Use Case: Enterprise Security

Bridging the Gaps in Security Infrastructure in Real Time

Today's dynamic organizations require flexible, scalable, real-time security solutions that can quickly and continuously adapt to new threats and changing business requirements. The simple, siloed monitoring of traditional security events is no longer sufficient.

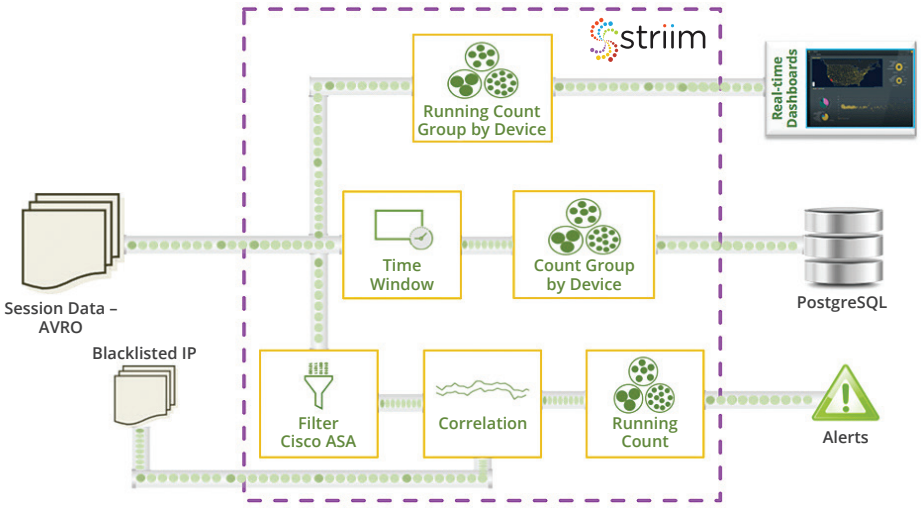
Enterprises that invest in SIEM (Security Information and Event Management) solutions often become frustrated maintaining the separate data sources that supply the SIEM tools with security events to analyze, or writing the correlation rules to make sense of the mountain of data. And the siloed and proprietary nature of SIEM applications leaves gaps in monitoring, context and visibility, resulting in inaccurate alerting.

Security experts must look for real-time insights from multiple data sources generated at massive scale and velocity.

Real World Case Study: A Leading Credit Card Network

Sophisticated pattern detection for simplifying and improving cybersecurity

This high-profile credit card network chose Striim to analyze security log files of 50+ siloed SIEM security solutions (monitoring servers, proxy, firewall, etc.). This information is combined with session data to enable pattern matching that was otherwise undetectable without an aggregate overview of all silos, and ability to implement complex rules.



The Striim Security Solution

- Transcend siloed SIEM environments to quickly understand and counteract cyberattacks and fraud
- Provide continuous data collection, enrichment and correlation of data and events from multiple sources in real time
- Trigger actions, workflows and alerts using new or existing notification, API or incident management systems
- Simplify operations with easy monitoring, visualization and alerting
- Enable user-defined security rules for flexible and custom threat detection involving multiple data sources

Use Case: Enterprise Security

Previously, the existing SIEM security solutions resulted in many alerts and false positives that the security team could not act upon. The goal of this project was to improve alert accuracy with more sophisticated rules, and improve the security team's understanding of the alerts generated.

The Striim platform is used to join the aggregated log file and session logs in AVRO format as input, enriching the streaming data with region and event type, correlating it with a blacklisted IP address list, detecting patterns based on complex rules, and providing meaningful alerts that now serve as the single source of truth for security threats.

Striim's results are sent to real-time dashboards and are written to datamarts in HAWQ via PostgreSQL to support reporting and to update the blacklist IP table.

The Striim Solution

Real-time Ingestion of Security Events, Continuous Monitoring and Anomaly Detection

Striim offers real-time data integration, streaming analytics and highly flexible platform-centric approach for solving security challenges. The Striim platform can ingest data from multiple sources (i.e., enterprise databases, a variety of log files, message queues, and sensors), analyze the information as it streams, and produce actionable results (i.e., alerts, actions, recommendations) in real time. The Striim platform takes advantage of real-time correlation of events and pattern matching to proactively identify threats.

The Striim platform is used for a broad array of security use cases. Here are a few examples:

- Detecting malicious employee behavior before the employee can steal and misuse confidential data
- Identifying violation-type events and enabling immediate response
- Continuously monitoring compliance and regulatory requirements
- Looking for malicious IP addresses attempting to login to applications, triggering a workflow, for example, that requires additional authentication
- Detecting network activity that might be indicative of new threats
- Streaming real-time comparison of security events with IoCs (Indicators of Compromise)
- Identifying fraud by impossible distance using login by IP and geolocation data

For companies with existing machine learning models, Striim is used to feed massive volumes of both streaming and static reference data in real time into the existing machine learning models, processing and enriching the data in-stream.

