splunk> turn data into doing™

CASE STUDY

FINRA schützt amerikanische Anleger mit Splunk Cloud und AWS

Zentrale Herausforderungen

Die Financial Industry Regulatory Authority (FINRA) benötigte eine zentralisierte Lösung zur Verarbeitung und Analyse ihrer Daten, die gleichzeitig vor unerwarteten Bedrohungen geschützt werden sollten.

Wichtige Ergebnisse

FINRA verlässt sich jetzt auf Splunk, um Daten aus 170 Anwendungen zu erfassen, die Kosten- und Betriebseffizienz zu steigern und Anleger vor Betrug zu schützen.

Branche: Finanzdienstleistungen

Lösungen: IT-Sicherheit, IT Operations

Marktintegrität ist ein Schlüsselfaktor zur Förderung aktiver Kapitalmärkte.

FINRA beaufsichtigt einen wichtigen Teil der Wertpapierbranche: Unternehmen, die in den Vereinigten Staaten öffentlich mit Wertpapieren handeln. Sie verarbeitet und analysiert dabei riesige Datenmengen. Eine Herausforderung besteht darin, diese Daten vor neuen und unerwarteten Bedrohungen zu schützen. Die Lösung für Security Information and Event Management (SIEM) der FINRA bot – trotz hoher Kosten – nur eingeschränkte Funktionalität.

Datengestützte Ergebnisse

- Erfassung von Daten aus 170 Anwendungen
- Analyse der meisten Transaktion auf dem US-Aktien- und -Optionsmarkt
- Gesteigerte Kosten- und Betriebseffizienz mit Splunk auf AWS

Die Marktintegrität bewahren

Jeden Tag finden in den Vereinigten Staaten bis zu 100 Milliarden Finanztransaktionen auf dem Wertpapiermarkt statt, bei denen es um Milliarden von Dollar von Anlegern geht. Die vom Kongress autorisierte, gemeinnützige Organisation FINRA überwacht dabei die Marktintegrität.

„Wir erfassen Tonnen von Daten zu jedem Auftrag, jedem Angebot und jeder Transaktion auf fast jedem Aktien- und Optionsmarkt in den Vereinigten Staaten und suchen nach Anomalien“, sagt Gary Mikula, Senior Director, Cyber and Information Security bei FINRA. „Es gab zahllose andere Logs, die wir gerne erfassen wollten, wie z.B. Ausweisinformationen und verschiedene Zugriffs-Logs, doch die Aufnahme dieser Daten war bei unserem SIEM nicht möglich. Außerdem bot es keine flexible Benutzeroberfläche.“

Auf der Suche nach einer besseren Lösung zog FINRA mehrere SIEMs in Betracht. Die Produkte konnten zwar Warnmeldungen generieren, verbesserten aber die Datenaufnahme oder -analyse nicht wesentlich. Dann besuchte Mikula SplunkLive! in Washington, D.C. und fand, wonach er suchte: eine Möglichkeit, Big Data aus allen gewünschten Quellen der FINRA in Echtzeit zu erfassen, zu indizieren und zu korrelieren sowie Abfragen durch flexible Dashboards anzupassen.

Alles auf Cloud

FINRA (Financial Industry Regulatory Authority) war bereits von den Fähigkeiten von Splunk Enterprise und Splunk Enterprise Security (ES) überzeugt. Als dann Splunk Cloud auf den Markt kam, beschloss die Behörde, der erste große Kunde dieses neuen Produkts zu werden. Dank des nutzungsbasierten Cloud-Modells passen sich FINRAs Computing-Kosten an mögliche Schwankungen im Bedarf an. Und anstatt Monate mit dem Aufbau einer Umgebung zu verbringen, nutzte FINRA die ausgereiften Datenerfassungs-Agents von Splunk und konnte schon wenige Tage nach der Vertragsunterzeichnung mit der Datenauswertung beginnen. Derzeit erfasst Splunk Logs von 170 verschiedenen

Anwendungen und AWS-Services, darunter Amazon Simple Storage Service (S3), Amazon CloudWatch, AWS Config und AWS CloudTrail. „Keine SIEM-Lösung könnte da mithalten“, sagt Mikula.

