécurité

Vue d'ensemble

Le catalogage des services décrit une approche de la sécurité basée sur des catalogues de services. Dans ce contexte, un catalogue de services décrit plusieurs niveaux de service, parmi lesquels vos clients – qu'il s'agisse d'unités métiers, si vous gérez la sécurité des informations pour une organisation, ou des organisations elles-mêmes, si vous êtes un MSP – peuvent faire leur choix. Par exemple, vous pouvez décider d'offrir un catalogue de niveaux de service de différentes catégories, tels que Bronze, Argent et Or, sur la base d'accords budgétaires ou de frais.

Ces niveaux de service peuvent avoir différents KPI, SLA, volumes de données acceptés, etc. Par exemple, le niveau de service Bronze peut prévoir jusqu'à 30 alertes triées par jour, sur un maximum de 100 Go de données, tandis que le niveau de service Argent peut prévoir jusqu'à 100 alertes triées sur 500 Go de données, avec un SLA de cinq heures.

Les catalogues de services peuvent être un moyen utile de s'assurer que votre entreprise répond aux clients les plus prioritaires. Splunk peut prendre en charge les catalogues de services grâce à une

combinaison de tiering des données, de RBAC, de gestion des workloads et d'étiquetage approprié des alertes dans Enterprise Security.

Splunk Professional Services peut vous aider à concevoir un catalogue de services qui répond à vos besoins métiers, à la fois au niveau de l'entreprise et en créant l'architecture technique adéquate pour le supporter.

Architectures SIEM hybrides et SIEM-of-SIEM

Une tendance récente dans la conception de SIEM est l'utilisation de plusieurs solutions SIEM en parallèle. Bien que les motivations puissent être diverses, la plupart du temps, c'est parce qu'un fournisseur inclut le tarif de son SIEM, bien souvent une solution publique basée sur le cloud, dans le cadre d'un accord de licence d'entreprise (ELA). Ce modèle de licence rend financièrement attrayante l'utilisation d'un SIEM pour assurer un certain niveau de supervision de la sécurité. Une motivation secondaire pourrait être qu'un SIEM soit spécialisé pour un type précis de source de données et qu'il soit consacré uniquement à cette source de données.

Splunk peut fonctionner avec de nombreuses autres solutions SIEM au sein d'une architecture SIEM-of-SIEM efficace. Cela signifie que si vous décidez de mettre en place un autre SIEM pour un scénario d'utilisation spécifique ou parce que votre équipe d'approvisionnement a imposé son utilisation, Splunk peut continuer à exister en tant que SIEM parent, en collectant les alertes et les résultats des sous-SIEM.

Les architectures SIEM-of-SIEM présentent l'inconvénient d'être plus complexes que lorsque vous utilisez un seul fournisseur, mais compte tenu des réalités des environnements complexes actuels, il incombe aux fournisseurs de répondre aux exigences métiers des clients en matière de configurations SIEM intégrées.

Bien que chaque configuration soit obligatoirement configurée sur mesure et ne puisse actuellement être basée sur une solution pré-packagée, Splunk dispose d'un ensemble de systèmes pouvant aider à la mise en place de ces architectures :

- RBA : elle peut être utilisée pour aider à agréger des alertes ponctuelles provenant de sous-SIEM disparates, Splunk étant le SIEM parent.
- SOAR : il peut être utilisé pour assurer l'automatisation entre divers composants SIEM, afin d'accélérer et d'automatiser la réponse aux incidents de sécurité, mais aussi en tant que middleware entre les composants SIEM, afin de garantir que tous les états des événements restent synchronisés lorsqu'ils sont transposés entre les différents outils.
- Plateforme ouverte : Splunk facilite l'importation et le transfert de données et d'alertes grâce à des API ouvertes. La plateforme ouverte de Splunk est donc un outil de centralisation idéal au sein d'une architecture à plusieurs SIEM.

Bien que les architectures SIEM hybrides soient de plus en plus courantes et qu'elles puissent être adaptées et accélérées, il convient de réfléchir à l'utilisation de plus d'un SIEM d'un point de vue métier et de se demander si cela permet réellement de réduire le TCO et les risques métiers. Les organisations doivent se demander si le coût du maintien de la connaissance et de l'intégration entre ces multiples plateformes l'emporte sur les avantages qu'elles en retirent ou non.

Scénarios de recherche fédérée et de transmission d'alertes entre plusieurs régions

Vue d'ensemble

Si votre déploiement Splunk doit couvrir plusieurs régions, Splunk met à disposition plusieurs technologies pour vous aider à garder vos analyses connectées tout en répondant aux exigences réglementaires et aux objectifs métiers.

Orchestration entre plusieurs régions

Les organisations peuvent être confrontées à un éventail de défis les obligeant à mettre en place plusieurs instances Splunk distinctes. Si l'une des raisons peut être l'obligation légale de conserver les données sur place, la raison est parfois plus complexe. Certaines organisations ont besoin d'ingérer des données provenant de navires ou d'avions qui, par nature, ont des possibilités très limitées pour envoyer des données télémétriques. Cela peut signifier que les architectures doivent prendre en charge la transmission intermittente d'alertes, par exemple lorsqu'un navire accoste ou qu'un satellite effectue un passage, et mettre ces informations à disposition des équipes d'analystes à terre de manière fiable.

La bonne nouvelle, c'est que Splunk SOAR peut aider à orchestrer les alertes sur plusieurs instances, le cas échéant. La Splunk Content Manager App peut vous aider à assurer la synchronisation du contenu entre plusieurs régions. Splunk a déjà aidé plusieurs clients à mettre en place des architectures qui atteignent ces objectifs et bien plus encore. Nous serions ravis de nous entretenir avec vous pour voir comment nous pouvons vous aider.

Souveraineté des données

La souveraineté des données fait référence aux exigences – juridiques ou autres – de conservation des données dans une région spécifique. Par exemple, une exigence de souveraineté des données peut signifier que toutes les données associées à un pays donné doivent rester dans ce pays. Si votre équipe SOC est basée aux États-Unis, cela peut vous faire réfléchir. C'est là que le transfert d'alertes et la recherche fédérée interviennent. Si les données elles-mêmes ne peuvent être transférées d'une région à l'autre, les détections peuvent toujours être effectuées localement et les alertes – qui ne sont pas des données mais des métadonnées – peuvent être envoyées, à condition qu'elles répondent à certaines exigences.

Recherche fédérée

Splunk peut prendre en charge des topologies de recherche fédérée, dans lesquelles plusieurs déploiements de Splunk sont interrogés à partir d'un déploiement central. Cela permet de mettre en place des architectures plus complexes répondant aux exigences métiers, telles que la souveraineté des données dans plusieurs régions.

Transfert d'alertes

Le transfert d'alertes fait référence à l'utilisation de Splunk Enterprise Security et de Splunk SOAR pour transférer les alertes entre les environnements Splunk, généralement pour les transférer dans une instance centralisée en vue d'une analyse plus approfondie.

Audit et menace interne

Il arrive que des organisations nous fassent part de leurs préoccupations quant à l'idée de savoir qui « supervise les superviseurs ». En d'autres termes, que se passerait-il si un analyste représentait lui-même une menace interne ? Le fait d'avoir accès à toutes les données d'une organisation ne lui permettrait-il pas de brouiller les pistes ?

Bien que certaines personnes puissent affirmer que si vous embauchez quelqu'un dans un rôle d'analyste, vous acceptez de leur accorder un certain degré de confiance et de vous exposer à un certain risque métier, ce type d'audit approfondi des menaces internes est possible dans Splunk. Les organisations peuvent soit utiliser la RBAC pour s'assurer que les analystes n'ont pas accès aux logs de la plateforme Splunk, soit transmettre les données à une instance Splunk séparée.

SIEM et gestion des vulnérabilités

Une autre question que nous recevons parfois de la part d'organisations est la suivante : pouvons-nous utiliser Splunk pour la gestion des vulnérabilités ?

La réponse est oui, tout à fait, mais attendez, ne jetez pas tout de suite votre scanner de vulnérabilité !

