LogRhythm
The Security Intelligence Company

AnalytiX

Data Visibility, Normalization, and Analysis – at Scale

Digital transformation is rapidly increasing sources of data, and your environment is constantly changing as a result. Data is stored locally, in the cloud, and in different organizational silos – making it difficult to obtain visibility across all your log data to troubleshoot and detect security events.

To further complicate things, devices and applications running in your environment generate log and machine data with a variety of logging standards, leading to increasing inconsistencies in the content, taxonomy, and syntax of logs across vendors. Without a standardized syntax, searching across your data is complicated. To search effectively, you would need extensive knowledge of the logs themselves, and even then the results would vary depending on how you query, creating inconsistencies and unintentional blind spots. You may have tried freemium or open-source solutions to organize the chaos of data and gain clarity, but operational complexity and unpredictable search results impede your ability to achieve pervasive visibility across your environment.

Real-Time Enterprise Visibility

To gain actionable insights from all your data, regardless of source or format, you need a log management solution that delivers a consistent schema across all data types while removing inherent inconsistencies. LogRhythm AnalytiX centralizes your organization's infrastructure, application logs, and data silos. It enriches your data with contextual details and translates various obscure log syntaxes to a consistent and predictable structure, improving search precision and analysis. With LogRhythm AnalytiX, you can quickly search across your organization's vast amount of data to answer any question, identify IT and security events, and quickly troubleshoot operational issues.

The ease of data consumption is just as important as data collection. AnalytiX establishes a consistent method for normalizing and activating your data, laying the foundation for intuitive visualizations and dashboards that quickly identify areas within your environment that need attention. By providing holistic views across your organization – coupled with the ability to drill-down into dashboards for further investigation – LogRhythm evolved the threat hunting process for more accurate and rapid results.

Benefits

- **Gain pervasive visibility** with dynamic collection capabilities and visualizations for clarity around security incidents and operational issues
- **Achieve full data utilization** by taking advantage of a consistent data model with enriched context for search
- **Realize immediate value** with precise search results and real-time analysis

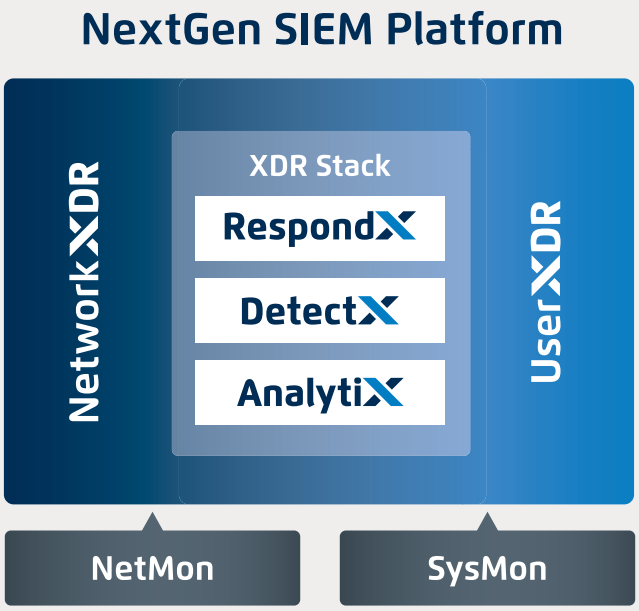
Features

- **Structured and unstructured search** makes finding answers easy, even without knowing the underlying data structure or learning a new query language
- **Machine Data Intelligence (MDI) Fabric** enables collection of an extensive array of log and security data across physical, virtual, and cloud environments, including collection of custom application logs
- **AI Engine** allows for automated, continuous analysis and correlation across all activity with minimal processing for real-time identification of risks, threats, and critical operational issues
- **Centralized dashboards and visualizations** support analysts' quick interpretation of search results and analysis

Simplified Data Analysis

Search across unstructured keywords, as well as across derived and tiered categories, yields higher levels of precision for a diverse set of needs and use cases across security, compliance, and operations. LogRhythm AnalytiX doesn't require memorization of a complex search language, so it reduces your training needs and simplifies the process of executing search queries. AnalytiX's intuitive search builders write effective queries that zero in on results accessible in powerful, customizable visualizations and dashboards that enable faster incident detection and qualification.

Effective analysis requires not only comprehensive collection of all data types, but also consistent normalization to ensure full utilization of the data collected. LogRhythm's Machine Data Intelligence (MDI) Fabric provides a consistent data structure that ensures accurate machine-based analytics to detect threats in real time. Additionally, LogRhythm's MDI Fabric is curated and updated so you can immediately collect and process data for expedited time to value while lowering the learning curve typically needed for other log analysis solutions.



Advance Your Security Operations Maturity with the XDR Stack

By managing data at scale for immediate visibility across your enterprise, you are solidifying a critical part of your security infrastructure that will act as your most powerful ally against threat actors.

With LogRhythm's modular NextGen SIEM Platform design, your organization can add capabilities and expand its security maturity as need arises.

LogRhythm's XDR Stack centralizes all the necessary components to establish a security foundation capable of identifying malicious patterns, uncovering unknown threats, and ensuring rapid threat response and compliance adherence.

See **AnalytiX** and the **XDR Stack** in action. Request a demo today.

logrhythm.com/demo

www.logrhythm.com

LogRhythm