Transformer la position de sécurité d'Intel avec des innovations dans la Data Intelligence

Défis clefs

Intel avait besoin de passer à un modèle commercial axé sur les données qui augmente la valeur des données tout en réduisant sa vulnérabilité.

Résultats clefs

En prenant Splunk® et Apache Kafka comme base, la plateforme de cyber-intelligence (CIP) offre une visibilité complète sur l'organisation InfoSec d'Intel, ce qui a permis de révolutionner la gestion de la sécurité des informations.

Secteur : Technologie

Solutions :
Sécurité, Opérations IT

Transformer les données en actions

- Accélère l'analyse des données et détecte les menaces avancées en quelques minutes ou heures, par rapport à plusieurs jours ou semaines
- Offre une approche unifiée et collaborative de la cybersécurité
- Fournit un traitement des flux et des outils de machine learning qui offrent une valeur commerciale dans d'autres domaines, tels que les opérations de sécurité et la santé des systèmes

On peut difficilement surestimer l'impact et l'importance des contributions technologiques d'Intel sur la société.

L'expertise technique de l'entreprise participe à sécuriser, alimenter et connecter des milliards d'appareils et l'infrastructure du monde intelligent et connecté. Avec le temps, l'entreprise centrée sur le PC qu'était Intel a fait des données son cœur de métier. Elle développe de nouveaux produits, pénètre de nouveaux marchés et séduit de nouveaux clients par des approches innovantes.

Brent Conran, Directeur de la sécurité des informations d'Intel, affirme : « Les données sont la base de tout. Les données sont reines. Elles sont le moteur de notre activité, le moteur de tout. Elles transforment les industries traditionnelles autant que celles qui sont nées dans le cloud. La capacité à extraire des informations des données fait la différence entre l'entreprise qui réussit et celle qui échoue. »

En raison de ce changement d'orientation et de cette dépendance nouvelle par rapport aux données, l'équipe de sécurité des informations (InfoSec) d'Intel devait mettre sur pied et maintenir une stratégie complète de « défense en profondeur ». L'équipe a automatisé les outils de prévention et de détection à de nombreux niveaux (périmètre, réseau, points de terminaison, applications et couche de données) pour traiter 99 % des menaces présentes dans l'environnement d'Intel.

À la recherche du dernier pourcent

La fréquence et la sophistication des menaces avancées continuent d'augmenter. Et Intel était aux prises avec un SIEM qui ne répondait plus à ses besoins. Seule une poignée d'experts savaient utiliser cet ancien SIEM, qui ne pouvait pas s'adapter à la demande toujours croissante de diversification des types de données.

L'InfoSec d'Intel avait besoin d'une stratégie pour détecter les menaces sophistiquées qui tentaient de pénétrer dans l'environnement de l'entreprise, ce qu'elle appelle la recherche du dernier pourcent. C'est ce qui a inspiré la création de la plateforme de cyber-intelligence (CIP) d'Intel, qui s'articule autour de technologies de pointe dont Splunk et Apache Kafka. Avec des serveurs hautes performances basés sur les processeurs Intel® Xeon® Platinum, des unités de stockage SSD Intel 3D NAND et SSD Intel® Optane™, la nouvelle plateforme CIP enregistre plus de 12 téraoctets de données par

jour et stocke 15 pétaoctets de données. Les données parviennent de centaines de sources vers un bus de messages Kafka, puis atteignent la plateforme Splunk, où les utilisateurs effectuent plus de 1,3 million de recherches par semaine.

Grâce à la plateforme Data-to-Everything de Splunk et des centaines d'outils tiers, l'équipe InfoSec d'Intel bénéficie désormais d'une visibilité richement contextualisée et d'une surface de travail commune qui améliore l'efficacité de toute son organisation. L'équipe peut désormais détecter et traiter les menaces en quelques heures ou minutes, alors qu'il lui fallait auparavant des jours, voire des semaines.

Agrandir la plateforme de cyber-intelligence (CIP) d'Intel

Les résultats de la CIP ont conduit à d'autres sources de données, à de nouveaux cas d'utilisation et à de nombreux autres modèles de données. Rapidement, l'utilisation de la CIP s'est étendue aux équipes de la gestion des vulnérabilités, de la conformité, de la gestion des risques et au-delà, ce qui a fait peser des exigences supplémentaires sur l'infrastructure tout en demandant des calculs et un stockage encore plus rapides. Pour optimiser les performances de la plateforme, l'architecte de solution et les ingénieurs de sécurité d'Intel avaient besoin de mieux comprendre la plateforme Splunk et les technologies Intel.

> Les données sont la base de tout. Les données sont reines. [. . .] Elles transforment les industries traditionnelles autant que celles qui sont nées dans le cloud. La capacité à extraire des informations des données fait la différence entre l'entreprise qui réussit et celle qui échoue. »
>
> **Brent Conran,** Directeur de la sécurité des informations

> Nous voyons le potentiel, et parce que nous le voyons, nous investissons du temps, de l'énergie et des ressources pour l'exploiter. Nous voulons que Splunk réussisse parce que nous sommes convaincus que cela nous aidera à remplir notre mission.
>
> **Brent Conran,** Directeur de la sécurité des informations

Une équipe commune de Splunk et d'Intel a développé une configuration de référence commune pour orienter l'expansion de CIP en termes de puissance de calcul, de mémoire et de stockage à l'aide des derniers produits et technologies Intel. Splunk et Intel partagent désormais leur succès avec leurs confrères de l'IT, ce qui permet à d'autres d'élargir leurs déploiements Splunk et Apache Kafka pour convertir plus efficacement les données brutes en informations opérationnelles, métier et de sécurité.

Délivrer de la valeur pour aujourd'hui et demain

L'équipe InfoSec d'Intel élargit son utilisation de Splunk et Kafka. Les analystes et les data scientists transforment, enrichissent, joignent, filtrent et exploitent les flux de données. L'équipe applique également de nouveaux outils de machine learning à la réponse aux incidents, aux opérations et à la supervision de la santé des systèmes, mais aussi à l'orchestration des workflows et aux alertes. En collaborant avec Splunk, Intel libère de la valeur pour aujourd'hui et demain.

M. Conran explique : « L'équipe de sécurité des informations d'Intel est bien plus agile que par le passé. Nous avons mis en place un tout nouveau lac de données Splunk et nous avons modernisé nos outils. En stockant les données aux bons endroits et en développant les compétences de nos collaborateurs, nous avons créé un véritable multiplicateur de force. Nous utilisons le machine learning pour accroître considérablement la profondeur et la vitesse de notre cyber-intelligence. »

20-14330-TransformingIntel_sSecurityPostureWithInnovativeDataIntelligence-A4-104-Tie2-CS_fr-FR