Splunk est idéal pour stocker des données de vulnérabilité afin de contextualiser les alertes et d'offrir des visualisations attrayantes qui aident à raconter l'histoire de ces données. Ces deux éléments constituent une partie essentielle du cycle de vie de la gestion des vulnérabilités. Cela dit, Splunk n'est pas un scanner de vulnérabilités à part entière. Vous devrez toujours utiliser un outil dédié à cette fin, qui fournira des données d'entrée à Splunk, ainsi qu'un logiciel de gestion de la configuration pour effectuer les mises à jour et les remédiations.

Gestion des scénarios d'utilisation

La mise en œuvre d'un nouveau SIEM représente une opportunité d'améliorer la gestion de vos scénarios d'utilisation. Dans cette section, nous allons illustrer certaines grandes pratiques et stratégies de gestion des scénarios d'utilisation, et comment elles peuvent être mises en œuvre dans Splunk.

Inventaires des scénarios d'utilisation

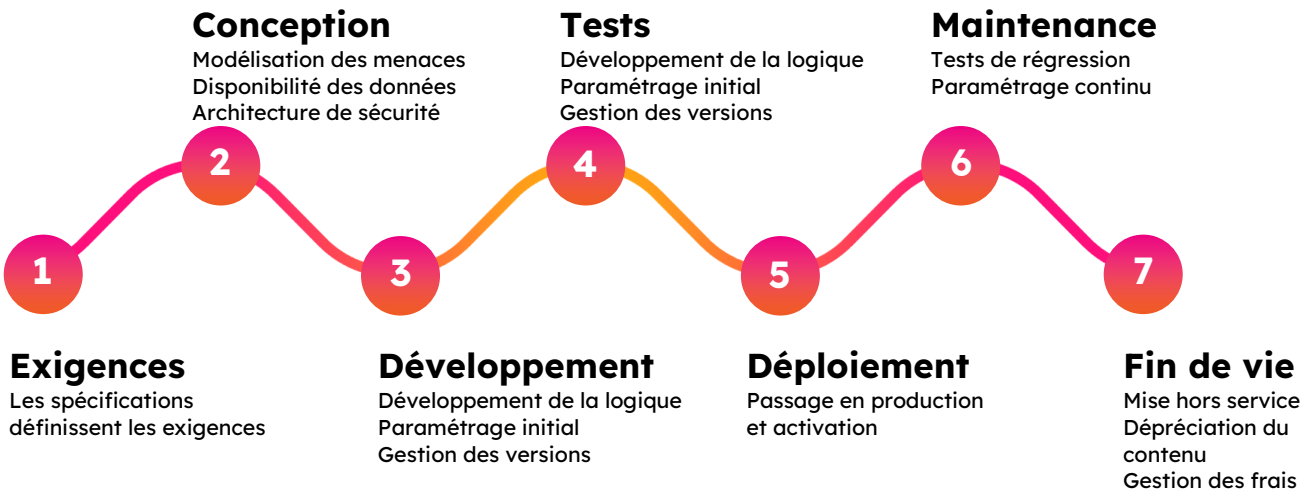
Un inventaire des scénarios d'utilisation est un système de suivi et d'organisation de vos scénarios d'utilisation. Il peut vous aider à suivre la couverture des scénarios à travers plusieurs outils et à vous assurer que vous disposez d'un point de référence unique pour montrer l'étendue de la couverture à vos parties prenantes. L'inventaire peut prendre la forme d'une feuille de calcul partagée ou s'appuyer sur une technologie de gestion des scénarios d'utilisation. Dans Splunk, vous pouvez utiliser Splunk Security Essentials pour mapper et gérer vos scénarios d'utilisation. Splunk Security Essentials étant une application Splunkbase disponible gratuitement, rien ne vous empêche de l'utiliser pour commencer à suivre et à mapper les scénarios d'utilisation avant la mise en œuvre de Splunk Enterprise Security.

Cycle de vie des scénarios d'utilisation

Lors de la mise en place d'un nouveau SIEM, vous avez l'occasion d'évaluer la façon dont votre organisation suit et déploie ses scénarios d'utilisation. De nombreuses organisations tombent dans le piège d'ajouter continuellement des scénarios d'utilisation techniques sans valider les scénarios précédemment mis en œuvre pour s'assurer qu'ils sont toujours fonctionnels et qu'ils sont toujours source de valeur. Cela peut entraîner un surplus de scénarios d'utilisation, ce qui affecte les performances des systèmes et se traduit par des alertes de faible qualité, des faux positifs ou, pire encore, des faux négatifs, les analystes partant du principe qu'il existe une couverture.

Le cycle de vie d'un scénario d'utilisation est un système permettant de suivre un scénario à travers ses différentes étapes et de s'assurer qu'un scénario est toujours une source continue de valeur. Dans le cas contraire, il est désactivé. Il peut atténuer le risque de dégradation des scénarios d'utilisation grâce à des tests, une maintenance et une mise hors service continus des scénarios qui ne sont plus pertinents.

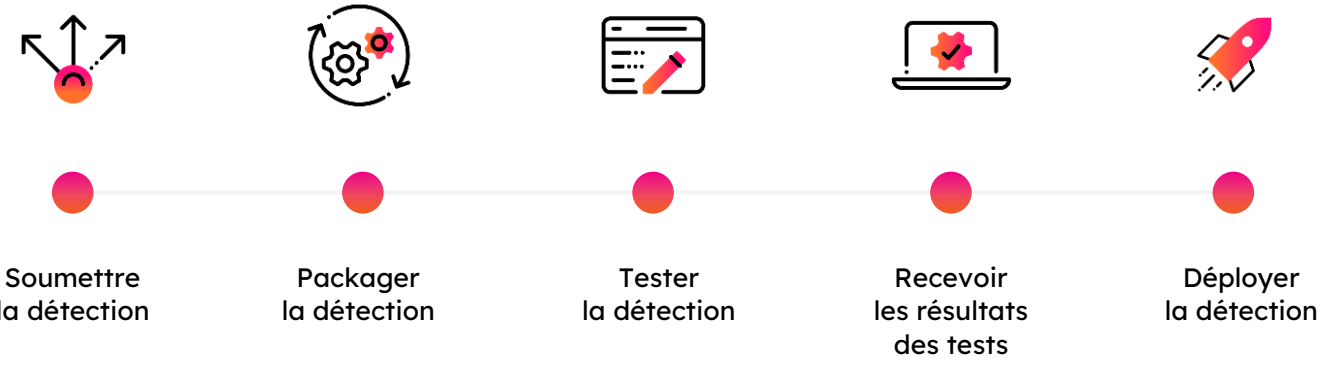
Splunk Professional Services peut vous aider à concevoir et à documenter le cycle de vie d'un scénario d'utilisation pour répondre à vos exigences métiers. Vous pouvez mettre en place ces cycles via Splunk Security Essentials et des méthodologies CI/CD.



Exemple du cycle de vie d'un scénario d'utilisation de Splunk

Détection en tant que code et CI/CD

La détection en tant que code désigne la pratique consistant à stocker les recherches de corrélation non seulement en tant qu'artefacts dans un SIEM, mais aussi en tant que code pouvant être contrôlé et géré par version, tout comme vous le feriez pour un logiciel dans le cadre d'un cycle de vie de développement logiciel standard. Cette pratique rend la gestion des détections robuste et évolutive et favorise le déploiement de détections de qualité.



Splunk prend directement en charge les méthodologies de détection en tant que code. Splunk fournit également un outil personnalisé, content ctl, qui facilite considérablement le processus de gestion de la détection en tant que code par le biais de pratiques CI/CD, et prend en charge les tests atomiques des détections grâce à son outil Attack Range.

Path to Live

Path to Live désigne la pratique consistant à tester le contenu dans plusieurs environnements d'essai avant de l'intégrer dans un environnement de production principal. Cela fait généralement partie du cycle de vie

d'un scénario d'utilisation. Splunk facilite ce processus grâce à Splunk Security Essentials et aux technologies CI/CD décrites ci-dessus, qui peuvent vous permettre de tester facilement le contenu avant de le pousser en production – même si cet environnement de test est sur site et que votre environnement de production est basé sur Splunk Cloud.

Modèles de migration SIEM

SIEM sur site vers SIEM cloud/SIEM SaaS vers SIEM SaaS

Il existe quelques différences entre la migration d'un environnement sur site vers SaaS et le passage direct d'un service SaaS à un autre service SaaS. Examinons l'impact que ces options pourraient avoir sur le remplacement de votre SIEM, d'un point de vue à la fois métier et technique.

