Carrefour répond 3 fois plus vite aux menaces de sécurité avec la plateforme Splunk Cloud

Défis clés

Carrefour a consacré des ressources importantes à la maintenance de son infrastructure et à la détection des événements de sécurité. Pourtant, il reste parfois difficile de fournir l'expérience multicanale attendue par les clients.

Résultats clés

Avec la plateforme Splunk Cloud, Carrefour obtient des informations exploitables sur les performances de ses systèmes et accélère la réponse aux incidents de sécurité, pour mieux protéger son activité et améliorer l'expérience des clients.

Carrefour

Secteur d'activité : Commerce de détail

Solutions : Plateforme, Sécurité

Dans les grandes surfaces d'aujourd'hui, les consommateurs attendent une expérience multicanale.

Carrefour, huitième au classement mondial de son secteur, possède des hypermarchés en Europe, en Amérique du Sud et en Asie. Le groupe sait que les clients attendent la même simplicité en ligne qu'en magasin, que ce soit sur l'application mobile ou pour la livraison en « click and collect ». Pour améliorer l'expérience client sur ses canaux d'achat en ligne, Carrefour a adopté une stratégie de digitalisation qui tire parti des services basés sur le cloud.

Avec la plateforme Splunk Cloud, Carrefour possède désormais l'agilité nécessaire pour développer de nouvelles fonctionnalités et de nouveaux services. La plateforme Splunk Cloud simplifie également la sécurité pour protéger les clients. Grâce aux informations en temps réel fournies par Splunk, Carrefour réagit désormais trois fois plus rapidement aux menaces de sécurité et prend des décisions plus judicieuses pour prévenir les incidents.

Des résultats axés sur les données

3 fois
Réponse aux menaces 3 fois plus rapide

10 Md €
(10,45 Md $) de projection de ventes d'e-commerce d'ici 2026

Plus
de capacités libérées pour des tâches de plus grande valeur

Un temps de réponse aux incidents de sécurité divisé par trois

L'équipe du SOC (centre des opérations de sécurité) de Carrefour exploite une infrastructure complexe basée sur un datacenter hérité. Elle passait auparavant un temps considérable à gérer les systèmes, sans pouvoir se consacrer à protéger l'entreprise contre les logiciels malveillants. En centralisant l'analyse de la sécurité et en intégrant de multiples sources de données, la plateforme Splunk Cloud a significativement amélioré la capacité de l'équipe SOC à répondre aux incidents en temps réel.

« La plateforme Splunk Cloud nous aide à gérer de nombreux logs, autant ceux de notre logiciel antivirus que ceux de la détection et de la réponse, » explique Romaric Ducloux, analyste SOC chez Carrefour. « Splunk donne l'alerte, ouvre un ticket et contacte l'analyste SOC d'astreinte. C'est la pierre angulaire de nos opérations de sécurité. »

Avec le modèle cloud, Splunk gère les opérations et l'infrastructure de sécurité : l'équipe du SOC de Carrefour a plus de temps à consacrer à la gestion des applications, à l'analyse des menaces et aux investigations de sécurité. Quand un incident se produit, l'équipe peut désormais intervenir avant qu'il n'endommage les systèmes ou n'affecte les clients. En cas de violation, il collecte des informations sur l'anomalie pour améliorer les systèmes.

Désormais, l'équipe réagit aux incidents trois fois plus rapidement. « La plateforme Splunk Cloud nous permet de nous focaliser sur notre tâche la plus importante : garantir aux clients une expérience d'achat toujours sécurisée, » affirme Romaric Ducloux.

Innovation et résilience avec Splunk

L'équipe Carrefour apprécie particulièrement à quel point Splunk Cloud est accessible à l'ensemble de l'équipe du SOC. En effet, le langage utilisé pour analyser les événements est à la fois facile à apprendre et très puissant : il permet à l'équipe du SOC d'extraire rapidement des informations détaillées sur les tactiques, les techniques et les outils utilisés par les cyberattaquants. C'est un facteur de protection essentiel contre les futurs incidents.

« Splunk apporte une réelle valeur ajoutée. » conclut M. Ducloux. « La plateforme maximise les informations que nous obtenons en analysant les scénarios de détection : nous ne perdons plus de temps à créer des règles ou à nous battre avec un outil trop compliqué. » Et comme les utilisateurs de l'équipe élargie ont désormais un accès complet aux informations relatives aux systèmes et aux opérations lors d'un événement de sécurité, ils peuvent réaliser des investigations et déclencher des alertes dans toute l'organisation de façon totalement autonome.

Splunk apporte une réelle valeur ajoutée. La plateforme maximise les informations que nous obtenons en analysant les scénarios de détection : nous ne perdons plus de temps à créer des règles ou à nous battre avec un outil trop compliqué. »

Romaric Ducloux, analyste SOC, Carrefour

Pour exploiter davantage les logs et les données, l'équipe du SOC tire profit des applications disponibles dans la Splunkbase. Elles s'intègrent de façon transparente à plusieurs sources pour permettre à Carrefour de réaliser certaines tâches – adopter des proxys SaaS, par exemple – avec un minimum d'effort. Aujourd'hui, le groupe Carrefour est convaincu de pouvoir lancer de nouvelles offres innovantes pour ses consommateurs, tout en préservant la résilience et l'efficacité des opérations de sécurité.

La plateforme Splunk Cloud est la pierre angulaire de nos opérations de sécurité. »

Romaric Ducloux, analyste SOC, Carrefour

Évoluer pour prendre en charge 10 milliards d'euros de ventes d'e-commerce

Carrefour a des projets ambitieux pour l'avenir : le détaillant vise en effet à tripler ses ventes en ligne pour atteindre 10 milliards d'euros (10,45 milliards de dollars) d'ici 2026, et à se développer à l'échelle mondiale. Parce qu'elle est capable d'évoluer facilement pour s'adapter à un SOC mondial couvrant plusieurs pays et de gérer des quantités croissantes de données et de logs issus de nouveaux pays et marchés, la plateforme Splunk Cloud donne à Carrefour les éclairages et l'agilité dont le groupe a besoin pour maintenir une base sécurisée sur laquelle construire un avenir innovant.

FINAL_AW-22-24856-Splunk-Carrefour-A4-CS-101