Delivery Hero am Ziel: zentralisierte Sicherheit dank der Splunk Cloud Platform

Zentrale Herausforderungen

Delivery Hero wächst weltweit und musste deshalb seinen Sicherheitsbetrieb erweitern und transparenter gestalten. Außerdem benötigte das Unternehmen eine Lösung, um potenzielle Sicherheitsrisiken schnell erkennen und beseitigen sowie Updates unternehmensweit bereitstellen zu können.

Wichtige Ergebnisse

Mit der Splunk Cloud Platform hat das globale Sicherheitsteam von Delivery Hero jetzt seine gesamte Hybrid- und Multi-Cloud-Umgebung im Blick und kann anhand von Echtzeiteinblicken Bedrohungen, Schwachstellen und Fehlkonfigurationen untersuchen.

Delivery Hero

Branche: Online Services

Lösungen: Security, Plattform

Funktionen: SIEM / Security Analytics, vereinheitlichte Security Operations, Untersuchung und Forensik

Wer alles liefert, muss auch alles im Blick haben.

Delivery Hero operiert in über 70 Ländern in Lateinamerika, Europa und Asien. Die Mission des Unternehmens: mit seinem Online-Lieferservice „ein herausragendes Erlebnis zu bieten – schnell, einfach und bis zur Haustür". Damit das gelingt, muss das Unternehmen sicherstellen, dass seine globalen Website-Dienste intuitiv und zuverlässig funktionieren.

Dabei stieß das Sicherheitsteam allerdings auf ein Nadelöhr: Die lokale Infrastruktur ließ keinen Gesamtüberblick über die Sicherheit der komplexen Hybridumgebung zu. Es musste also eine zentrale Lösung her, mit der Anomalien und Fehlkonfigurationen in der gesamten IT-Umgebung schnell identifiziert und beseitigt werden können.

Kürzere Latenzzeiten und mehr Einblicke ermöglichen schnelleres Handeln

Splunk bietet genau das, wonach Delivery Hero suchte: Lösungen zur raschen Erkennung und Behebung von Sicherheitsproblemen und Leistungsengpässen. Mit der Splunk Cloud Platform untersucht, überwacht und analysiert das Sicherheitsteam von Delivery Hero jetzt seine Daten, um anormale Aktivitäten aufzudecken und schneller denn je zu reagieren.

Datengestützte Ergebnisse

- Zeiteinsparung durch zentralisiertes Monitoring für über 250 Accounts
- Verkürzte Latenzzeiten in einer komplexen Multi-Cloud-Umgebung
- Gefahrenerkennung für über 14.000 EDR-Endpunkte

Die Vorteile gegenüber der früheren lokalen Umgebung liegen auf der Hand: Latenzzeiten wurden dank der Splunk Cloud Platform verkürzt, und die Sicherheitsexperten können nun jederzeit präzisere, aussagekräftigere und aktuellere Daten einsehen. „Früher haben wir Splunk lokal genutzt, zentrale Einblicke gab es nur auf Standortebene", erläutert Mauro Papa, Director of Information Security bei Delivery Hero. „In der Folge variierten die Latenzzeiten für Teams in verschiedenen Teilen der Welt."

Durch die verbesserte Transparenz kann Delivery Hero nun schneller agieren. Das Unternehmen verfügt über eine komplexe Umgebung mit mehreren Multi-Cloud-Anbietern und lokalen Infrastrukturen. Mittlerweile sind jedoch alle Logs in der Splunk Cloud Platform zusammengeführt. So können die Sicherheitsteams Fehlkonfigurationen in der Cloud-Umgebung leicht aufspüren. Anschließend korrelieren sie die Daten in Splunk und senden Trigger an die betreffenden AWS- oder GCP-Verantwortlichen, die dann umgehend reagieren können. „Früher haben wir Splunk nur für lokale Logs genutzt und konnten deshalb diese Fehlkonfigurationen nicht entdecken", so Papa. „Jetzt deckt Splunk unsere gesamte Multi-Cloud-Umgebung ab., wodurch wir einen viel besseren Überblick haben und Probleme binnen Minuten beheben können. Wir erkennen heute viele Anomalien, die uns früher entgangen wären."