SIEM sur site vers SIEM SaaS

Lorsque vous passez d'un SIEM sur site à un SIEM SaaS, vous devez tenir compte du fait que vous effectuerez deux transformations en même temps : un remplacement de SIEM et une migration vers le cloud.

Cela ajoute quelques éléments à votre projet de remplacement :

- Vous devrez bien réfléchir à l'ordre de vos opérations. Le passage à un SIEM sur le cloud impliquera la mise hors service de votre matériel sur site, la mise en place d'un transfert de données à partir de votre environnement sur site et, ce qui sera peut-être le plus difficile pour vos équipes, l'adoption d'un état d'esprit cloud-first. Ce changement peut prendre du temps et les coûts de reconfiguration, de mise hors service et de mise en œuvre du cloud doivent être pris en compte dans votre budget.
- Si vous migrez des données de votre SIEM sur site vers une plateforme IaaS, vous devrez tenir compte des coûts d'entrée et de sortie des données. N'oubliez pas que vous risquez de devoir supporter des coûts supplémentaires pour l'entrée ou la sortie des données.
- Vous devrez vérifier quelles sont vos limites. Même si vous passez d'un SIEM sur site à un SIEM dans le cloud auprès d'un même fournisseur, n'oubliez pas que si vous passez à une plateforme SaaS, comme son nom l'indique, il ne s'agit que d'un service. Ce n'est pas parce que vous faisiez quelque chose dans votre environnement sur site, sur lequel vous aviez un contrôle total, qu'il sera possible de faire la même chose dans votre nouvel environnement cloud. Des limites existent pour assurer votre sécurité et garantir que votre service est fourni conformément à ce que vous avez payé, mais assurez-vous bien de comprendre ces limites avant de migrer.

SaaS vers SaaS

Passer d'un SIEM SaaS vers un autre SIEM SaaS simplifie quelque peu les choses. La migration vers le cloud n'est plus un problème, mais il y a encore quelques points à prendre en compte :

- **Vérifiez les règles relatives aux données.** Il se peut que votre fournisseur actuel de SIEM cloud ne vous permette pas de migrer les données hors de la plateforme, ou qu'il vous impose des frais supplémentaires. Vous devrez lire votre contrat de service SaaS pour comprendre ce qui est autorisé ou non.

8. Présentation de Splunk Professional Services

Introduction

L'équipe Splunk Professional Services met son expertise à votre disposition pour vous aider à créer de la valeur plus rapidement, à optimiser et à améliorer votre instance Splunk et à identifier de nouvelles fonctionnalités à partir de votre investissement.

La proposition de valeur de Splunk Professional Services

Splunk Professional Services réalise des projets dans le monde entier pour des organisations comme la vôtre.

Splunk Professional Services en un coup d'œil

Une équipe œuvrant à la réussite de nos clients !

+ de 1 800
experts Splunk

Augmenter ou réduire les ressources en fonction de la demande

+ de 5 000
accréditations

Accès anticipé aux nouveaux produits Splunk

+ de 1 000
projets réalisés chaque année

Accès direct aux équipes d'ingénierie et d'assistance de Splunk

91
entreprises du Fortune 100

Vaste réseau de partenaires certifiés

110
pays

Des résultats probants

Splunk Professional Services propose des offres sur mesure à votre organisation. Cette approche flexible nous permet d'établir rapidement un cahier des charges et un devis, tout en nous adaptant à vos besoins.

	Déploiement Splunk Enterprise	Sources de données	Déploiement Splunk ES	Scénarios d'utilisation
Base	✓	**7**	✓	**5-10**
Standard	✓	**9**	✓	**10-20**
Premium	✓	**+ de 9**	✓	**+ de 20**

Formules de Splunk Enterprise Security

Pour commencer à concevoir et à mettre en œuvre un SIEM de pointe, vous pouvez contacter votre équipe Splunk dès aujourd'hui ou utiliser le site web de Splunk pour contacter directement Splunk Customer Success.

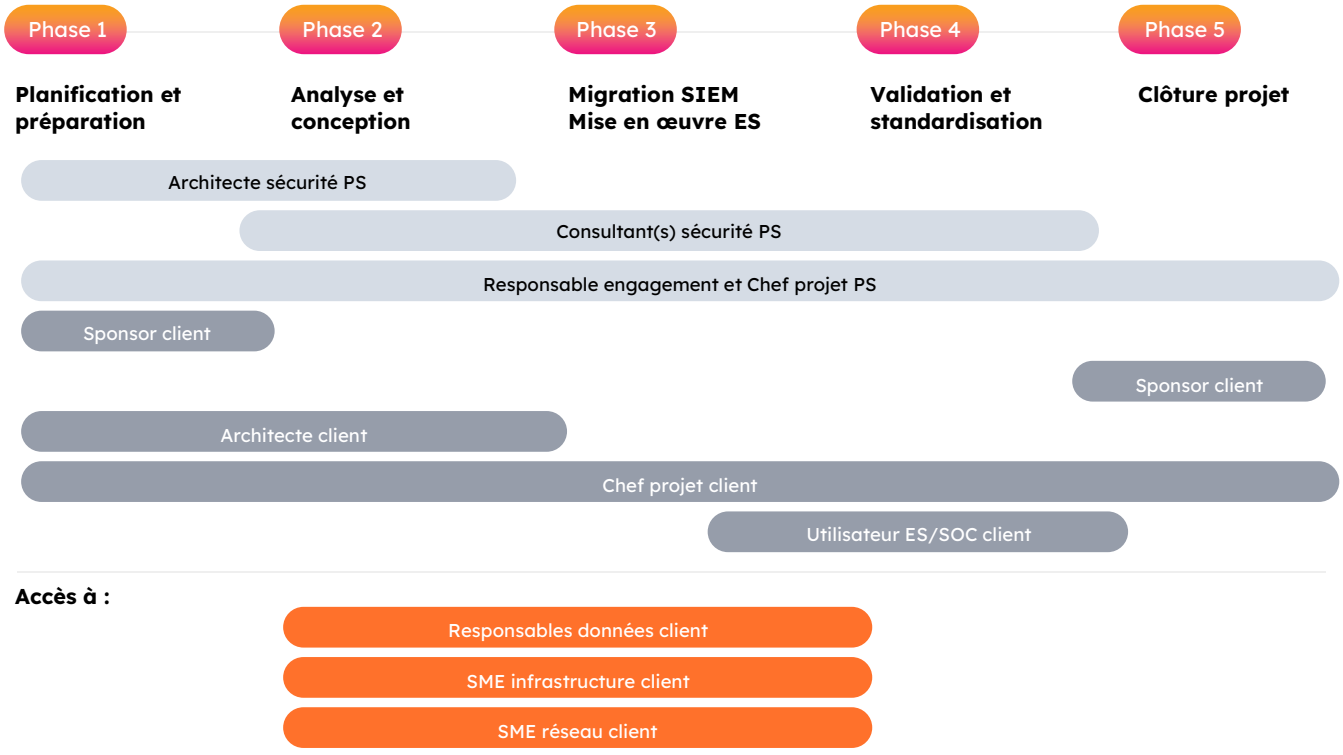
9. L’approche Splunk du remplacement d’un SIEM

Présentation de la méthodologie de Splunk Professional Services

Notre équipe Splunk Professional Services est très efficace et peut entraîner une création de valeur et une rentabilisation rapides. Notre équipe d’experts a mené à bien des centaines de projets de remplacement de SIEM et continue d’évoluer et d’optimiser son approche afin de pouvoir gérer n’importe quel projet.

Splunk Professional Services suit une approche rigoureuse, qui a montré son efficacité dans le monde entier. Elle se décompose en cinq phases :

Abordons plus en détail chacune d’entre elles pour mieux comprendre leur rôle.



Aperçu conceptuel des phases de mise en œuvre utilisées par Splunk Professional Services

Planification et préparation

Cette phase d’engagement décrit les activités initiales de planification. La durée de cette phase peut varier en fonction de l’ampleur du projet.

Cette phase englobe généralement les activités suivantes :

- définir la méthodologie et les échéances du projet,
- se mettre d'accord sur les grandes lignes des livrables,
- créer et se mettre d'accord sur un plan de mise en œuvre,
- mobiliser les ressources,
- réunions de lancement.

