securonix

SOLUTION BRIEF

Log Automation & Real-Time Enrichment

Data-Driven Approach to Identify Security Events

Is your SIEM giving you the whole story?

Most SIEMs focus on making logs available without including real-time context. Contextual data helps you see the whole story based on an alert or event. If contextual information isn't a part of the real-time enrichment process, the burden falls on analyst, which can lead to longer response times. Adding to this, most SIEMs must manually onboard data sources for ingesting data and collecting logs. Manual onboarding is a time-consuming process. Securonix automates the data onboarding process and provides auto discovery of log sources and devices. This reduces detection times and helps analysts to quickly gather data for further investigation and analysis. Securonix Next-Gen SIEM provides better visibility and context with real-time data ingestion and data parsing. Securonix enriches data in real-time with contextual information to pull relevant information together for SOC analysts, giving them context for a threat actor and target before they even start an investigation.

Real-time Context Enrichment for Rapid Investigation

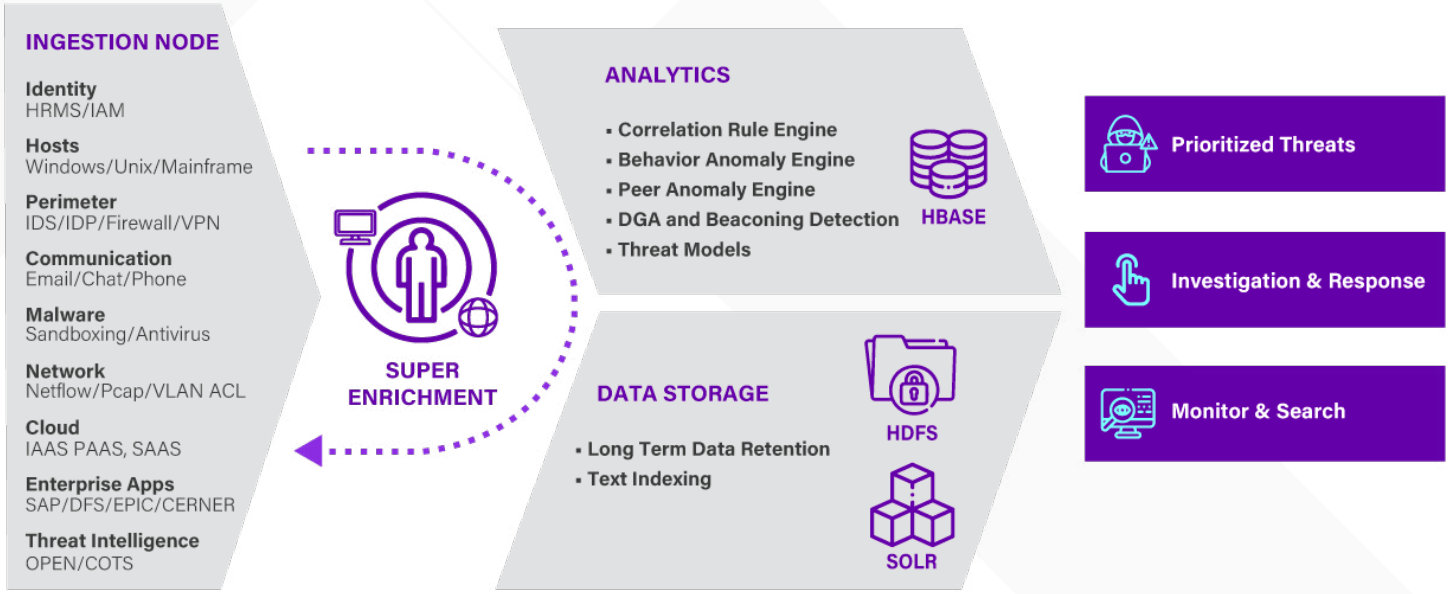
Without context, your analysts aren't getting the whole story and must spend time pulling together the contextual puzzle pieces while investigating. Adding contextual information such as user IP address, asset inventory, and geolocation, along with a host of other sources, provides valuable insights to SOC analysts to help them identify real threats faster. Your SOC team will discover risks faster if this enrichment is done in real-time at the time of ingestion/parsing instead of during an investigation. Securonix provides a comprehensive view that allows you to gain value faster by simplifying data onboarding through automation and intuitive workflows. Automated device discovery ensures onboarding of log data from all devices while keeping you in compliance.

Faster Threat Detection With Simplified Data Ingestion

Onboarding data from various data sources from your environment can be a very time-consuming process. Automation helps improve the data onboarding process. Securonix automatically detects data/log sources and provides an intuitive onboarding workflow, to make data available for better visibility, search, and analytics.

