Case Study: Counteract Security Breaches

Leading Investment Company Looks to Streaming Analytics for Cybersecurity

Summary

A leading Investment company uses Striim's streaming data platform to analyze application log files for their Windows workstation and trading platforms in real time, to detect unauthorized access and wrong passwords attempts and prevent a security breach.

Business Needs

A leading Investment firm, which presents a multitude of products and services to customers and has access to a broad base of investors, needed an enhanced security measure to combat the potential breaches to its trading platforms and employee-facing workstations to minimize the risk and losses.

Challenges

The investment company had deployed HP ArcSight and intended to leverage the technology to monitoring security logs. However, the application was never put into production and the company was in pressing need for an enterprise-grade solution to prevent any security attack.

Solutions and Results

The investment company deployed Striim's real-time data integration and streaming analytics platform to support more sophisticated prevention scenarios with an easy, reliable, and flexible solution. The following IT security applications were built with Striim to prevent the internal and external security attacks:

1. Monitoring Microsoft Workstation Login Security Applications

In this application, Striim analyzes Microsoft Security Event logs in real time to detect unauthorized access and wrong password attempts. When the number of failed login attempts by a particular user or workstation exceeds a given threshold, the application generates alerts via web and email. Striim platform also enables the end users to visualize the data via the Striim dashboard using bar charts.

Leading Investment Bank in Europe

About:
Highly ranked Forbes Global 2000 bank

Industry:
Money Center Banks

Region:
EMEA

Solution:
Detect and Alert

Case Study: Counteract Security Breaches

2. Multiple Log Correlation for Trading Platform's Login Security

As the next project, the investment company implemented Striim for detecting any unauthorized access and wrong password attempts on its online trading platform. In this application, Striim correlates VPN log with their trading applications' logs to check whether there are any users trying to use the trading application with login information other than the information they used to login to the company VPN.

With multi-log correlation capabilities, Striim identifies for any given user the temporary IP address provided by the VPN for their ongoing VPN session, and cross checks their info with the trading application logs to match to the unique user so it can track their log-in behavior in real time. The Striim platform detects within the 2-hour time window, which is the maximum VPN session duration in this investment company, if the user logs in to the trading platform with any different credentials other than the one used for the VPN. For example, if someone logs into the VPN as "Joe Smith" but afterward tries to log into the trading application as an "admin" or "Jane Brown" or has multiple different login attempts with different names, Striim's application sends alerts, and the login attempt is invalidated. With this application, the company can detect and prevent if someone stole VPN login credentials and wanted to hack into other company applications.

If the company chose to do this correlation after the fact with batch files, it would be significantly more time consuming to correlate the log files from multiple different sessions with different users. Striim's real-time analysis of multiple logs enables the company to detect possible threats accurately and promptly with minimal effort.

3. Anti-Money Laundering (AML)

The investment company implemented an application with Striim for money laundry detection as well. In this use case, the Striim platform identifies potential money laundry cases by analyzing trade transaction data and market data. The application identifies the equities in the National Equity Market with the transaction ratio (market cap/transaction volume) over 6% and the customers who are generating more than 25% of the transaction volume of those equities. As another potential money laundry scenario, Striim detects the customers that are generating equity transaction volumes of 5% of the Emerging Companies Market and 10% or more of the National Equity Market.

The parent company of this investment company also uses Striim for preventing ATM fraud. The application built with Striim detects the cases when a credit or debit card is used from two different ATM devices more than 10km distance from each other within a 5-minute window.