Analyse et conception

Cette phase d'engagement consiste à analyser toute solution existante et à définir la future solution SIEM. Les architectes et les chefs de projet de Splunk travailleront à la collecte et à la documentation des différentes exigences, puis consigneront les bonnes pratiques de Splunk afin d'accélérer le délai de rentabilité et la concrétisation de la valeur à long terme. Cette phase est cruciale pour un projet de remplacement de SIEM car elle pose les bases de la réussite du projet, à la fois pour l'équipe Splunk Professional Services qui effectue toutes les activités de mise en œuvre en aval, mais aussi pour la valeur potentielle pour le client à long terme.

Atelier de remplacement de SIEM

Un atelier de remplacement de SIEM se compose d'un atelier de développement de scénarios d'utilisation et d'un atelier de conception de SIEM. Ces deux ateliers peuvent être réalisés séparément, mais comme ils sont tous les deux nécessaires pour réussir son remplacement de SIEM, il est plus facile de les regrouper.

Un atelier de développement de scénarios d'utilisation Splunk vise à :

- effectuer des recherches pour analyser l'état actuel et planifier l'état futur de votre environnement SIEM,
- définir les bonnes pratiques et approches pour créer de la valeur à partir de vos scénarios d'utilisation métiers avec votre nouveau SIEM,
- rédiger une feuille de route des scénarios d'utilisation en plusieurs phases, qui soutient à la fois la mise en œuvre immédiate par Splunk Professional Services et la mise en œuvre à long terme par le client.

Cet atelier est une activité de niveau architecte de Splunk Professional Services. Il est très fortement recommandé dans le cadre de tout remplacement de SIEM dirigé par Splunk Professional Services.

Mappage des scénarios d'utilisation

Un atelier de développement de scénarios d'utilisation Splunk permet une rentabilisation rapide en vous permettant d'abord de comprendre les scénarios d'utilisation métiers que vous essayez d'appliquer avec votre stratégie de détection et de supervision, puis de mapper une combinaison de fonctionnalités prêtes à l'emploi de Splunk et de nouvelles fonctionnalités personnalisées pour parvenir à les concrétiser. Ce processus de mappage peut inclure n'importe quel produit du portefeuille de sécurité de Splunk, y compris les applications disponibles gratuitement telles que Splunk Security Essentials ou Splunk SOAR, en fonction de l'étendue du projet.

Splunk Professional Services apporte une connaissance et une expérience approfondies des scénarios d'utilisation de base de Splunk, ainsi que des recommandations pour obtenir une rentabilisation rapide en fonction des exigences. Lorsque qu'il n'existe pas de contenu prêt à l'emploi, Splunk Professional Services peut concevoir un modèle pour développer des scénarios d'utilisation personnalisés permettant au client, seul ou en collaboration avec Splunk Professional Services, de gérer le développement d'un contenu personnalisé.

Remplacement à l'identique ou en fonction des objectifs

Remplacement à l'identique

Lorsqu'elles envisagent de remplacer leur SIEM, de nombreuses organisations s'orientent naturellement vers une stratégie de remplacement de leur SIEM à l'identique. Dans cette optique, le nouveau SIEM doit d'abord démontrer qu'il peut gérer des scénarios d'utilisation *techniques* et répondre à des niveaux d'ingestion de données identiques à ceux du SIEM précédent avant de passer à du nouveau contenu. Cette approche est souvent une erreur. Le mappage du contenu technique de votre SIEM existant vers Splunk Enterprise Security a beau être simple et rapide, il n'est pas nécessairement synonyme de valeur ajoutée proportionnelle.

Considérons les affirmations suivantes :

- Vous remplacez votre ancien SIEM pour une raison valable, telle qu'un TCO ou des fonctionnalités insuffisantes.
- Vous souhaitez contrôler votre TCC et le maintenir à un niveau acceptable. Cela signifie que vous ne pouvez pas consacrer de temps à une activité qui n'est pas directement source de valeur.
- Votre nouveau SIEM fonctionne différemment de votre ancien SIEM, notamment grâce à des méthodes différentes et vraisemblablement meilleures, pour créer des contenus de recherche de corrélation ou d'autres scénarios d'utilisation techniques, ainsi que pour gérer et stocker les données pertinentes.

Si ces affirmations sont vraies, alors pourquoi voudriez-vous reproduire le contenu de votre ancienne solution SIEM alors que vous savez qu'elle ne vous a pas donné satisfaction ? Au début de cette section, nous avons dit que nous envisagions ici le remplacement à l'identique des scénarios d'utilisation techniques.
Même si nous nous en tenons à cette déclaration, pour autant, tout n'est pas à jeter. Nous devrions plutôt nous pencher sur les scénarios d'utilisation métiers, parfois également appelés scénarios d'utilisation de haut niveau, qui pourraient bien s'avérer tout aussi pertinents aujourd'hui qu'ils ne l'étaient auparavant.

	Niveaux des scénarios	Exemples
	Exigences métiers	Prévenir les risques métiers inacceptables, les ransomwares étant la plus grande source de risque
Haut niveau	Scénarios d'utilisation métiers	Détecter et signaler les ransomwares
Bas niveau	Scénarios d'utilisation techniques	**Règle de corrélation 1 :** une recherche de corrélation Splunk ES détectant les déplacements latéraux via les logs réseaux
		Règle de corrélation 2 : une recherche de corrélation Splunk ES détectant un IoC spécifique sur un log associé à un ransomware à partir de logs EDR agrégés
		Tableau de bord 1 : un tableau de bord montrant les incidents de ransomwares pour toutes les détections, etc.

Il en va de même pour les données. Les données dont vous avez besoin pour appliquer les scénarios d'utilisation de votre ancien SIEM ne sont pas nécessairement les mêmes que celles nécessaires pour les scénarios d'utilisation de votre nouveau SIEM.

Remplacement en fonction des objectifs

Nous avons expliqué pourquoi, lorsque vous passez d'un ancien SIEM à Splunk, vous devriez envisager de ne plus tenir compte de vos scénarios d'utilisation *techniques* précédents. Cependant, vos scénarios d'utilisation métiers pourraient toujours être valables, et c'est là que Splunk Professional Services intervient pour appliquer notre processus de découverte. Une fois que nous comprenons les objectifs que vous essayez d'atteindre avec votre nouvelle solution SIEM, nous pouvons alors mapper ces scénarios d'utilisation métiers à des scénarios techniques de bas niveau dans Splunk. Cela signifie que nous pouvons utiliser notre contenu prêt à l'emploi et les bonnes pratiques de Splunk pour produire rapidement de la valeur en lien avec vos objectifs, plutôt que de compromettre votre TCC en perdant du temps à essayer de reproduire le contenu de votre ancien SIEM.

SIEM basé sur l'ingestion/SIEM basé sur les scénarios d'utilisation

Lors de la mise en place d'un SIEM, que ce soit pour la première fois ou pour remplacer un système existant, vous devez évaluer votre stratégie en matière de données. Votre stratégie de données est l'approche à long terme que vous adoptez pour déterminer quelles données vous importerez dans votre SIEM et comment vous les classerez.

SIEM basé sur l'ingestion

La stratégie de nombreuses organisations se base sur l'ingestion. Cette stratégie met d'abord l'accent sur l'importation des données dans la plateforme. Il s'agit ensuite de découvrir et d'élaborer des applications à valeur ajoutée à partir de ces données. Cette stratégie est populaire pour plusieurs raisons :

1. **Sa simplicité** : il est facile de commencer par des sources de données importantes et évidentes et de les importer dans votre SIEM, puis de déterminer ensuite comment les utiliser. Cependant, bien que cette approche puisse être pertinente initialement, elle s'essouffle rapidement, car les données en elles-mêmes n'apportent pas de valeur. Dans le pire des cas, le SOC est évalué non pas en fonction de la valeur qu'il apporte, mais plutôt en fonction de la quantité de nouvelles données qu'il importe dans la solution SIEM, augmentant ainsi l'impression de « couverture » du parc technologique de l'organisation.
2. **Le SIEM est un service :** le SIEM est fourni en tant que service à tout un éventail d'unités métiers. En raison de la façon dont cette approche est parfois structurée, il existe une séparation entre ces unités métiers et le SIEM, ce qui fait que les unités métiers soumettent simplement leurs données au SIEM et qu'une équipe de sécurité distincte en retire ensuite de la valeur. Ce processus, bien que quelque peu dysfonctionnel, est assez courant.
3. **La conformité :** il s'agit là de la raison la plus valable d'adopter une stratégie de données basée sur l'ingestion. Certains sous-ensembles de données peuvent être qualifiés de nécessaires à des fins de conformité, par exemple pour respecter certaines réglementations ou exigences d'audit. Dans ce cas, quelles que soient les possibilités d'utilisation des données, celles-ci doivent être importées dans le SIEM pour éviter des sanctions.