Weniger Aufwand und mehr Kontrolle durch individuelle Berichte

Die Splunk Cloud Platform unterstützt mit ihren zentralisierten Funktionen eine große und stetig wachsende Zahl an Datenquellen, ohne die Ressourcen des Sicherheitsteams unnötig zu beanspruchen. So sorgt beispielsweise ein individuell optimiertes Warnsystem dafür, dass Delivery Hero weniger unnötige Warnungen erhält – das spart Zeit beim Troubleshooting. „Mit Splunk konnten wir unsere Warnmeldungen individuell anpassen und False Positives reduzieren“, erläutert Papa.

Und die verbesserten Erkennungs- und Warnfunktionen sind noch nicht alles. Die Plattform liefert auch aussagekräftigere Kennzahlen und Berichte. So lassen sich mit der Splunk Cloud Platform Berichte in Echtzeit erstellen, in beliebigen Intervallen planmäßig ausführen und in Dashboards verwenden. „Wir haben jetzt sämtliche Schwachstellen im Blick und senden Berichte an die jeweils Verantwortlichen, damit sie über die Leistung ihrer Anwendungen im Bilde sind“, so Papa.

Besonders wichtig ist dies für das globale Sicherheitsteam von Delivery Hero. Papa: „Wir haben mehrere Sicherheitsteams in aller Welt, und jedes davon muss jederzeit in der Lage dazu sein, auf seine Berichte und Warnmeldungen zugreifen und Verbesserungen vornehmen zu können.“

> Früher haben wir Splunk nur für lokale Logs genutzt und konnten deshalb diese Fehlkonfigurationen nicht entdecken. Jetzt deckt die Splunk Cloud Platform unsere gesamte Multi-Cloud-Umgebung ab, wodurch wir einen viel besseren Überblick haben und Probleme binnen Minuten beheben können. Wir erkennen heute viele Anomalien, die uns früher entgangen wären.
>
> **Mauro Papa,** Director of Information Security, Delivery Hero

Erleichtert wird dieser Monitoring-Prozess durch das benutzerfreundliche und individuell anpassbare Dashboard der Splunk Cloud Platform. Außerdem verbessern nahtlose Plug-ins die Konnektivität der Performance-Datenpunkte. Beispielsweise ist Splunk mit dem Projektmanagement-Tool Jira verbunden, sodass das Team wichtige Kennzahlen messen und überwachen kann.

> Dank der Splunk Cloud Plattform kann sich das Security-Team auf Sicherheitsaspekte statt auf die Wartung der Infrastruktur konzentrieren. Unsere Experten befassen sich nun vor allem mit der Konfiguration zusätzlicher Indizes, wobei sie sich auf Einblicke aus den neuen Dashboards stützen und unsere Erkennungsfunktionen erweitern.
>
> **Mauro Papa,** Director of Information Security, Delivery Hero

Mehr Zeit fürs Wesentliche

Splunk nimmt den Sicherheitsexperten von Delivery Hero zeitraubende Infrastruktur-Wartungsaufgaben ab, sodass sie sich voll und ganz der Leistungsoptimierung widmen können.

„Dank der Splunk Cloud Platform kann sich das Security-Team auf Sicherheitsaspekte statt auf die Wartung der Infrastruktur konzentrieren“, fasst Papa zusammen. „Unsere Experten befassen sich nun vor allem mit der Konfiguration zusätzlicher Indizes, wobei sie sich auf Einblicke aus den neuen Dashboards stützen und unsere Erkennungsfunktionen erweitern.“

Um mit dem globalen Wachstum von Delivery Hero Schritt zu halten, hat das Sicherheitsteam schon den nächsten Schritt geplant: Es will Splunk Enterprise Security implementieren, um damit Die Lösung soll im großen Stil datenbasierte Erkenntnisse liefern – Erkenntnisse, die das Unternehmen für die Erfüllung seiner Mission braucht, Kunden „alles zu liefern“. Delivery Hero wird seine enge Zusammenarbeit mit Splunk also fortsetzen, damit sein Ökosystem – das 70 Länder und vier Kontinente umspannt (Tendenz steigend) – weiterhin Heldenhaftes leisten kann.

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