Carrefour reagiert mit der Splunk Cloud Platform 3x schneller auf Sicherheitsbedrohungen

Zentrale Herausforderungen

Obwohl Carrefour viel in die Pflege der alten Infrastruktur und die Erkennung von Sicherheitsvorfällen gesteckt hat, wird es manchmal schwierig, den Kunden das Multi-Channel-Erlebnis zu bieten, das sie erwarten.

Wichtige Ergebnisse

Mit der Splunk Cloud Platform, verwertbaren Erkenntnissen zur Systemleistung und schnellerer Reaktion in Sicherheitsfragen kann Carrefour seine Geschäftsabläufe besser schützen und die Customer Experience verbessern.

Carrefour

Branche: Einzelhandel

Lösungen: Platform, Security

Die Hypermarkt-Kundschaft von heute kauft im Multi-Channel.

Carrefour ist das zweitgrößte Einzelhandelsunternehmen Europas und das achtgrößte weltweit, mit Supermärkten (Hypermarchés) in Europa, Südamerika und Asien. Das Unternehmen weiß, dass die Menschen online heute den gleichen Komfort erwarten wie im Geschäft, ob bei Bestellungen über die Mobile-App oder per „Click and Collect“. Um die Customer Experience bei sämtlichen Online-Einkaufskanälen zu optimieren, hat Carrefour eine Digitalisierungsstrategie gestartet, zu der auch Cloud-Dienste gehören.

Mit der Splunk Cloud Platform hat Carrefour die Agilität zurückgewonnen, sich wieder verstärkt auf die Entwicklung neuer Funktionen und Services konzentrieren zu können. Die Plattform hat außerdem das Thema Security einfacher gemacht, sodass Kunden bei Carrefour unbesorgt einkaufen können. Da Carrefour durch Splunk jetzt Einblicke und Erkenntnisse in Echtzeit erhält, kann das Unternehmen nun dreimal schneller auf Sicherheitsbedrohungen reagieren und potenzielle Vorfälle intelligenter unterbinden.

Datengestützte Ergebnisse

3x
kürzere Reaktionszeiten

€ 10 Mrd.
Umsatzwachstum im E-Commerce bis 2026 erwartet

Mehr
Teamkapazität für wichtige Aufgaben

Dreimal schnellere Reaktion auf Sicherheitsereignisse

Das SOC-Team (Security Operations Center) von Carrefour arbeitet mit einer komplexen Infrastruktur in einem klassischen Rechenzentrum. Darum musste das Team früher viel Zeit und Mühe in die Pflege der Systeme investieren, während der Schutz vor Malware mitunter zu kurz kam. Durch die zentrale Zusammenführung der Sicherheitsanalytik und durch die Integration vielfältiger Datenquellen auf der Splunk Cloud Platform kann das SOC-Team auf Vorfälle nun praktisch in Echtzeit reagieren.

„Die Splunk Cloud Platform verarbeitet alle unsere Logs, ob aus der Antivirensoftware oder von Endpoint Detection and Response,“ sagt Romaric Ducloux, SOC-Analyst bei Carrefour. „Splunk gibt die Warnmeldungen aus, legt ein Ticket an und kontaktiert die SOC-Analysten in Bereitschaft. Es ist der Eckpfeiler unserer Security Operations.“

Durch das Cloud-Modell hat das SOC-Team von Carrefour mehr Zeit, sich auf App-Management, Bedrohungsanalysen und Sicherheitsuntersuchungen zu konzentrieren, da sie mit Splunk den Sicherheitsbetrieb einfacherer und automatisierter verwalten können und sich keine Gedanken mehr um die Infrastruktur machen müssen. Das Team kann bei

Vorfällen jetzt live eingreifen, bevor die Systeme Schaden nehmen oder die Customer Experience davon beeinträchtigt wird. Im Fall einer Kompromittierung lässt sich anhand der gesammelten Informationen rasch erkennen, woran es gelegen hat und wie Carrefour seine Systeme in Zukunft härten kann.

Jetzt reagiert das Team dreimal schneller auf Vorfälle als zuvor. „Dank der Splunk Cloud Platform können wir uns wieder auf unsere wichtigste Aufgabe konzentrieren: dafür zu sorgen, dass unsere Kundschaft immer ein sicheres Einkaufserlebnis hat“, sagt Ducloux.

Innovation und Resilienz dank Splunk

Das Carrefour-Team schätzt besonders, wie gut Splunk Cloud für das gesamte SOC-Team zugänglich ist. Die Abfragesprache zur Untersuchung von Sicherheitsereignissen ist leicht zu verstehen und ermöglicht leistungsstarke Analysen, sodass das SOC-Team rasch tiefgehende Erkenntnisse zu den Taktiken, Techniken und Tools der Cyberangreifer gewinnt und dadurch in Zukunft sehr viel besser gegen Vorfälle gewappnet ist.

> Splunk bietet einen echten Mehrwert. Wir ziehen damit das Maximum an Erkenntnissen aus der Analyse unserer Erkennungsfälle und verschwenden keine Zeit mit der Erstellung von Regeln oder überkomplizierten Tools.“
>
> **Romaric Ducloux,** SOC Analyst, Carrefour

„Splunk bietet einen echten Mehrwert“, sagt Ducloux. „Wir ziehen damit das Maximum an Erkenntnissen aus der Analyse unserer Erkennungsfälle und verschwenden keine Zeit mit der Erstellung von Regeln oder überkomplizierten Tools.“ Und weil mit Splunk nun auch Usern aus anderen Teilen der Welt Zugriff auf alle Informationen gewährt werden kann, die bei einem Sicherheitsereignis auf System- und Betriebsebene anfallen, können sie selbstständig handeln, Untersuchungen durchführen und unternehmensweit Warnmeldungen erzeugen.

> Die Splunk Cloud Platform ist der Eckpfeiler unserer Security Operations.“
>
> **Romaric Ducloux,** SOC Analyst, Carrefour

Zur genaueren Untersuchung von Logs und Daten verwendet das SOC-Team die passende Splunkbase-App. Sie arbeitet nahtlos mit vielfältigen Quellen zusammen, sodass Carrefour Aufgaben wie die Integration von SaaS-Proxy-Servern mit minimalem Aufwand erledigen kann. Das Unternehmen kann jetzt zuversichtlich innovative Funktionen und neue Services für seine Kundschaft einführen, in der Gewissheit, dass solide und effiziente Security Operations gewährleistet sind.

Skalierung auf 10-Milliarden-Umsatz im E-Commerce

Carrefour hat ehrgeizige Pläne für die Zukunft: Der Händler will seinen E-Commerce-Umsatz bis 2026 auf 10 Milliarden Euro verdreifachen und weltweit expandieren.

Die Splunk Cloud Platform skaliert problemlos und kann leicht ein zentrales SOC beherbergen, das zahlreiche Länder umfasst, sowie das wachsende Volumen an Daten und Logs aus zusätzlichen Regionen und Märkten verarbeiten. Mit Splunk gewinnt Carrefour so die Transparenz und die Agilität, die das Unternehmen braucht, um seine innovative Zukunft auf eine verlässlich sichere Grundlage zu stellen.

22-24856-Splunk-Carrefour-A4-CS-101_GER