Bien que ces raisons puissent toutes être valables, le fait de suivre l'une ou l'autre de ces stratégies basées sur l'ingestion entraîne une fracture entre les données elles-mêmes et les scénarios d'utilisation de sécurité que le SOC doit prendre en charge. De plus, le simple fait d'ingérer des données sans comprendre comment ces données seront utilisées dans le SIEM pour créer de la valeur peut générer des coûts sans aucun résultat réel de sécurité.

Splunk Professional Services peut prendre en charge une stratégie de données basée sur l'ingestion, et dans certaines situations, cela peut s'avérer avantageux, voire nécessaire – par exemple à des fins de conformité. En règle générale, cependant, l'approche privilégiée consiste à adopter une stratégie de données basée sur les scénarios d'utilisation.

SIEM basé sur les scénarios d'utilisation

Dans le cadre d'une stratégie de données basée sur les scénarios d'utilisation, nous orientons plutôt nos priorités d'ingestion de données en fonction de leur relation avec nos scénarios d'utilisation prioritaires. Dans ce scénario, nous prenons en compte les exigences de l'entreprise et nous les mettons en correspondance avec les scénarios d'utilisation métiers. Ces scénarios de haut niveau déterminent alors des scénarios techniques de bas niveau, classés par ordre de priorité en fonction de leur valeur pour l'entreprise et d'une liste de sources de données disponibles connues. Certaines de ces sources de données existent peut-être déjà dans votre SIEM actuel, mais d'autres ne sont peut-être pas encore ingérées. Cela signifie que nous pouvons prioriser nos efforts d'intégration des sources de données en fonction des résultats que les données sont censées générer pour l'entreprise. Cela garantit également la traçabilité de l'atténuation des risques, des exigences métiers aux scénarios d'utilisation techniques, et nous permet de justifier les données que nous ingérons à chaque étape du processus.

Approche par phase : scénarios d'utilisation et données

Scénarios d'utilisation

La valeur ajoutée la plus rapide que Splunk Professional Services peut apporter est d'aider le client à prioriser l'implémentation des scénarios d'utilisation via une approche standardisée et divisée en plusieurs phases, en s'appuyant sur notre expertise.

Par exemple, pour un client dont la priorité absolue est la détection des ransomwares, nous pourrions suivre les phases suivantes :

- **Phase 1** – Scénarios d'utilisation critiques : nous devons activer les scénarios d'utilisation associés aux indicateurs de compromission des ransomwares et intégrer les sources de données de détection et de réponse des points de terminaison (EDR) pour permettre l'identification des scénarios critiques conformément aux priorités de MITRE ATT&CK.
- **Phase 2** – Scénarios d'utilisation prioritaires : nous devons activer d'autres scénarios plus complexes et intégrer d'autres sources de données.
- **Phase 3** – Scénarios d'utilisation personnalisés : nous devons créer des scénarios personnalisés pour répondre aux besoins métiers et intégrer les sources de données associées, notamment en configurant des scénarios de détection d'anomalies basés sur le machine learning adaptés aux besoins du client.

Ces phases sont toujours personnalisées en fonction des exigences de chaque client, et Splunk Professional Services créera une feuille de route d'implémentation des scénarios d'utilisation couvrant chaque phase. Splunk Professional Services ne travaille généralement avec le client que pour mettre en œuvre la première phase, car l'objectif est d'assurer une rentabilisation rapide et de former les équipes des clients afin qu'elles prennent ensuite le relais pour les prochaines phases. Veuillez cependant noter que Splunk Professional Services peut réaliser l'intégralité d'un projet de remplacement de SIEM si le client le souhaite.

Données

Splunk Professional Services peut rédiger une feuille de route en plusieurs phases des scénarios d'utilisation prioritaires, avec les sources de données prioritaires qui leur sont associées. Cette hiérarchisation peut également permettre de s'assurer que les sources de données sont importées en même temps que leurs sources de données associées. Vous pouvez alors soit commencer par une approche big bang, en migrant les sources de données de l'ancien SIEM, en collaboration avec l'équipe Splunk Professional Services pour transférer toutes vos sources de données dans le cadre d'une phase de migration préalable, ou vous pouvez procéder à un dual forwarding à plus long terme. Quoi qu'il en soit, Splunk Professional Services peut s'assurer que vous disposez d'une stratégie complète pour importer les

bonnes données au bon moment afin de rentabiliser rapidement votre migration et d'éviter les coûts inutiles.

Planification

Un programme typique pour un atelier de développement de scénarios d'utilisation de cinq jours peut inclure une journée de découverte et la participation des principales parties prenantes du client, telles que le sponsor du projet. Après une courte séance d'ouverture avec les participants du client, le reste de la journée ne concerne que l'équipe de projet du client.

Le programme peut ressembler à ceci :

Jour 1

- Première moitié : Découverte
- Deuxième moitié : Conseils

Jour 2

- Première moitié : Conseils
- Deuxième moitié : Documentation

Jour 3

- Première moitié : Conseils/Mappage et création du contenu
- Deuxième moitié : Documentation

Jour 4

- Première moitié : Conseils/Mappage et création du contenu
- Deuxième moitié : Documentation

Jour 5

- Activités restantes ; présentation à l'équipe de projet client pour la rédaction finale
- Documentation

Le résultat d'un atelier de développement de scénarios d'utilisation est généralement une feuille de route personnalisée de mise en œuvre de scénarios d'utilisation mappés à vos sources de données.

Atelier de RBA

Un atelier de RBA vise à soutenir la mise en œuvre de votre SIEM en établissant la feuille de route pour votre RBA. Il peut être organisé dès le départ ou après la mise en œuvre de votre SIEM. Splunk Professional Services peut utiliser les résultats d'un atelier RBA pour mettre en place la RBA, ou vous pouvez utiliser les résultats pour la mettre en œuvre vous-même, soit avec vos équipes, soit avec un partenaire de Splunk.

Suite à l'atelier, vous disposerez d'une feuille de route et d'un plan de mise en œuvre de la RBA.

Atelier de conception de SIEM

Faisant partie de l'atelier de remplacement SIEM, cet atelier consiste à dresser les contours de tous les éléments de la solution SIEM de remplacement.

L'atelier peut aborder :

- la configuration des actifs et des identités,
- la configuration de la threat intelligence,
- le workflow de case management des analystes,
- le dual forwarding,

- la multi-tenancy,
- la classification des données,
- la recherche fédérée,
- les architectures SIEM hybrides,
- les exigences en matière de menaces internes.

Planifier la mise en place de votre plateforme SIEM Splunk peut vous amener à réfléchir à divers facteurs architecturaux. Ces facteurs peuvent avoir un impact significatif, à tel point que nous avons consacré une section de ce document à leur prise en compte.

Suite à l'atelier, vous disposerez d'un document de conception de SIEM.

Atelier de conception de plateforme

Cet atelier consiste à concevoir la plateforme Splunk sous-jacente sur laquelle le SIEM Splunk fonctionnera. Il s'agit d'un atelier d'architecture Splunk typique. Il prend la Splunk Validated Architecture adaptée pour répondre aux exigences d'échelle et de disponibilité du client, puis la personnalise. Ce processus est tout aussi important dans une configuration Splunk Cloud, où des considérations telles que les couches intermédiaires de transfert de données, les intégrations de cloud à cloud et les modèles CI/CD basés sur Admin Config Service (ACS) devront être abordées, entre autres.

Si la plateforme du client est extrêmement simple – par exemple, un seul nœud tout-en-un ou Splunk Cloud avec des sources de données de cloud à cloud uniquement – ces sujets peuvent être inclus dans l'atelier de conception de SIEM.