Quicker Incident Response Through Context Enrichment

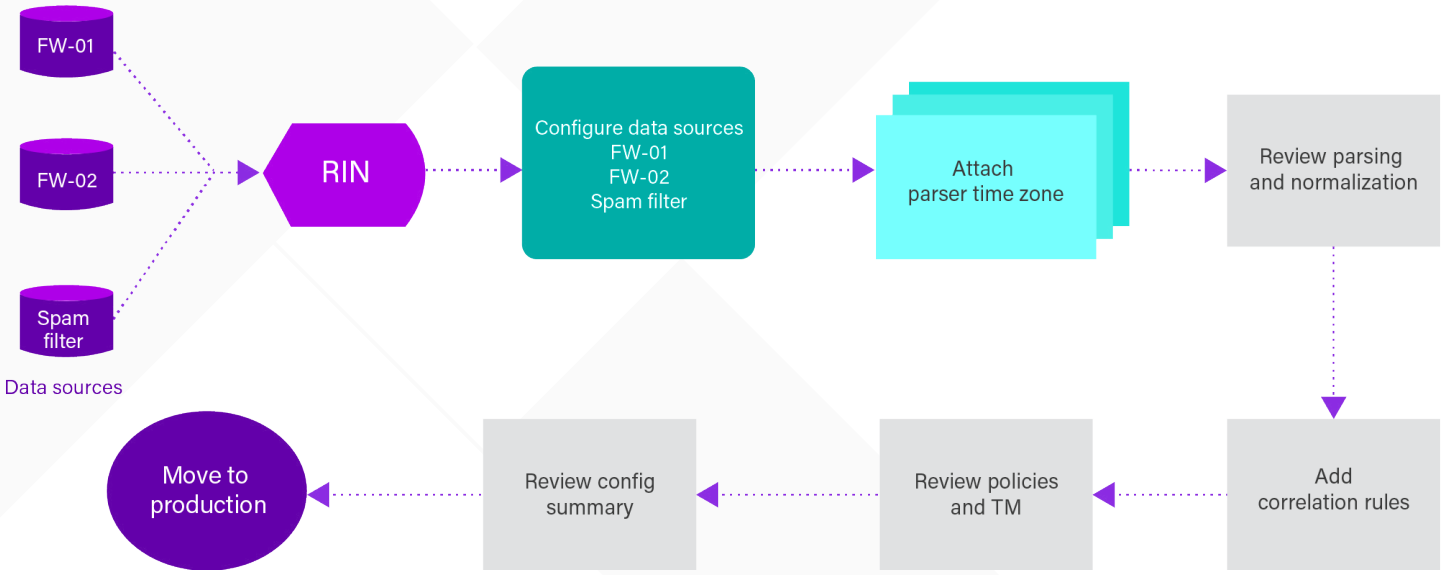
Security alerts without context slow down security investigations. When every second counts, having context in real time and not correlated after an investigation starts, lowers the mean time to respond. Securonix Next-Gen SIEM combines security events with user context before incident response begins.



Faster Detection With Simplified Data Ingestion

Streamline and consolidate security data to create a single, unified view of data, users, hosts, and events. Securonix provides stronger visibility for your security team by having all your data and contextual information in the same place for a unified view.

- **Data Onboarding Automation:** Securonix Next-Gen SIEM automates the data onboarding process and provides auto discovery of log sources and devices. This onboarding process features an intuitive workflow and fewer clicks for a better user experience and visibility into device status. For example, it will alert and notify you when a device turns off.Customize and configure your filters to send only relevant logs (on criteria such as user, data type, etc.) to the Securonix SIEM.
- **Centralized Configuration:** Securonix simplifies parsing, classification, and data enrichment settings when data is onboarded. Our Next-Gen SIEM provides a single view making reviews and parser creation easier, allowing you to review, map, and add conditional actions on the same page.
- **Auto-discovery:** Securonix provides auto-discovery of syslog-based data sources that simplifies and automates the onboarding process. This new workflow improves the time to value for onboarding data sources. With this, you can auto-discover devices, attach parser and time zones in the discovery phase, and seamlessly onboard bulk devices to provide faster time to value.



Quicker Incident Response With Real-Time Contextual Enrichment

Securonix enriches data with contextual information to provide enhancement and normalization that explains user-host relationships and how they interact. Securonix Next-Gen SIEM enriches data in real time and seamlessly provides context for the artifacts identified in the incident. Incidents are multiple security detections that are combined into a single alert. This allows you to prioritize critical incidents and reduce the noise of trivial detections. The enriched data can be used in analytics and is searchable for threats.

Key use cases include:

- **Event and Risk Aggregation:** Securonix enriches security data and connects it with an entity such as a user, host, or IP address. By pivoting on any entity, this offers event aggregation and the ability to search enhanced events across data sources. It allows risk scores to be grouped and assigned to a specific entity for threat prioritization.
- **Point-in-time Context:** Threat intelligence, vulnerability context, and IP addresses are all data that is only available at a specific point of time. This augmented data can be used in analytics and is searchable for threat hunting, where contextual knowledge dramatically reduces inquiry time.
- **Threat Intelligence:** Securonix adds threat intelligence context from sources like WHOIS, VirusTotal, and several others. This contextual information can be used for real-time analytics, behavior profiling, and risk boosting, as well as updating watchlists, look-up tables, and active lists.
- **Real-time Analytics:** Securonix uses Apache Spark analytics jobs on enriched Kafka topics to perform real-time streaming analytics. Doing this on enriched events enables Securonix to include contextual data in the analytics.
- **Business Context Integration:** Integrate business-relevant contextual information such as organization hierarchies and risk tables as well as user offices and email addresses. This enhances your ability to evaluate risk within individual organizations and enables the isolation of more types of vulnerabilities and threats.

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.
For more information visit securonix.com