splunk>

CASE STUDY

Finanz Informatik optimiert Risikomanagement mit einer einzigen SIEM-Lösung

finanz informatik

Kurzfassung

Finanz Informatik ist der IT-Dienstleister der Sparkassen-Finanzgruppe mit ihren 416 Sparkassen, 18 Landesbanken bzw. Landesbausparkassen, der DekaBank und verschiedenen Verbundpartnern. Das Angebot der Finanz Informatik umfasst das gesamte IT-Spektrum – von der Entwicklung und Bereitstellung von IT-Anwendungen, Netzwerken und technischer Infrastruktur bis hin zu Beratung, Schulung und Support. Ziel der Finanz Informatik war es, eine verbesserte bereichsübergreifende Sicht auf die zahlreichen Umgebungen sowie entsprechende Analysefunktionen zu erhalten. Seit der Einführung von Splunk Enterprise zeichnen sich für die Finanz Informatik deutliche Verbesserungen ab, wie etwa:

- Schnellere Erkennung und Untersuchung von Vorfällen
- Weniger Komplexität, geringere Fehlerquoten und Kosteneinsparungen
- Optimierter Schutz von Kundendaten

Warum Splunk?

Bisher setzte Finanz Informatik (FI) auf verschiedene SIEM-Lösungen (Security Information and Event Management) für seine Mainframe-, Netzwerk-, Unix- und Windows-Umgebungen. Finanz Informatik wollte auf eine einzige, unternehmensweit eingesetzte SIEM-Plattform umstellen, um eine verbesserte bereichsübergreifende Sicht sowie entsprechende Analysefunktionen zu erhalten.

Zusätzlich zu den technischen Anforderungen wie Datenintegrität, Skalierbarkeit, Hochverfügbarkeit und Support hatte die Korrelation von Sicherheitsereignissen zwischen mehreren Plattformen Top-Priorität für Finanz Informatik. Die neue SIEM-Lösung musste nahtlos in die bestehende IT-Infrastruktur integrierbar und mandantenfähig sein. Heute werden alle von den Plattformen bei Finanz Informatik generierten Maschinendaten in Splunk Enterprise indiziert und analysiert. Dazu zählen Daten von mehreren Tausend Rechnern einschließlich Servern sowie Netzwerk- und Middleware-Komponenten.

Branchen

- Finanzdienstleistungen

Splunk Use Cases

- Security
- Compliance

Herausforderungen

- Mehr Transparenz bei Tausenden Rechnern
- Erkennen von Sicherheitsereignissen in Echtzeit
- Nahtlose Integration der neuen SIEM-Lösung in bestehende Infrastruktur

Auswirkungen für das Unternehmen

- Eine einzige, bereichsübergreifende SIEM-Lösung für die schnellere, umfassendere Untersuchung und Behebung von Sicherheitsvorfällen
- Optimierter Schutz von Kundendaten
- Operative Transparenz über mehrere Plattformen hinweg

Datenquellen

- Logs von Mainframe-Servern
- Logs von Unix-Servern
- Logs von Windows-Servern
- Netzwerklogs
- Logs von Middleware-Komponenten (z. B. Datenbanken und Anwendungsserver)

Splunk-Produkte

- Splunk Enterprise

Erstellen eines umfassenden Sicherheitsinformationssystems

Mit seiner Anwendung OSPlus stellt Finanz Informatik eines der führenden IT-Systeme für den deutschen Bankenmarkt, das 98 Milliarden technischer Transaktionen im Jahr ausführt. Tochterunternehmen wie die Finanz Informatik Technologie Service, die Finanz Informatik Solutions Plus, die Star Finanz und die inasys ergänzen das IT-Portfolio des Unternehmens. Die Finanz Informatik übernimmt den Service für 125 Millionen Konten.

Mit Splunk Enterprise kann die FI – in Echtzeit oder historisch – über mehrere Plattformen hinweg prüfen, wie, wann, wo und von wem auf Informationen und Daten zugegriffen wurde. In Splunk Enterprise wurden Benachrichtigungen eingerichtet, die über Sicherheitsereignisse, Autorisierungsverstöße oder ungewöhnliche Abfragemuster informieren. Die Splunk-Plattform erfüllt die Anforderungen der FI an ein umfassendes Sicherheitsinformationssystem und bietet zudem Vorteile in anderen Anwendungsfällen.

Mehr Sicherheit durch schnellere Erkennung und Untersuchung von Vorfällen

Die Finanz Informatik optimierte ihre Sicherheit durch die schnellere Untersuchung von Vorfällen. Splunk Enterprise löste die zuvor verwendeten SIEM-Tools ab und bietet der FI eine einheitliche Lösung für umfassendes Security Information and Event Management.

Die Analyse von Maschinendaten ist jetzt viel einfacher. Die vorhandenen Daten können schneller und plattformübergreifend ausgewertet werden, was die Erkennung und Analyse potenzieller Sicherheitsvorfälle erleichtert. Mit Splunk Enterprise als Fundament der neuen, zentralen SIEM-Lösung kann die Finanz Informatik den vollen Schutz ihrer Daten besser gewährleisten und gleichzeitig die Komplexität, Fehlerquoten und Kosten für das Unternehmen senken.

„Splunk Enterprise ist eine sehr durchdachte Lösung. Die Software ist für Entwicklung und Betrieb konzipiert und kann in einer Vielzahl von Bereichen umgehend Ergebnisse liefern.“

Irena Wagner-Osterloh
Abteilungsleiterin
Berechtigungstechnologien
Finanz Informatik GmbH & Co. KG

Laden Sie Splunk kostenlos herunter oder testen Sie die Online-Sandbox. Ob für cloud-basierte oder lokale Umgebungen, große oder kleine Teams – Splunk hat auf jeden Fall ein passendes Modell für Sie.

splunk> SplunkCe@Splunk.com www.splunk.com

CS-Splunk-Finanz-Informatik-A4-101_DE