Delivery Hero atteint son objectif de sécurité centralisée avec la plateforme Splunk Cloud

Défis clés

En raison de sa croissance mondiale, Delivery Hero devait augmenter la portée et la visibilité de ses opérations de sécurité et de supervision pour identifier et résoudre rapidement tout problème de sécurité potentiel. De plus, l'entreprise tenait à partager les informations entre les différentes unités commerciales.

Résultats clés

La plateforme Splunk Cloud offre à l'équipe de sécurité mondiale de Delivery Hero une vue centralisée de son environnement informatique hybride et multicloud. Elle l'aide à analyser les menaces, les vulnérabilités et les erreurs de configuration en lui fournissant des informations en temps réel.

Delivery Hero

Secteur d'activité : Services en ligne

Solutions : Sécurité, Plateforme

Capacités : SIEM/Analyse de sécurité, Opérations de sécurité unifiées, Examen et investigation des incidents

Tout livrer, c'est aussi tout superviser.

Dans plus de 70 pays répartis dans l'Amérique latine, l'Europe et l'Asie, la mission de Delivery Hero est d'« offrir une expérience extraordinaire, rapide et facile, à votre porte » via son service de livraison en ligne. Pour accomplir cette mission au quotidien, l'entreprise doit garantir la convivialité et la fiabilité des services de ses sites web mondiaux.

Mais son infrastructure sur site privait l'équipe de sécurité d'une vue globale de la sécurité dans un environnement hybride complexe. Pour assurer la supervision nécessaire et gagner en visibilité sur la sécurité, Delivery Hero avait besoin d'un moyen centralisé d'identifier et de résoudre rapidement les anomalies et les erreurs de configuration dans son environnement informatique.

Une latence réduite et une visibilité accrue pour réduire le délai d'action

Grâce aux solutions Splunk, Delivery Hero identifie et résout les menaces de sécurité et les problèmes de performances plus rapidement que jamais. La plateforme Splunk Cloud permet à l'équipe de sécurité de Delivery Hero d'investiguer, de superviser, d'analyser et d'agir sur ses données. Elle dispose d'une capacité sans précédent à détecter les activités anormales.

Des résultats axés sur les données

- Gain de temps grâce à la supervision centralisée de 250 comptes
- Latence réduite dans un environnement multicloud complexe
- Détection des menaces pour plus de 14 000 terminaux EDR

Par rapport à son précédent déploiement sur site, Delivery Hero a désormais réduit la latence en optant pour la plateforme Splunk Cloud, qui donne à l'équipe de sécurité mondiale de l'entreprise une image plus précise et à jour. Mauro Papa, Directeur de la sécurité des informations chez Delivery Hero affirme : « Quand Splunk était utilisé sur site, il était centralisé à un seul endroit. Et cela se traduisait par différents degrés de latence pour les équipes réparties dans le monde entier. »

Cette visibilité accrue réduit le délai d'action. Combinant fournisseurs multicloud et infrastructure sur site, Delivery Hero maintient un environnement complexe. Mais en centralisant tous les journaux au sein de la plateforme Splunk Cloud, les équipes de sécurité de l'entreprise détectent et identifient facilement les erreurs de configuration dans l'environnement cloud de l'entreprise. Elles corrèlent ensuite ces données dans Splunk et envoient des déclencheurs aux responsables AWS ou GCP concernés pour une résolution rapide. Mauro Papa explique : « Avant, nous n'utilisions Splunk que pour les logs sur site : nous étions donc dans l'impossibilité de détecter ces erreurs de configuration. Désormais, Splunk couvre l'ensemble de notre environnement multicloud, et cette large visibilité nous aide à résoudre les problèmes en quelques minutes. Nous détectons aujourd'hui de nombreuses anomalies qui passaient autrefois inaperçues. »

Les rapports personnalisés permettent de gagner du temps et renforcent la responsabilisation

Le contrôle centralisé de la plateforme Splunk Cloud prend en charge un nombre croissant de sources de données sans occuper inutilement les ressources de l'équipe de sécurité. Par exemple, grâce à un système d'alertes rationalisé et personnalisé, Delivery Hero perd moins de temps à traiter des alertes et des dépannages inutiles. « Nous avons pu utiliser Splunk pour personnaliser nos alertes, ce qui a réduit les taux de faux positifs », précise Mauro Papa.

Au-delà de la détection et de la notification, la plateforme Splunk fournit également des métriques et des rapports plus complets aux parties prenantes. Avec la plateforme Splunk Cloud, vous pouvez créer des rapports en temps réel, les programmer pour qu'ils s'exécutent à intervalles réguliers, et les faire apparaître dans des tableaux de bord. « Nous suivons toutes nos vulnérabilités et nous envoyons des rapports à chacun des responsables afin qu'ils puissent suivre les performances de leurs applications », déclare Mauro Papa.

C'est particulièrement crucial pour maintenir la responsabilité et les performances de l'équipe de sécurité mondiale de Delivery Hero. Mauro Papa ajoute : « Nous avons plusieurs équipes de sécurité dans le monde, il est donc crucial que chacune puisse accéder à ses propres rapports et alertes et apporter des améliorations. »

> Avant, nous n'utilisions Splunk que pour les logs sur site : nous étions donc dans l'impossibilité de détecter ces erreurs de configuration. Désormais, Splunk couvre l'ensemble de notre environnement cloud, et cette large visibilité nous aide à résoudre les problèmes en quelques minutes. Nous détectons aujourd'hui de nombreuses anomalies qui passaient autrefois inaperçues. »
>
> **Mauro Papa,** Directeur de la sécurité de l'information, Delivery Hero.

Grâce au tableau de bord personnalisable et facile d'accès de la plateforme, ce processus de supervision est considérablement simplifié pour les membres de l'équipe. De plus, des plug-ins transparents améliorent la connectivité des points de données de performance. Par exemple, Splunk est intégré à l'outil de gestion de projet Jira afin que l'équipe puisse suivre et mesurer les KPI.

> La plateforme Splunk Cloud permet à l'équipe de sécurité de se focaliser sur sa mission principale plutôt que sur la maintenance de l'infrastructure. Aujourd'hui, nos ingénieurs se concentrent sur la configuration de nouveaux indices, exploitent les informations de nos nouveaux tableaux de bord et mettent en place de nouvelles détections. »
>
> **Mauro Papa,** Directeur de la sécurité de l'information, Delivery Hero

Cibler les menaces stratégiques

La plateforme Splunk Cloud soulage les spécialistes de la sécurité de Delivery Hero des lourdeurs de la maintenance de l'infrastructure, et ils peuvent désormais se concentrer sur l'optimisation des performances.

Mauro Papa affirme : « La plateforme Splunk Cloud permet à l'équipe de sécurité de se focaliser sur sa mission principale plutôt que sur la maintenance de l'infrastructure. Aujourd'hui, nos ingénieurs en sécurité se concentrent sur la configuration de nouveaux indices, exploitent les informations de nos nouveaux tableaux de bord et mettent en place de nouvelles détections. »

Pour poursuivre sa croissance mondiale, la prochaine étape pour l'équipe de sécurité de Delivery Hero consiste à mettre en œuvre Splunk Enterprise Security pour produire des informations basées sur les données à grande échelle. Ces informations aideront l'entreprise à remplir sa mission : « tout livrer » à ses clients. Le partenariat étroit avec Splunk aidera Delivery Hero à conserver son statut héroïque dans un écosystème réparti sur 70 pays et quatre continents, et qui ne cesse de croître.

22-26065-Splunk-Delivery Hero-CS2-A4-102