Striim for Enterprise Security

A Holistic Approach to Real-Time Enterprise Security Analysis

Striim™ (pronounced 'Stream') enables businesses to achieve a comprehensive view of their potential internal and external vulnerabilities, and deliver a more timely and effective response to real threats.

Striim is not meant to replace SIEMs. Striim complements existing security solutions and traditional SIEM software with an end-to-end streaming integration and analytics platform in support of a holistic security strategy. By ingesting, organizing, correlating, visualizing, and alerting on all security events – automatically, in real time – Striim enables businesses to detect and act on security threats immediately, with fewer false alarms.

In addition, Striim enables users to operationalize artificial intelligence (AI) results via integration with leading AI frameworks, and to validate machine learning models.

Striim Security Use Cases

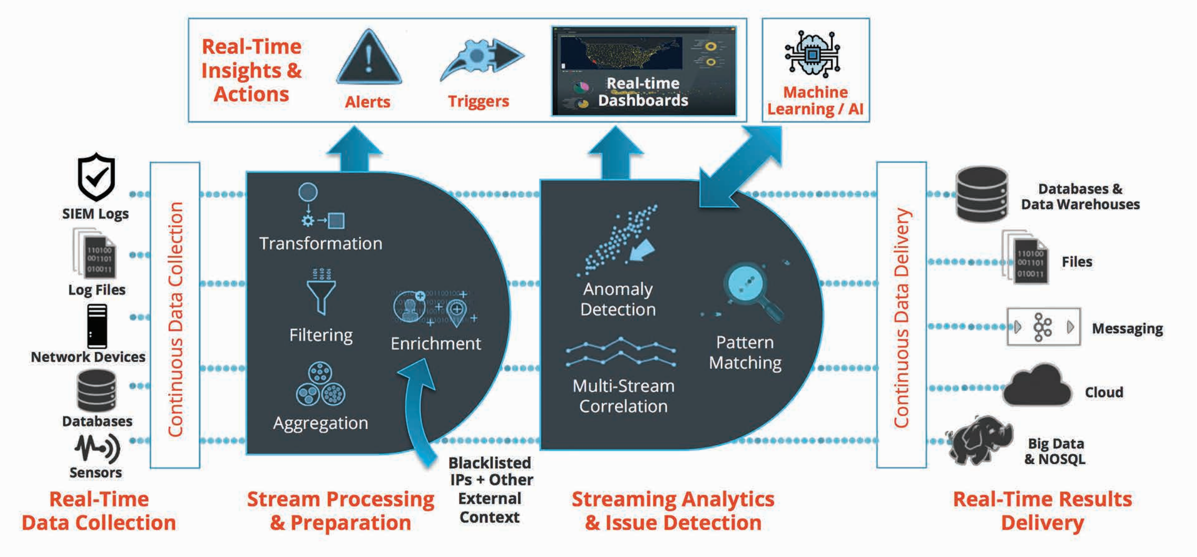
Real-Time Security Log Correlation: Striim analyzes multiple endpoint security solutions' logs and different infrastructure components' logs in real time to identify issues or exploits that are not obvious from a single security solution. Striim correlates security events (such as a file executing from the recycle bin) with operational logs for context (such as login and logout times and locations). This comprehensive view enables incident assessment in seconds that would otherwise take hours for an analyst to compile and correlate by hand, and helps eliminate false positives.

Alerting On and Containing Malware Infections: Striim analyzes the logs from the Anti-Virus software and the logs from the IDS that show the compromised computer performing scans and attempting to infect other systems with malware, and issues alarms. By visualizing logs via Striim in real time, incident handlers can identify all affected computers at once and focus their efforts on the infected systems immediately.

Benefits of Striim for Enterprise Security

- ✓ Faster response and remediation
- ✓ Fewer false positives
- ✓ Fast, accurate, and detailed delivery of analysis to incident handlers
- ✓ Higher productivity for security analysts
- ✓ Ability to customize alerts and application logic
- ✓ Proactive response to internal and external threats
- ✓ Easier compliance with regulations
- ✓ Support beyond security use cases for real-time operational intelligence

Real-Time Monitoring of Failed and Invalid Logins: Striim analyzes system logs, and tracks invalid user IDs and invalid passwords by source IP in real time. The platform cross-checks against blacklisted IPs and triggers alarms based on event counts and other custom criteria. Striim can share this data with machine learning software to augment anomaly detection. This rich, live information enables security analysts to quickly and accurately take action such as blocking a problematic IP address.



Core Striim Platform Capabilities

Striim offers the following key features to support a holistic security strategy:

- **Real-Time Integration for All Security Events:** Integrate and analyze from different sources including existing SIEM event logs, network IDS logs, firewall logs, router logs, application logs, as well as sensors, transactional databases; can interface with existing logging systems such as SYSLOG-NG
- **Enterprise-wide, Multi-Log Correlation:** Correlate multiple streaming sources to see patterns that point SIEM solutions cannot detect
- **Live Dashboards:** Display rich contextual data on interactive dashboards enabling fast and accurate threat assessment
- **Real-Time Alerts:** Send alerts via email, text, and dashboards instantaneously
- **Real-Time Action:** Trigger automatic actions to mitigate damage
- **Easy Customization:** Allow easy modification to application logic to adapt to new threats
- **Easy Integration:** Distribute events and analytics results to downstream analytics, artificial intelligence, and log repositories for broader analytics and compliance purposes

For more information or to request a demo of the Striim platform, please contact the Striim Team at **info@striim.com**.