splunk> a CISCO company

ÉTUDE DE CAS

Johnson Matthey lutte contre le phishing et réduit la durée de ses investigations de 83 % grâce à Splunk

Défis clés

Avant de s'équiper de Splunk, l'équipe de sécurité de Johnson Matthey était submergée d'alertes et n'avait aucun moyen de les filtrer pour traiter les plus urgentes en priorité.

Résultats clés

En adoptant Splunk Enterprise Security, Splunk SOAR et Splunk Attack Analyzer, l'équipe de Johnson Matthey a amélioré la fidélité des alertes et la précision de la détection du phishing, ce qui a considérablement renforcé la sécurité et les défenses de l'organisation.

JM Johnson Matthey
Inspiring science, enhancing life

Industrie : Fabrication

Solutions : Sécurité

Produits : Splunk Enterprise Security, Splunk SOAR et Splunk Attack Analyzer

Le développement durable est la responsabilité de tous

Fondée au début des années 1800, l'entreprise Johnson Matthey est un leader mondial des technologies durables basé à Londres. De grands acteurs mondiaux de l'énergie, des produits chimiques et de l'automobile comptent sur ses technologies et son expertise pour décarboner leurs activités, réduire les émissions nocives et rendre leurs opérations plus durables.

Fortement axée sur la science et l'innovation dans plusieurs domaines, la structure commerciale de Johnson Matthey intègre des fonctions d'informatique d'entreprise et de technologie opérationnelle (OT), où la cybersécurité joue nécessairement un rôle décisif. La moindre faille peut affecter la disponibilité des systèmes, la production et même la sécurité des employés.

Résultats

- Fidélité des alertes augmentée de 30 %
- Délai de gestion des investigations réduit de 83 %
- 61 % des cas de phishing résolus par l'automatisation avec le SOAR

Le centre des opérations de sécurité (SOC) de Johnson Matthey était confronté à un grand volume d'alertes, et n'avait pas le contexte et les technologies nécessaires pour identifier les signalements légitimes et critiques. Le SOC de Johnson Matthey avait donc besoin d'une solution capable d'apporter le contexte nécessaire pour accélérer l'examen des alertes et préserver la sécurité de l'entreprise, afin qu'elle puisse se concentrer sur sa véritable mission : lutter contre le changement climatique.

Éliminer le bruit

Avant d'utiliser Splunk, l'équipe de sécurité de Johnson Matthey ne parvenait pas à traiter le volume considérable d'alertes de sécurité. Il manquait à l'équipe le contexte indispensable pour hiérarchiser efficacement les alertes et identifier les 15 à 20 % de signalements qui nécessitaient son attention immédiate. Trouver les véritables alertes revenait à chercher une aiguille dans une botte de foin.

Après avoir adopté Splunk Enterprise Security, l'équipe de sécurité de Johnson Matthey a mis en place des alertes basées sur les risques (RBA) : cette approche combine plusieurs alertes en une plus précise pour permettre à l'équipe de se concentrer dessus. Au lieu de recevoir un grand nombre d'alertes de sécurité séparées, la RBA les compile et présente les informations sous forme d'une seule alerte au sujet de l'actif ou de l'identité à examiner. De cette façon, toutes les données entrantes peuvent être analysées et utilisées pour rechercher les menaces sans submerger le SOC sous des milliers d'alertes inutiles. Cette approche améliore non seulement l'efficacité des opérations, mais aussi la posture de sécurité dans son ensemble. Grâce aux alertes enrichies, Johnson Matthey a pu

augmenter le volume de scénarios d'utilisation de 40 à 50 % tout en réduisant le nombre d'alertes et de faux positifs.

Grâce aux alertes basées sur les risques dans Splunk Enterprise Security, nous pouvons définir avec précision ce que nous voulons savoir sur le système. Toutes les données nous parviennent et peuvent être analysées, mais sans submerger notre SOC d'alertes inutiles », conclut Nathan Lowey, Ingénieur en cybersécurité chez Johnson Matthey.