Powerhouse Design

Zusätzlich verstärkt wird die Leistungsfähigkeit der Splunk Cloud-Lösung von FINRA durch die Integration mit Amazon Web Services. Dank AWS Lambda kann FINRA Code ausführen, ohne Server bereitzustellen oder zu verwalten, und bezahlt dabei nur die genutzte Rechenzeit. Der Managed Service, Amazon Kinesis Data Firehose, liefert Splunk Streaming-Daten in Echtzeit. Mikula bezeichnet Amazon Kinesis Data Firehose als ideale Lösung für die Erstellung von Abonnementfiltern, um AWS-Logs zuverlässig, sicher, schnell und kosteneffizient zur Analyse in Splunk zu übertragen. Diese Fähigkeit kommt sowohl Entwicklern und Netzwerkfachleuten als auch Sicherheitsspezialisten zugute und verhindert Silostrukturen. „Es ist so eine Partnerschaft zwischen unseren Security- und Operations-Teams entstanden“, erklärt Mikula. „Wir sind alle an denselben Logs interessiert. Jetzt haben wir einen zentralen Ort, an dem wir sie erfassen und auswerten können.“

> Als wir den Leistungsumfang anderer Anbieter prüften, stellten wir fest, dass sie Splunk und seinen Möglichkeiten immer ein Stück hinterherrannten.“
>
> **Gary Mikula,** Senior Director, Cyber and Information Security, FINRA

> Wir setzen unser wertvollstes Gut ein – unsere Fähigkeit, jede Transaktion an jedem Tag auf nahezu jedem US-Aktien- oder Optionsmarkt durchzuführen und die betreffenden Daten in der Cloud zu analysieren. Und wir nutzen Splunk, um dafür zu sorgen, dass dieses wertvolle Gut sicher ist. Splunk und AWS bieten uns gemeinsam eine so noch nie dagewesene Möglichkeit, unsere Investoren zu schützen.“
>
> **Gary Mikula,** Senior Director, Cyber and Information Security, FINRA

Durch solch effiziente Prozesse bleibt FINRA den aufkommenden Bedrohungen einen Schritt voraus, da die Teams Daten jetzt flexibel analysieren können. FINRA ist einer der größten Benutzer von Amazons EMR Hadoop-Framework. Durch die Bereitstellung des Splunk-Agents auf dieser Platform-as-a-Service stehen Informationen zur Verfügung, mit der FINRA die Ressourcenzuweisung optimieren kann. Außerdem hat FINRA ein dediziertes Abrechnungstool eines Drittanbieters ausgemustert und durch einen eigenen Prozess für die Aufnahme der Daten in Splunk ersetzt. Mit Splunk Cloud verfügt FINRA über bessere Analysen und Reportingfunktionen, was zu einer besseren Projektverfolgung bei AWS Services und geringeren Kosten geführt hat.

„Wir verwalten unsere Cloud-Kosten mit unserer Splunk-Lösung effektiver und das für weniger als fünf Prozent der Kosten für die dedizierten Tools“. Zusätzlich zu ihrer Ausrichtung auf Cloud-Computing setzt FINRA auf Open-Source-Softwareentwicklung und sponsert mehrere Open-Source-Projekte in den Bereichen Big Data, DevOps und Qualitätssicherung. Mikulas Team entwickelte sogar ein Tool, um AWS CloudTrail-Logs zu erfassen und aufzunehmen.

Angesichts von Innovationen wie dem serverlosen Computing in der Cloud ist es für FINRA wichtiger denn je, Logs zu verfolgen. „Man kann nie wissen, was die nächste Bedrohung sein wird und welche Fragen wir an unsere Daten stellen möchten. Splunk ermöglicht uns, alle gewünschten Daten einfach zu sammeln und ad hoc abzufragen“, sagt Mikula. „Dazu kommt, dass wir dank der Erkenntnisse aus Splunk mehr AWS-Services nutzen können. Wir setzen unser wertvollstes Gut ein – unsere Fähigkeit, jede Transaktion an jedem Tag auf nahezu jedem US-Aktien- oder Optionsmarkt durchzuführen und die betreffenden Daten in der Cloud zu analysieren. Und wir nutzen Splunk, um dafür zu sorgen, dass dieses wertvolle Gut sicher ist. Splunk und AWS bieten uns gemeinsam eine so noch nie dagewesene Möglichkeit, unsere Investoren zu schützen.“

20-15394-Tier2-FINRA-A4-101-CS_DE