L'atelier peut aborder :

- le choix d'une Splunk Validated Architecture adaptée aux besoins du client identifiés pendant cet atelier et tout autre atelier précédent,
- le dimensionnement,
- les échéances d'intégration,
- la planification de la couche de forwarding intermédiaire, le cas échéant,
- la conception de la RBAC,
- la planification de l'indexation et de la conservation des données,
- la conception d'un Edge Compressor, le cas échéant,
- la conception d'un serveur de déploiement.

Pour les projets d'une ampleur suffisante, les étapes de conception RBAC et de planification de l'indexation et de conservation des données peuvent faire l'objet d'ateliers dédiés.

Suite à cet atelier, vous disposerez d'un document de conception de plateforme Splunk.

Atelier de conception de plateforme SOAR

Cet atelier consiste à concevoir la plateforme Splunk sous-jacente sur laquelle le SIEM Splunk fonctionnera. Il s'agit d'un atelier d'architecture Splunk standard, qui prend la Splunk SOAR Validated Architecture adaptée aux exigences d'échelle et de disponibilité du client, puis la personnalise.

L'atelier peut aborder :

- le choix d'une Splunk SOAR Validated Architecture adaptée aux besoins du client identifiés pendant cet atelier et tout autre atelier précédent,
- le dimensionnement,
- la planification de la HA (haute disponibilité),
- les échéances d'intégration,

- la planification de la couche intermédiaire, le cas échéant ; par exemple à l'aide d'Automation Brokers,
- la conception de la RBAC.

Suite à cet atelier, vous disposerez d'un document de conception de plateforme SOAR.

Atelier de conception de plan de réponse SOAR

Splunk peut vous aider dans votre parcours de maturité SOAR et propose des formules flexibles pour l'implémentation de Splunk SOAR. La première étape est un atelier de conception. L'équipe Splunk Professional Services travaille avec le client pour choisir la bonne méthode d'implémentation, puis conçoit les plans de réponse adaptés pour répondre aux scénarios d'utilisation du client. Les plans de réponse sont des constructions logiques qui répondent à un scénario d'utilisation et sont constitués de playbooks modulaires.

Suite à cet atelier, vous disposerez d'un plan de réponse Splunk

Build (Mise en œuvre)

Mise en œuvre du SIEM

L'approche de mise en œuvre de SIEM de Splunk prévoit l'intégralité du déploiement.

Elle peut inclure :

- l'intégration des données et la configuration de la conformité au CIM,
- la configuration de la Splunk Enterprise Security App,
- la configuration du Splunk Threat Intelligence Framework,
- la configuration du Splunk Asset and Identity Framework,
- la configuration des scénarios d'utilisation de Splunk,
- la formation de vos équipes,
- la configuration des intégrations.

Suite à cette mise en œuvre, votre SIEM Splunk sera entièrement configuré.

Mise en œuvre du SOAR

Une fois le modèle d'architecture adapté choisi, Splunk Professional Services fournira les ressources nécessaires pour installer et configurer Splunk SOAR et commencer le processus d'intégration de la liste préliminaire d'intégrations pour ingérer les événements, rechercher des informations et effectuer des actions. Cela inclut l'intégration de SOAR avec Splunk Enterprise Security.

L'équipe Splunk Platform a identifié trois catégories de playbooks :

- Enrichissement : effectuer le travail préparatoire avant la présentation aux analystes.
- Utilité : régit les tâches quotidiennes réalisées par les équipes de sécurité.
- Autonome : réponse entièrement automatisée avec prise de décision humaine, au besoin.

L'équipe SOAR travaillera avec vous pour exploiter notre bibliothèque d'exemples de playbooks afin d'offrir des capacités d'automatisation et d'orchestration de la sécurité pour aider les équipes de sécurité.

Suite à cette mise en œuvre, votre déploiement Splunk SOAR sera configuré et vous disposerez d'un ou plusieurs plans de réponse Splunk SOAR.

Validation

Vue d'ensemble

Cette étape confirme que la mise en œuvre a été réalisée conformément aux bonnes pratiques de Splunk.

Passation du projet

Cette étape couvre la transmission du projet de l'équipe Splunk Professional Services à vos équipes. Elle implique le partage de la documentation finale et la clôture du projet.

L'approche flexible de Splunk Professional Services

Collaboration

Splunk Professional Services suit une approche collaborative. Cela signifie que nous ne nous attendons pas à prendre le contrôle de votre environnement, ni à ce que vos équipes se retrouvent face à une solution qu'elles ne comprennent pas. Chaque étape de notre mise en œuvre vise à garantir que vos équipes reçoivent la formation théorique et l'expérience pratique dont elles ont besoin pour réussir avec Splunk. Dans la mesure du possible, nous travaillerons aux côtés de vos équipes sur les activités d'implémentation et nous collaborerons avec elles pour nous assurer que le produit final répond à leurs attentes et à leurs exigences, même si celles-ci évoluent.

Adaptabilité

Splunk fonctionne sur la base d'un modèle flexible. Nous utilisons donc des formules pour structurer l'étendue de l'engagement et garantir que les petites organisations disposent d'options rentables, prévisibles et prêtes à l'emploi. Lorsque nous devons personnaliser notre approche pour répondre aux besoins de nos clients, nous n'hésitons pas ; nous pouvons également adapter notre approche aux plus grands clients et projets du monde.

Assistance prescriptive/réactive

L'équipe Splunk Professional Services peut adopter une approche d'assistance à la fois prescriptive et réactive, en fonction des besoins du client. Lorsqu'elle est prescriptive, nous pouvons orienter vos équipes vers les modèles et les cadres de sécurité sur lesquels s'appuient les organisations de taille et de secteurs similaires. Lorsque nos clients savent ce qu'ils veulent, nous pouvons passer à une approche plus réactive, en tenant compte de leurs exigences et en adaptant notre approche à leurs besoins.

Échéances et livraison simultanée

Splunk est capable d'assurer la livraison simultanée de plusieurs parties du projet. Cela nous permet de raccourcir les délais de mise en œuvre, notamment si vous découvrez que vous avez un délai à respecter, par exemple si la licence de votre ancien SIEM arrive à expiration.

Pour ce faire, nous faisons appel à des chefs de projet Splunk pour superviser plusieurs workflows, en veillant à ce que les travaux soient réalisés efficacement et sans chevauchement.

Il reste toutefois important de planifier votre remplacement longtemps à l'avance afin de vous donner suffisamment de temps pour une transition sans risque important pour l'entreprise.

Concrétisation de la valeur après la mise en œuvre

Splunk ne propose pas uniquement des services d'implémentation. Splunk Professional Services et des services d'abonnement peut être utilisés pour obtenir des conseils sur la création de valeur.

Collaborer avec Splunk tout au long de votre parcours de données

Optimisez votre investissement Splunk à n'importe quelle étape

Accélérer
le délai de rentabilité

Déployez et adoptez
des services d'implémentation et d'adoption

Optimiser
votre solution

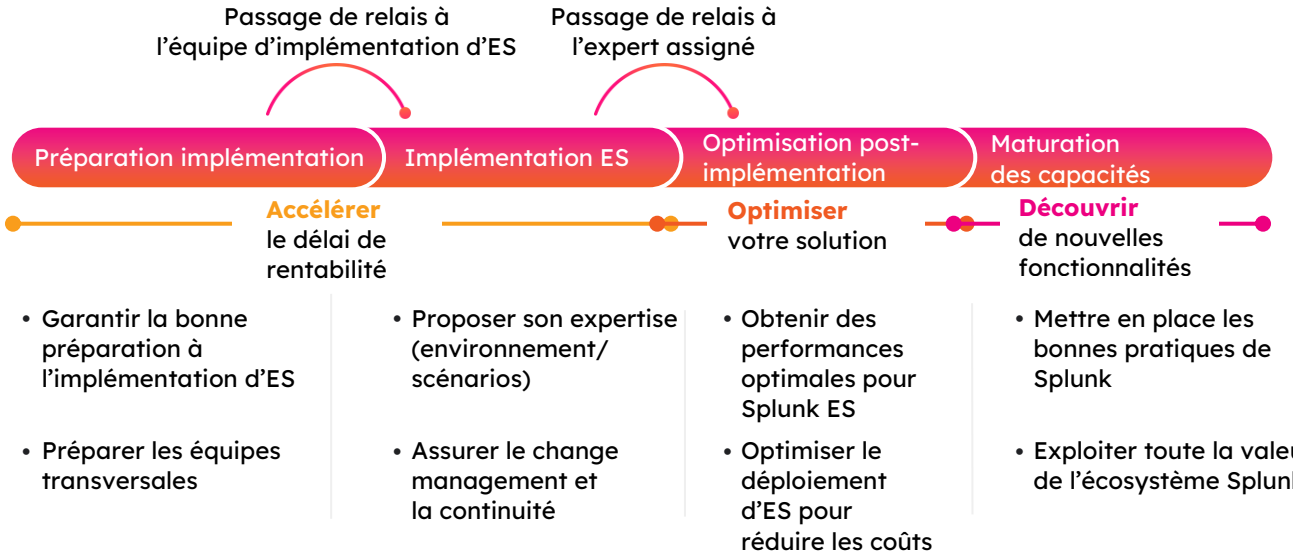
Faites appel
à des services de conseil et de modernisation

