Le fabricant de logiciels de cybersécurité Check Point choisit Splunk pour bénéficier d'informations détaillées

Défis clefs

Check Point souhaitait tirer des informations plus utiles de ses multiples ensembles de données afin d'améliorer ses opérations et son efficacité, tout en réduisant les menaces.

Résultats clefs

Splunk fournit des informations en temps réel sur les opérations commerciales, grâce auxquelles le personnel et les systèmes de Check Point gardent une longueur d'avance, même en cas d'événements imprévus comme le passage au télétravail pendant la pandémie.

Check Point SOFTWARE TECHNOLOGIES LTD

Secteur : Technologie

Solutions : Securité

Comment une entreprise de logiciels de sécurité sécurise-t-elle ses propres systèmes ?

Check Point crée des solutions de cybersécurité qui aident plus de 100 000 entreprises de toutes tailles. Lorsqu'il s'agit de protéger ses propres systèmes et son personnel de 5 400 employés, Check Point applique les normes les plus strictes. L'entreprise souhaitait tirer des informations plus utiles des téraoctets de données que ses systèmes collectaient quotidiennement, afin de mieux comprendre son activité et d'assurer la sécurité de l'ensemble de ses opérations.

Des investigations plus rapides et plus intelligentes pour une prévention efficace des menaces

Lorsque Check Point a mis en place un centre d'opérations de sécurité pour améliorer la responsabilité de la protection de l'organisation, l'entreprise a choisi Splunk Enterprise Security. Splunk peut importer les nombreux formats de données utilisés par Check Point et fonctionne avec toutes les technologies que nous exploitons.

Jony Fischbein, Responsable mondial de la sécurité des systèmes d'information chez Check Point, explique : « Nous sommes une entreprise axée sur les données. Notre plus grand défi consistait à agréger les énormes quantités de données que nous collectons et à les convertir en informations utiles. »

Seulement 17 jours après l'adoption de Splunk, Check Point a commencé à constater des avantages tels qu'une meilleure connaissance des menaces et des investigations de sécurité plus rapides, par rapport à son ancien outil de gestion des informations de sécurité et des événements.

Résultats chiffrés

5 fois
Investigations de sécurité 5 fois plus rapides

17
jours pour migrer sur Splunk

100 %
de la main d'œuvre en télétravail respecte la nouvelle politique de sécurité relative au COVID-19

Les tableaux de bord de Splunk aident Check Point à visualiser l'état actuel de ses systèmes, et des alertes automatisées les informent de toute activité malveillante ou vulnérabilité du réseau. Selon M. Fischbein, Splunk permet également à son équipe d'investiguer rapidement et efficacement les problèmes potentiellement dangereux, comme des développeurs qui font sortir du code source des locaux ou l'apparition d'une nouvelle vulnérabilité dans un produit qu'ils utilisent, avant qu'elle ne puisse causer des dommages.

« Nous savons quoi investiguer et si nous avons résolu le problème. Et pas seulement en nous basant sur nos intuitions. Les données nous le démontrent avec certitude », ajoute Jony Fischbein.

Travailler en toute sécurité pendant la pandémie

La capacité de Splunk à extraire des informations pertinentes des données a également aidé Check Point à travailler de manière sûre et productive pendant la pandémie de COVID-19.

Lorsqu'un employé a été testé positif au COVID-19, l'équipe IT de Check Point a utilisé Splunk pour suivre les badges d'accès du personnel et identifier le niveau d'exposition des employés qui avaient été en contact avec lui au cours des 14 jours précédents. Les employés à risque ont été informés immédiatement et ont été invités à travailler à domicile et à s'isoler.

« Nous n'aurions pas pu faire cela avec une autre solution », déclare M. Fischbein.

Splunk a également aidé Check Point à sécuriser le travail à distance pendant la pandémie. Lorsque la direction a défini de nouvelles mesures de sécurité pour le travail à domicile, Splunk a révélé quels employés s'y conformaient, et en deux semaines, M. Jony Fischbein a pu montrer au PDG qu'ils avaient atteint 100 % de conformité aux nouvelles règles. « Cela a vraiment fait comprendre à l'équipe de direction la valeur de l'utilisation de Splunk. Les données ont prouvé que le personnel en télétravail était en sécurité et pleinement productif. »

> Nous sommes une entreprise axée sur les données. Notre plus grand défi consiste à agréger les énormes quantités de données que nous collectons et à les convertir en informations utiles. »
>
> **Jony Fischbein,**
> Directeur mondial de la sécurité des systèmes d'information, Check Point

Avec ses équipes en télétravail, Check Point a également utilisé Splunk pour découvrir et atténuer les risques de sécurité : par exemple, un développeur utilisait son propre ordinateur portable pour accéder au dark web, et un membre de l'équipe financière avait donné à un autre collaborateur l'accès à son ordinateur portable professionnel. Une fois informés de ces problèmes, les responsables ont demandé au personnel de respecter des politiques visant à protéger les données de l'entreprise et les informations sensibles.

> Nous savons quoi investiguer et si nous avons résolu le problème. Et pas seulement en nous basant sur nos intuitions. Les données nous le démontrent avec certitude. »
>
> **Jony Fischbein,**
> Directeur mondial de la sécurité des systèmes d'information, Check Point

Se développer pour l'avenir avec Splunk

Check Point est ravi des avantages de Splunk et envisage d'élargir son utilisation.

M. Fischbein affirme : « Nous ne voulons pas d'une solution qui réponde uniquement à nos besoins du jour. Nous voulons de l'aide sur des sujets que nous ignorons encore et qui ne se présenteront pas avant six mois ou un an. Splunk nous offre cette aide, Splunk évolue avec nous. »

Check Point prévoit de tirer parti de la capacité de Splunk à automatiser des tâches comme l'isolement d'un appareil potentiellement vulnérable et l'amélioration de la gestion des codes secrets des employés. L'équipe cherche également comment d'autres équipes que le SOC peuvent utiliser Splunk, comme le personnel du service d'assistance qui apprend à identifier les alertes sur lesquelles ils peuvent agir.

M. Fischbein déclare : « Avec Splunk, nous avons les yeux sur l'ensemble de notre organisation. C'est extrêmement utile à tout ce que nous faisons. »

21-19735-Splunk-Tier2-Check Point-CS-A4-101_FR