splunk>

ÉTUDE DE CAS

DKB honore la confiance de ses clients et traite les menaces 90 % plus vite avec Splunk

Défis clés

Quand DKB s'est lancée dans son parcours de migration vers le cloud, il est devenu difficile pour l'institution financière de superviser ses systèmes complexes et de détecter les compromissions survenant dans son environnement.

Résultats clés

Après avoir adopté Splunk et obtenu une visibilité complète sur son infrastructure, DKB a réduit le nombre de faux positifs dans ses alertes et accéléré de 90 % la détection et l'investigation des menaces.

DKB
Deutsche Kreditbank AG

Secteur d'activité : Services financiers

Solutions : Sécurité

Dans le monde de la banque, la confiance des clients est primordiale.

Quatre millions et demi de clients font confiance à la Deutsche Kreditbank (DKB). Deuxième banque directe en Allemagne, elle propose des services de prêt, de carte de crédit, d'épargne et bien d'autres. Pour garantir la fluidité des transactions, des paiements et autres opérations, DKB a migré vers le cloud tout en intensifiant ses investissements dans la cybersécurité. L'institution a d'abord utilisé Splunk par le biais d'un fournisseur de services gérés avant de le déployer en interne.

La transition vers le cloud de DKB fut plus élaborée que prévu. Il lui fallait une solution pour voir tous les aspects de son infrastructure hybride : outils de sécurité, environnement cloud et systèmes locaux. La banque voulait profiter d'une visibilité complète pour être rapidement informée des problèmes, une exigence d'autant plus cruciale que le risque d'attaque par ransomware et de menaces de cybersécurité ne met pas seulement en péril la stabilité de ses systèmes, mais aussi la confiance de ses clients.

Résultats

- Détection et investigation des menaces accélérées de 90 %
- Visibilité accrue sur les outils et les environnements
- Réduction du nombre de faux positifs

Minimiser les angles morts

DKB a commencé à utiliser Splunk pour ses opérations de supervision de sécurité et de gestion des incidents, et exploite depuis peu ses outils de threat intelligence. L'institution a déjà utilisé une multitude d'outils de sécurité, mais Splunk lui permet d'agréger les données de tous ses outils et de les interroger.

Et elle a déjà gagné un temps considérable. Andreas Hennich, Directeur du SOC de DKB, explique : « Le plus grand avantage de Splunk réside dans la visibilité. Nous voyons tout. Nous voyons la moindre alerte de tous nos outils de sécurité, dans tous nos environnements, cloud ou locaux. Comme tout est centralisé, nous analysons et nous utilisons ces données bien plus rapidement. »

Aucune compromission ne passe inaperçue

Les équipes de DKB ont amélioré la sécurité du réseau en accélérant la réponse aux alertes. Auparavant, le nombre d'alertes était bien trop grand pour être gérable, d'autant plus qu'elles étaient décentralisées. Résultat : des retards et des alertes ignorées. M. Hennich détaille : « Nous devions passer des fichiers de log au peigne fin pour trouver les erreurs réseau. Cela prenait un temps fou et nous pouvions facilement passer à côté de certaines alertes. Aujourd'hui, tous les composants de notre infrastructure sont connectés à Splunk qui joue le rôle de SIEM. Tous les types d'activités en lien avec la sécurité du réseau sont rapidement visibles au sein d'une base de données centralisée et corrélée. En cas de compromission, nous voyons les alertes plus rapidement, et nous intervenons immédiatement. »

Dans le domaine des menaces, DKB a réduit le temps d'investigation et de résolution de 90 % selon M. Hennich. « Avant Splunk, il fallait parcourir des fichiers de log, chercher des données supplémentaires, rédiger des requêtes, etc. Aujourd'hui, tout va beaucoup plus vite avec Splunk. »

Aujourd'hui, tous les composants de notre infrastructure sont connectés à Splunk qui joue le rôle de SIEM. Tous les types d'activités en lien avec la sécurité du réseau sont rapidement visibles au sein d'une base de données centralisée et corrélée. En cas de compromission, nous voyons les alertes plus rapidement, et nous intervenons immédiatement. »

Andreas Hennich, Directeur du centre des opérations de sécurité de DKB

24-splunk- 133169 - EMEA DKB Customer Story-102_FR