Découvrir
de nouvelles fonctionnalités

Faites évoluer
des solutions de conseil stratégique

Assistance Premium (formation incluse)

Le service d'abonnement Premium de Splunk est l'expert assigné. Il s'agit d'une période pendant laquelle un expert Splunk vous aidera à tirer le maximum de valeur de votre investissement Splunk.



Splunk propose également des services à la demande, qui fonctionnent comme un service d'abonnement à base de crédits. Vous pouvez y faire appel pour réaliser des tâches ponctuelles sans avoir à rédiger de cahier des charges.

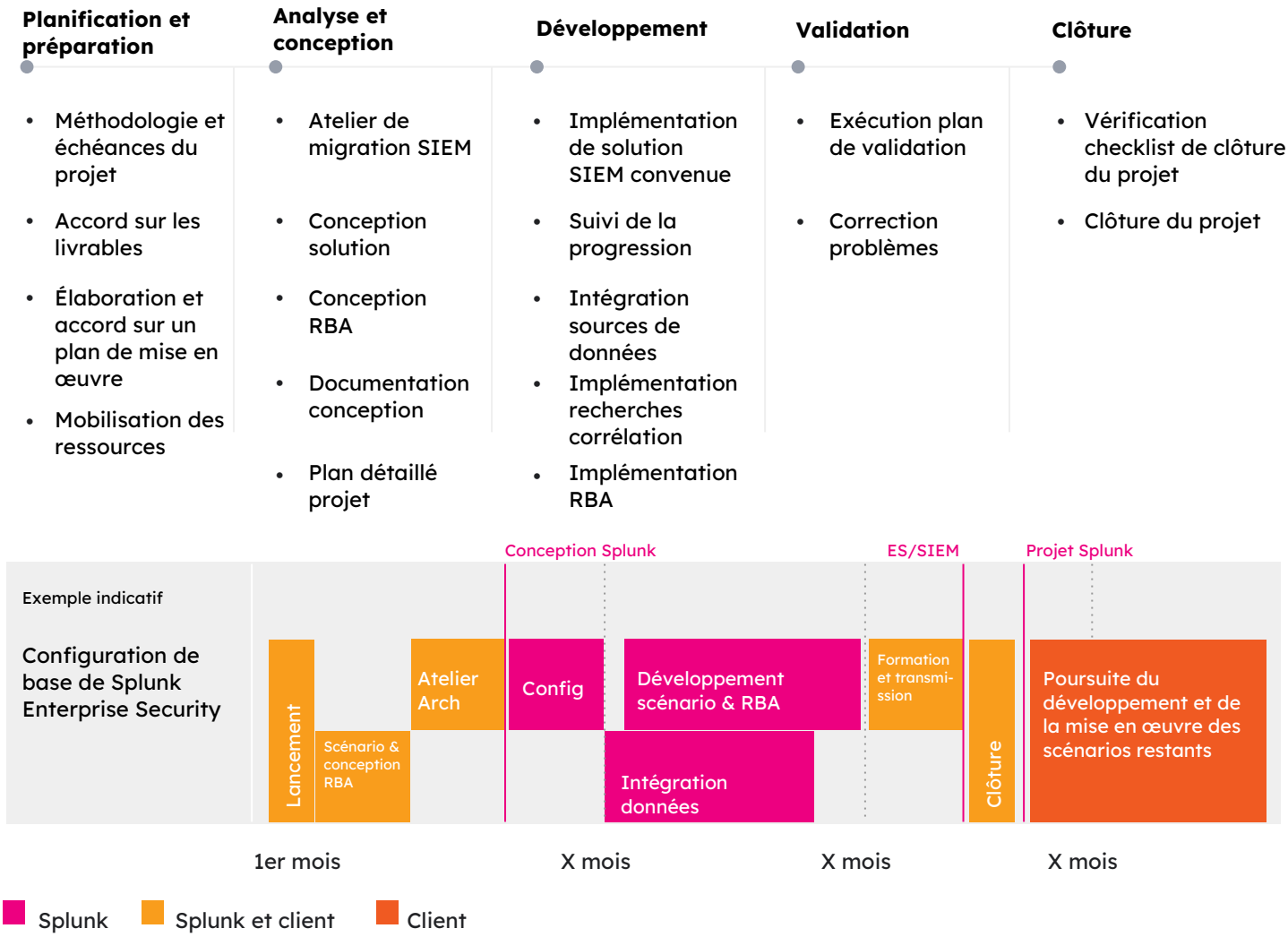
Détail des services à la demande (ODS)

Réalisez des activités courantes liées à l'utilisation et à la gestion des produits Splunk

Optimiser les résultats **Cataloguez les tâches par discipline :** Base, ITOA, Sécurité, DevOps	**Accélérer**	**Optimiser**	**Découvrir**
	Exécutez rapidement les tâches quotidiennes une fois opérationnel		
• Abonnement : via des plans de réussite • Activités prédéfinies ; aucun SOW nécessaire • Pool de ressources expérimentées	• Créer de la valeur plus rapidement en mettant en place le premier scénario d'utilisation • Accéder aux conseils techniques nécessaires pour réussir	• Intégrer les données et créer de nouveaux tableaux de bord • Peaufiner en appliquant les bonnes pratiques	• Planifier et préparer le déploiement de nouveaux scénarios • Apprendre à optimiser l'utilisation des nouvelles fonctionnalités

Conclusion

Comme nous l'avons vu, l'approche de remplacement d'un SIEM de Splunk est flexible et s'adapte aux besoins de chaque organisation. Bien que chaque organisation soit différente, nous pouvons visualiser comment les différentes étapes et les ressources de Splunk Professional Services peuvent s'imbriquer pour assurer un délai de rentabilité court grâce à notre approche collaborative.



Tâches Splunk Professional Services et client par phase

Annexe

Termes et acronymes

Terme	Description
SOC	Centre d'opérations de sécurité
TCO	Coût total de possession
TCC	Coût total du changement
TTV	Délai de rentabilité
Scénario d'utilisation	Application d'une technologie pour résoudre un problème métier. Chez Splunk PS, ils sont divisés en scénarios de haut et de bas niveau.
FTE	Équivalent temps plein
Coût global	Coût total d'un FTE, incluant tous les coûts et fonctions associés tels que les RH, la gestion, les dépenses, les soins de santé, etc.
Fidélité d'une alerte	Dans le contexte d'une recherche de corrélation Splunk, la fidélité d'une alerte fait référence à la probabilité que la recherche identifie avec précision un événement de sécurité spécifique.
Faible fidélité	Indique que la recherche peut générer des alertes non spécifiques ou des faux positifs plus fréquemment, ce qui nécessite une investigation plus approfondie pour confirmer la menace réelle.
Haute fidélité	Indique que la recherche est très spécifique et que les alertes générées sont susceptibles de mettre en évidence un vrai positif sans investigation approfondie nécessaire.
Faux positif	Alerte signalant de manière inexacte une menace de sécurité
Faux négatif	Alerte ne signalant pas une véritable menace de sécurité
Splunk Professional Services	Splunk Professional Services propose des conseils d'experts aux entreprises, les aidant à mettre en œuvre et à optimiser les solutions Splunk pour la sécurité, les opérations IT et la business intelligence, maximisant ainsi leur retour sur investissement.
RBA	Alertes basées sur les risques : framework d'alertes basé sur Splunk Enterprise Security
OOTB	Out-of-the-box : fonctionnalité prête à l'emploi intégrée au produit
MTTR	Temps moyen de réponse : délai moyen pour réagir à un incident
MTTA	Temps moyen de reconnaissance : délai moyen pour identifier ou trier un incident
EDR	Détection et réponse des points de terminaison : logiciel supervisant en permanence les endpoints (ordinateurs, serveurs, etc.) à la recherche d'activité suspecte, dans le but de détecter les cybermenaces telles que les malwares et les ransomwares et d'y répondre en temps réel
SSE	Splunk Security Essentials : application Splunkbase gratuite permettant aux utilisateurs de Splunk de mettre en œuvre plus rapidement des scénarios d'utilisation de sécurité en utilisant du contenu prêt à l'emploi activable en quelques clics.

