splunk> a CISCO company

ÉTUDE DE CAS

La Poste reçoit 10 fois moins de faux positifs et protège les données de 1,3 million de clients

Défis clés

Les volumes élevés de données à traiter entraînaient de la latence ou des plantages des systèmes utilisés par les équipes de cybersécurité de La Poste. Les conséquences ? Un ralentissement des investigations et une mise en danger des informations personnelles des clients.

Résultats clés

Après avoir adopté Splunk Enterprise Security, l'équipe de sécurité de La Poste parvient mieux à détecter et à atténuer les menaces en divisant par 10 le nombre de faux positifs et en corrigeant les alertes plus rapidement.

LA POSTE

Secteur d'activité : Secteur public

Solutions : Sécurité

Produits : Splunk Enterprise Security

La Poste est le plus grand opérateur de services postaux en France.

Chaque fois que vous passez une commande en ligne, demandez une nouvelle carte de crédit ou envoyez une lettre à votre grand-mère, vous comptez sur les services postaux pour assurer la livraison de votre commande dans les délais, la remise en toute sécurité de votre carte de crédit et la délivrance de votre lettre à vos proches. Chaque jour, 1,3 million de clients répartis dans 63 pays confient non seulement leurs lettres et leurs colis à La Poste, mais aussi leurs données personnelles, telles que leur adresse et leurs coordonnées. En plus d'offrir des services postaux fiables, La Poste doit également protéger les données de ses clients.

Cette responsabilité incombe principalement à son Service de Lutte Contre la Cybercriminalité (SLCC) qui compte 80 collaborateurs. Une tâche colossale. Comme beaucoup d'autres organisations, La Poste fait face à un paysage de menaces dangereux, caractérisé par des attaques de plus en plus sophistiquées et des incidents géopolitiques. La tenue d'événements majeurs tels que les Jeux Olympiques de Paris 2024 n'arrange en rien la situation et il n'a jamais été aussi vital de renforcer les défenses du groupe.

Résultats

- 80 % des alertes sont maintenant traitées en moins de 13 minutes
- Le nombre de faux positifs est 10 fois moins élevé
- Jusqu'à 20 téraoctets de données sont traités chaque jour

L'équipe de cybersécurité de La Poste a adopté Splunk Enterprise Security en tant que solution SIEM en 2015. En raison de la complexité de son environnement, La Poste avait besoin d'une solution capable de gérer d'immenses quantités de données et des systèmes variés, et disposant de fonctionnalités permettant à ses équipes de mener des investigations efficaces et de déjouer les menaces. Olivier Cassignac, Responsable Détection des Incidents de Sécurité chez La Poste, affirme : « Notre mission est de protéger le Groupe contre les menaces et les acteurs malveillants. Ces attaques sont diverses et variées et protéger le Groupe signifie protéger son infrastructure, ses employés et ses clients. »

Une accélération des investigations

L'objectif principal du SLCC est d'identifier le plus tôt possible les anomalies afin que les analystes de premier niveau puissent les traiter et prévenir les services concernés. Cependant, les volumes élevés de données à traiter entraînaient des plantages des

systèmes et ralentissaient les investigations. En règle générale, La Poste traite plus de 20 téraoctets de données chaque jour, dont 5 téraoctets en moyenne pour le seul SLCC. Avant la mise en place de Splunk, même avec un volume de données bien moindre, la recherche d'événements spécifiques prenait des heures ou entraînait le plantage du système.

Après avoir adopté Splunk Enterprise Security, le SLCC peut maintenant analyser de grands volumes de données sur des semaines voire des mois en quelques secondes. Ainsi, l'équipe gagne du temps et des ressources afin d'offrir une base solide à l'infrastructure de cybersécurité du groupe. M. Cassignac ajoute : « Pendant les investigations, la performance des outils de recherche est primordiale car les volumes de données à traiter sont énormes. Splunk est un atout majeur car les données sont interrogées à grande vitesse, ce qui donne aux analystes plus de temps pour les interpréter et faire avancer les investigations. »

> « Le niveau de personnalisation offert par Splunk est essentiel. L'outil n'a aucune limite. Il y a beaucoup de solutions sur le marché, mais à ma connaissance, aucune ne propose un tel niveau de personnalisation. Vous pouvez véritablement adapter chaque tableau de bord, chaque fonction, chaque règle et chaque recherche à vos besoins. »
>
> **Olivier Cassignac,** Responsable Détection des Incidents de Sécurité, La Poste

Une uniformisation des alertes

Le SLCC reçoit des milliers d'alertes chaque année, l'équipe avait donc besoin d'une solution capable de filtrer, trier et hiérarchiser chaque menace potentielle. La solution d'alertes basées sur les risques (RBA) de Splunk répondait à tous ces besoins et a permis de réduire le nombre de faux-positifs et d'accélérer le traitement. Il faut maintenant seulement 13 minutes au SLCC pour transférer une alerte au service concerné après l'avoir reçue.

Comment La Poste a-t-elle réussi à obtenir de tels résultats ? Le SLCC a exploité et affiné les fonctionnalités de Splunk Enterprise Security en fonction de ses besoins. Tous les tableaux de bord, fonctions, règles et recherches sont désormais personnalisés. Les fonctionnalités de RBA de Splunk ES attribuent également des scores de risque aux événements et aux incidents, puis envoient une alerte si ce score dépasse un certain seuil. Cela signifie que le SLCC peut maintenant détecter de manière efficace les menaces potentielles et les activités suspectes. Le nombre de faux positifs a également été divisé par 10. Les analystes peuvent ainsi se concentrer sur les menaces concrètes et urgentes et travailler plus efficacement.

Une collaboration face aux nouvelles menaces

Dans un paysage des risques en constante évolution, la fonction Threat Intelligence Management de Splunk Enterprise Security est un outil précieux dans l'arsenal de La Poste. Lorsque l'équipe du SLCC détecte une nouvelle menace, la fonction de gestion de la threat intelligence l'analyse et la convertit en indicateur technique. Cette métrique est ensuite utilisée pour enrichir les alertes afin de pouvoir identifier et hiérarchiser la nouvelle menace. Surtout, une détection rétroactive est mise en place et analyse les événements passés pour voir si cette nouvelle menace a déjà été rencontrée auparavant.

Tout le monde doit se mobiliser pour repousser les menaces et assurer la sécurité d'une organisation, et La Poste ne fait pas exception à la règle. Son organisation de cybersécurité de 200 personnes se compose du SLCC et de différents SOC dans ses filiales. L'adoption de Splunk permet à toutes les équipes de regrouper l'ensemble des informations et d'utiliser un outil commun avec des interfaces personnalisées, peu importe le scénario d'utilisation concerné : analyse avancée, supervision des KPI, recherches manuelles, la liste est longue. Splunk a non seulement permis aux équipes de cybersécurité de mener des investigations plus rapides et approfondies, mais aussi de collaborer davantage avec les autres équipes.

Téléchargez Splunk gratuitement ou commencez dès maintenant avec l'essai gratuit de la version cloud. Que ce soit dans le cloud ou sur des serveurs locaux, pour de grandes ou petites équipes, il existe un modèle de déploiement Splunk adapté à vos besoins.