Le travail est toujours plus facile en équipe

Comme les données sont enfermées dans des silos et que les signalements ne sont pas normalisés, il arrivait que plusieurs analystes travaillent indépendamment sur la même alerte sans collaborer. Les méthodes de travail variaient d'un analyste à l'autre, et tous n'appliquaient pas les mêmes standards. Il faut également savoir que 90 % des alertes étaient générées par 20 % des scénarios d'utilisation seulement. Avec Splunk SOAR, l'équipe de Johnson Matthey a commencé à utiliser des playbooks pour harmoniser et normaliser le processus de traitement des alertes. Le travail des analystes est ainsi devenu plus organisé et les rapports ont gagné en cohérence. Résultat : des données plus normalisées et précises pour un ajustement plus proactif.

Auparavant, lorsque les analystes enregistraient une menace, ils devaient créer manuellement un ticket et saisir eux-mêmes les informations utiles. Splunk SOAR a transformé ce processus en automatisant les tâches répétitives et en enrichissant les alertes grâce à du contexte supplémentaire. L'examen des investigations prenait jusqu'ici 30 minutes en moyenne. Aujourd'hui, il dure seulement cinq minutes. Nathan Lowey, Ingénieur en cybersécurité chez Johnson Matthey, explique : « Splunk SOAR facilite la communication. Si l'un de nos analystes a besoin de communiquer des informations à un membre de la fonction OT, il suffit d'un clic pour extraire toutes les données de l'investigation et les transférer à la gestion des services IT. Tout reste protégé au sein du même système. »

> Splunk SOAR et Splunk Attack Analyzer nous ont permis d'automatiser une partie de notre processus de prise en charge du phishing. Nos analystes ont moins de cas à traiter parce que ceux qui ne représentent pas réellement une menace sont automatiquement clos. Nous avons apporté des améliorations supplémentaires pour que le travail des analystes soit le plus productif possible. Actuellement, 61 % des tentatives de phishing sont analysées et traitées sans notre intervention. »
>
> **Nathan Lowey,** Ingénieur en cybersécurité, Johnson Matthey

Gérer les risques, anciens et émergents

Face à l'arrivée de cybermenaces innovantes et sophistiquées, les entreprises doivent garder une longueur d'avance sur les pirates. Quand les équipes de Johnson Matthey ont rencontré les premiers cas de « quishing », une forme de phishing basée sur des codes QR impossibles à distinguer d'images normales par les systèmes de détection, elles se sont tournées vers Splunk Attack Analyzer.

L'adoption de Splunk Attack Analyzer a dopé la précision de tout le système de détection du phishing qui affichait jusque-là un taux de faux positifs problématique. Auparavant, tous les e-mails dont l'objet contenait le mot « urgent », « paiement » ou « avis de rapport » étaient signalés comme suspects. Depuis l'introduction de Splunk Attack Analyzer, la précision de la détection du phishing a atteint 80 %, contre 50 % auparavant. Cette amélioration dénote une meilleure identification des menaces authentiques. Aujourd'hui, 61 % des tentatives sont automatiquement identifiées comme de fausses alertes et les incidents sont clos sans faire intervenir d'analyste. Une fois qu'une URL malveillante a été détectée, elle est automatiquement ajoutée au proxy cloud.

Avec Splunk Enterprise Security, Splunk SOAR et Splunk Attack Analyzer, Johnson Matthey a simplifié et amélioré sa stratégie de sécurité des données, harmonisé ses processus et amélioré son processus de prise de décision. D'autre part, les équipes de cybersécurité jusque-là isolées les unes des autres peuvent désormais communiquer et collaborer de façon fluide pour assurer la sécurité de l'organisation.

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.

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

Splunk, Splunk> et Turn Data Into Doing sont des marques commerciales de Splunk Inc., déposées aux États-Unis et dans d'autres pays. Tous les autres noms de marque, noms de produits et marques commerciales appartiennent à leurs propriétaires respectifs. © 2024 Splunk Inc. Tous droits réservés.