splunk> a CISCO company

CASE STUDY

La Poste reduziert Fehlalarme um das 10-Fache und schützt die Daten von 1,3 Mio. Kundinnen und Kunden

Zentrale Herausforderungen

Große Datenmengen führten zu langen Latenzzeiten oder sogar zum Absturz der Systeme des Cybersecurity-Teams von La Poste. Dies verlangsamte Untersuchungen und gefährdete die Sicherheit von Kundendaten.

Wichtige Ergebnisse

Seit der Einführung von Splunk Enterprise Security kann das Security-Team von La Poste Bedrohungen besser erkennen und beheben. False Positives wurden um das 10-Fache reduziert; Warnmeldungen werden schneller verarbeitet.

LA POSTE

Branche: Öffentlicher Sektor

Lösungen: Security

Produkte: Splunk Enterprise Security

La Poste – der größte Postzusteller in Frankreich

Wer in Frankreich eine Onlinebestellung tätigt, eine neue Kreditkarte beantragt oder seiner Oma einen Brief schickt, verlässt sich auf La Poste. Der Postzusteller sorgt dafür, dass die bestellte Ware pünktlich eintrifft, die Kreditkarte sicher ankommt und Oma nicht zu lange auf Neuigkeiten warten muss. 1,3 Millionen Kundinnen und Kunden in 63 Ländern vertrauen La Poste tagtäglich nicht nur ihre Briefe und Pakete an, sondern auch ihre Daten – beispielsweise private Adressen und Kontaktinformationen. La Poste muss also nicht nur zuverlässige Zustellungsdienste bereitstellen, sondern auch die Daten seiner Kundschaft schützen.

Für diese Aufgabe ist vor allem die 80-köpfige Cybersecurity-Abteilung, Service de Lutte Contre la Cybercriminalité (SLCC), zuständig. Und die hat alle Hände voll zu tun. Wie andere Unternehmen auch sieht sich La Poste mit einer zunehmend komplexen Bedrohungslandschaft, immer raffinierteren Cyberangriffen und geopolitisch motivierten Vorfällen konfrontiert. Noch dringlicher wird das Thema Cybersecurity durch Großveranstaltungen wie die Olympischen Spiele 2024 in Paris.

Ergebnisse

- 80 % der Warnmeldungen werden nun in unter 13 Minuten verarbeitet.
- False Positives wurden um das 10-Fache reduziert.
- Pro Tag werden bis zu 20 Terabyte an Daten verarbeitet.

2015 führte das Cybersecurity-Team von La Poste Splunk Enterprise Security (Splunk ES) als SIEM-Lösung ein. Das Unternehmen benötigte eine Lösung, mit der es die gewaltigen Datenmengen und vielfältigen Systeme seiner komplexen Umgebung in den Griff bekommen konnte. Außerdem brauchte es starke Funktionen für Untersuchungen und zur Bedrohungsabwehr. „Unsere Mission ist es, die Gruppe vor Bedrohungen und Bedrohungsakteuren zu schützen“, sagt Olivier Cassignac, Leiter der Abteilung zur Erkennung von Sicherheitsvorfällen bei La Poste. „Wir erleben Angriffe jeder Art und Größenordnung. Die Gruppe zu schützen, heißt letztlich, unsere Infrastruktur, Mitarbeiter und Kundschaft zu schützen.“

Sekundenschnelle Untersuchungen mit Splunk

Ziel Nummer eins des SLCC-Teams ist die möglichst frühzeitige Erkennung von Anomalien, damit spezialisierte Analysten diese untersuchen und die zuständigen Teams informieren können. Doch Systemabstürze, verursacht durch die enormen Datenmengen, zogen Untersuchungen immer wieder in die Länge. An einem durchschnittlichen Tag verarbeitet La Poste

über 20 Terabyte an Daten. Fünf Terabyte entfallen allein auf das SLCC-Team. Vor der Einführung von Splunk dauerte die Suche nach bestimmten Ereignissen selbst bei einem deutlich kleineren Datenvolumen Stunden oder endete mit einem Systemabsturz.