Data lake	Sert de dépôt central pour le stockage et la gestion de tous les types de données brutes, quel que soit leur format ou leur structure, ce qui permet une analyse flexible et la découverte d'informations dans divers ensembles de données.
S3	Amazon S3 ou Amazon Simple Storage Service : solution de stockage d'objets hautement évolutive et rentable offrant une durabilité, une disponibilité et une sécurité inégalées pour le stockage de gros volumes de données
Recherche fédérée	La recherche fédérée Splunk permet d'effectuer des requêtes en toute simplicité sur plusieurs index et instances Splunk, quel que soit leur emplacement physique, offrant ainsi une vue unifiée des données pour des informations complètes sur la sécurité et les opérations.
SVA	Splunk Validated Architectures : architectures de référence éprouvées pour assurer des déploiements Splunk stables, efficaces et reproductibles
ACS	Admin Config Service : API cloud-native offrant des fonctionnalités d'administration programmatique en libre-service pour Splunk Cloud Platform. Les administrateurs de Splunk Cloud Platform peuvent utiliser l'API ACS pour effectuer des tâches administratives courantes sans l'aide de l'assistance Splunk.
Splunkbase	L'identification, l'ingestion et l'interprétation correctes des données est une étape fondamentale dans la réussite de votre mise en œuvre de vos solutions de sécurité Splunk. Si vous y parvenez, vous optimiserez au maximum la rentabilité de votre environnement Splunk. Pour ce faire, vous pouvez utiliser des add-ons et des applications Splunk, que vous retrouverez sur Splunkbase, pour accéder facilement à de nouvelles sources d'information renforçant votre position de sécurité. Les add-ons et applications créés par la communauté de Splunk visent à rendre l'importation de nouvelles données simple, efficace et accessible, et à vous aider à mettre en œuvre vos scénarios d'utilisation plus rapidement.
Attaque low and slow	Cyberattaque visant à perturber les systèmes en envoyant des quantités minimes de données sur une longue période. Ces attaques imitent un trafic légitime, ce qui les rend difficiles à détecter et peut conduire à l'épuisement des ressources et à la dégradation des services.
IaaS	Infrastructure en tant que service : fournit un accès à la demande à une infrastructure cloud, comme le stockage, le réseau et les serveurs virtuels, ce qui permet aux entreprises d'adapter leurs ressources en fonction de leurs besoins, sans avoir à gérer l'aspect matériel. La plupart des fournisseurs de cloud public offrent ce service.
SaaS	Logiciel en tant que service : offre des applications prêtes à l'emploi, hébergées dans le cloud et accessibles par le biais d'un navigateur web. Les entreprises peuvent s'abonner à des solutions SaaS, ce qui leur évite d'avoir à installer des logiciels, à les entretenir et à les mettre à jour sur leur propre infrastructure.
Splunk Cloud	Splunk Cloud Platform offre tous les avantages de la plateforme primée Splunk Enterprise sous la forme d'un service cloud. Avec Splunk Cloud Platform, vous bénéficiez des fonctionnalités de Splunk Enterprise pour la collecte, la recherche, la supervision, le reporting et l'analyse de toutes vos données machine historiques et en temps réel, grâce à un service cloud fourni de manière centralisée par Splunk à son large portefeuille de clients cloud, d'entreprises du Fortune 100 à des PME.
Splunk SmartStore	SmartStore est une fonctionnalité d'indexation qui permet d'utiliser des magasins d'objets distants, tels qu'Amazon S3, Google GCS ou Microsoft Azure Blob Storage, pour stocker des données indexées.

Rencontrez votre équipe Splunk Professional Services

Consultants

Les consultants Splunk Professional Services sont accrédités et expérimentés dans la mise en place de solutions Splunk. Ils ont chacun un domaine d'expertise et mettent à votre disposition leur connaissance approfondie du marché. Dans le cadre d'un remplacement de SIEM, ces consultants se spécialisent dans la sécurité.

Lors d'un remplacement de SIEM, ils se chargent notamment :

- d'implémenter la plateforme,
- d'implémenter le SIEM,
- d'implémenter les scénarios d'utilisation,
- de développer des applis Splunk,
- de développer des applis SOAR,
- de créer des playbooks SOAR,
- de configurer Splunk Enterprise Security,
    - de configurer et d'installer les applis Splunk Enterprise Security,
    - d'implémenter la RBA,
    - de configurer les actifs et les identités,
    - de configurer la threat intelligence,
- de former et de passer le relais aux équipes du client,
- d'organiser la réunion de lancement.

Architectes

Un architecte Splunk Professional Services est un spécialiste qui dirige des ateliers, met en place des architectures et assure des activités d'implémentation spécialisées. L'architecte est principalement impliqué en début de projet lors du remplacement d'un SIEM, mais selon l'ampleur du projet, il peut également superviser une équipe tout au long des différentes phases du projet.

Dans le cadre d'un remplacement de SIEM, il se charge notamment :

- d'analyser les besoins et d'offrir un avis technique sur les échéances du projet,
- d'organiser des ateliers pour les phases d'analyse et de conception, notamment :
    - atelier de scénarios d'utilisation,
    - atelier de conception de SIEM,
    - atelier de conception de plateforme,
    - atelier de conception de plateforme SOAR,
    - atelier de conception de plan de réponse (playbook) SOAR,
    - atelier de planification d'indexation et de conservation des données,
- d'analyser les modèles architecturaux existants dans le cadre d'une vérification d'optimisation,
- de superviser et de guider les équipes projet élargies,
- de rédiger de la documentation de conception de haut niveau et de bas niveau,
- de former et de passer le relais aux consultants Splunk et aux équipes du client,
- d'organiser les réunions de lancement.

Chef de projet

Un chef de projet (PM) de Splunk Professional Services est un acteur essentiel d'un projet de remplacement de SIEM. Il est une grande source de valeur et permet aux architectes et aux consultants de se consacrer aux activités pour lesquelles ils sont formés et expérimentés. Ils ne réalisent pas les même activités que les PM de votre organisation. Ne pas faire appel à un PM lors d'un projet de remplacement de SIEM peut certes réduire le coût des services de l'équipe Splunk Professional Services, mais cela augmentera drastiquement le délai de rentabilité et donc le coût total du changement.

Dans le cadre d'un remplacement de SIEM, un MP Splunk se charge notamment :

- de définir la méthodologie du projet et la fréquence des communications,
- de créer et de se mettre d'accord sur un plan de livraison,
- de travailler avec les parties prenantes du client, notamment les PM, pour garantir une bonne communication,
- de servir de point de contact unique avec les parties prenantes internes de Splunk afin d'assurer la transmission des informations au client et d'éviter les répétitions inutiles,
- d'aider à la planification et à l'affectation du temps pour les différentes ressources,
- de cocréer un plan de mise en œuvre et de fixer les échéances avec l'architecte de Splunk,
- de gérer les différents points, par exemple en organisant des réunions quotidiennes,
- de consigner le temps passé et de gérer les comptes-rendus,
- de créer et de superviser les plans de validation et de test,
- de clôturer le projet.

Résumé des rôles de l'équipe Splunk Professional Services

Ensemble, les membres de Splunk Professional Services forment une équipe très efficace pour amener de la valeur et assurer une rentabilisation rapide. Cette méthode de travail est systématiquement recommandée par Splunk Professional Services, car elle a démontré son efficacité à travers les multiples projets de remplacement de SIEM de nos clients.