Case Study: Leading Credit Card Network

Streaming Integration and Analytics Enables Timely and Accurate Threat Detection

Overview

A major U.S.-based credit card network uses the Striim™ platform to build an enterprise-wide real-time security event hub that delivers a comprehensive security analytics solution. The company augments its existing security solutions with Striim's real-time data integration and streaming analytics platform to identify potential internal and external security threats immediately, and to reduce the number of false alarms.

Challenges

This leading credit card network was using 50+ IT security solutions including several security information and event management (SIEMs) systems monitoring numerous aspects of their IT infrastructure. Each solution was using near real-time data and provided a siloed perspective, without a comprehensive view. As such, security analysts were unable to identify combinations of alerts from various point solutions that could more accurately signal a specific type of threat. Instead, they spent excessive amounts of time chasing false positives, and risked missing the real threats that needed immediate action.

Solution

With Striim, the credit card network built a user behavior analytics solution on top of a SIEM platform, delivering comprehensive and real-time visibility into all security events to detect threats accurately and immediately. Unlike traditional, siloed SIEM solutions, Striim can collect, prepare, and correlate all types of security data, and distribute to various targets.

The Striim platform ingests events from sources including Syslogs, website logs with card management events, existing SIEM solutions such as CorreLog, end-point security solutions such as Crowdstrike, firewall logs from Palo Alto Networks, network traffic flow logs from Netflow – all in real time. Striim easily handles the high-volume and high-velocity data, and prepares it with transformations and enrichments – such as with blacklisted IPs – for easy and accurate analysis.

While publishing pre-processed events to the Kafka-based enterprise bus in JSON format, the Striim platform tracks and records key metrics about all the events collected, and performs analytics and file management

About:

Fortune 100 Multinational Corporation

Industry:

Financial Services

Region:

Global

Key Solution Benefits:

- Faster response to and remediation of security incidents
- Fewer false positives
- Fast, accurate, and detailed information delivery to incident handlers
- Proactive response to internal and external threats

Case Study: Leading Credit Card Network

where needed. To support timely network security analytics with Cisco Stealthwatch, Striim delivers NetFlow log data in real time to Amazon S3 with highly complex parsing to detect different formats coming from different network devices. Striim also displays card management events coming from the website via real-time dashboards, and runs machine learning algorithms on this streaming data for improved customer experience.

Benefits

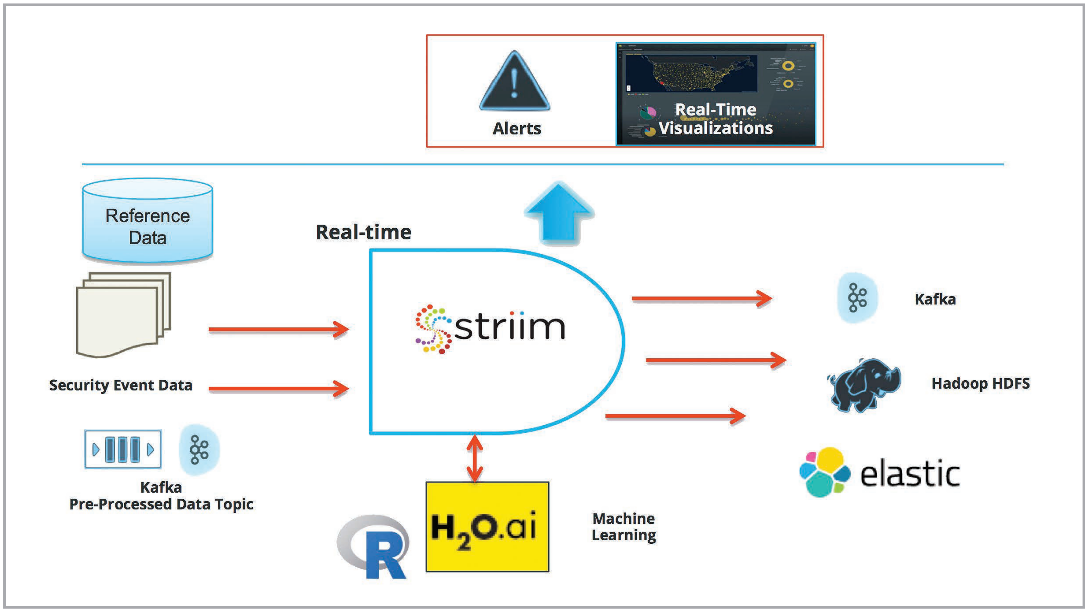
Through Striim's integration with Kafka and ability to pre-process events before delivery, the company has a complete event hub solution that enables flexible access to any security event that occurred in last few hours without any manual effort and the ability keep up with "fast producer-slow consumer" situations.

By correlating end-point security events with other security device logs in real time, Striim enables the customer to immediately and accurately assess potential endpoint hacking incidents – such as file executing from the recycle bin, suspicious SVC host activity, PowerShell abuse, DNS abuse – with full context and broader assessment criteria. The solution also enables them to determine immediately if a blacklisted IP is attempting to log in to the website. On the interactive dashboards, users can see live threat maps showing attacking IPs in real time, and take timely action.

Striim provides the security analysts with relevant event data for assessing the situation further for a more comprehensive and proactive response, increasing their productivity. The pre-processed security events are eventually delivered to their big data analytics environment for further and deeper downstream analysis.

Technology Used

Striim Real-time Data Integration and Intelligence platform.



Alerts
Real-Time
Visualizations
Reference
Data
Real-time
striim
Security Event Data
Kafka
Pre-Processed Data Topic
Kafka
Hadoop HDFS
elastic
H2O.ai
R
Machine
Learning