Seitdem das Team Splunk Enterprise Security (Splunk ES) nutzt, kann es riesige Datenmengen, die wochen- oder monatelange Zeiträume umfassen, in Sekundenschnelle analysieren. Dadurch spart es wertvolle Zeit und Ressourcen und schafft ein solides Fundament für die Cybersecurity-Infrastruktur der Gruppe. „Angesichts der großen Datenmengen kommt es bei Untersuchungen vor allem auf eine leistungsstarke Suchfunktion an. Splunk ist eine riesige Hilfe, denn damit können wir Daten im Nu abrufen und Analysten haben mehr Zeit für Untersuchungen“, fasst Cassignac zusammen.

> “Für uns ist es enorm wichtig, dass Splunk so umfassend angepasst werden kann. Bei diesem Tool gibt es keine Grenzen. Es gibt viele Lösungen auf dem Markt, doch meines Wissens lässt sich keine davon in diesem Maß anpassen. Jede Funktion, Regel, Suche und jedes Dashboard kann man auf seine Anforderungen zuschneiden.“
>
> **Olivier Cassignac,** Leiter der Abteilung zur Erkennung von Sicherheitsvorfällen bei La Poste

Schluss mit der Warnmeldeflut

Jahr für Jahr wird das SLCC-Team mit Tausenden Warnmeldungen überflutet. Es benötigte also eine Lösung zum Filtern, Kategorisieren und Priorisieren potenzieller Bedrohungen. Und die fand es in Risk-Based Alerting (RBA) von Splunk: Der mittlere Zeitaufwand zur Verarbeitung einer Warnmeldung ist seitdem auf nur 13 Minuten gesunken. (Diese Zeitspanne umfasst alle Schritte vom Eingang der Meldung bis zur Weiterleitung an das zuständige Team.)

Wie ist La Poste das gelungen? Zunächst passte das SLCC-Team Splunk ES – jede Funktion, Regel, Suche und jedes Dashboard – an seine konkreten Anforderungen an. Mithilfe der RBA-Funktionen weist Splunk ES jedem Ereignis eine Risikobewertung zu und gibt eine Warnmeldung aus, wenn das Risiko eine bestimmte Schwelle überschreitet. Das Team wird also nur über potenzielle Bedrohungen und verdächtige Aktivitäten benachrichtigt. Dadurch wurden False Positives um das Zehnfache reduziert, sodass sich Analysten auf wirklich dringliche Bedrohungen konzentrieren und effizienter arbeiten können.

Mit vereinten Kräften gegen neue Bedrohungen

Als nützliche Waffe im Kampf gegen dynamische Bedrohungen hat sich das Threat Intelligence Management von Splunk ES erwiesen. Mit dieser Funktion kann das SLCC-Team neu erkannte Bedrohungen analysieren und in technische Metriken umwandeln. Anhand dieser Metriken lassen sich dann die Warnmeldungen verbessern, sodass die neue Bedrohung künftig leicht identifiziert und eingeordnet werden kann. Auch eine rückwirkende Bedrohungserkennung ist möglich, indem zurückliegende Ereignisse nach früheren Vorkommnissen dieser Bedrohungen durchsucht werden.

Wer zahlreiche Bedrohungen abwehren und ein großes Unternehmen schützen will, braucht dafür jede Menge Personal. La Poste ist hier keine Ausnahme: Die Cybersecurity-Organisation des Unternehmens besteht aus 200 Profis, darunter das SLCC-Team mit mehreren SOC-Experten. Mit Splunk können nun sämtliche Teams ihre Einblicke zusammenführen und gemeinsam maßgeschneiderte Schnittstellen für Anwendungsfälle jeder Art nutzen – sei es für komplexe Analysen, die Überwachung von KPIs oder manuelle Suchen. Splunk hat also nicht nur den Cybersecurity-Teams schnellere, gründlichere Untersuchungen ermöglicht, sondern zugleich auch die Zusammenarbeit mit anderen Teams verbessert.