LogRhythm Intelligence

See the threats that matter with behavior analytics that apply machine-learning (ML) to security data in LogRhythm SIEM. Combat user and entity-based cyberthreats with a holistic approach through the industry's most accurate threat detection, investigation, and response (TDIR) platform.

With the dramatic increase in the number of cyberattacks and the advancement in their complexity and sophistication, it's crucial to expand detection capabilities with advanced analytics such as ML. Most breaches involve credential theft or misuse that appears as anomalous activity on an endpoint, server, or application. With many of the most costly breaches involving compromised credentials, the need to combine fact-based rules with behavior analytics is more important than ever. Using ML, behavior analytics identifies anomalies by developing a baseline of normal behavior for user and entities, and then raises observations when activity deviates from that baseline.

LogRhythm Intelligence, a cloud-native add-on to LogRhythm SIEM, collects data from LogRhythm SIEM and processes it using ML to detect anomalies related to potential user attacks such as insider threats, compromised accounts, and administrator misuse. By upgrading an organization's defenses, analysts can contend with sophisticated and credential-based attacks, all within the simplified workflow of LogRhythm SIEM.

LogRhythm Intelligence adapts through ML by establishing baselines and auto-scoring events by risk level. ML boosts entity context classification, distinguishing between workstations, servers, service accounts, and human users, enabling continuous tuning without manual intervention. Ingest logs, alerts, and other telemetry; enrich them with intelligence, location, and user/host context; then run behavioral detections. Risk-based prioritization within the LogRhythm SIEM workflow helps analysts triage, investigate, and respond to insider threats more efficiently.

Benefits

→ **Detect User and Entity Behavior Anomalies**

→ **See the Entire Security Story**

→ **Increase SecOps Efficiency**

> "No other technology provides insights and behavioral model customization like Exabeam. They pioneered user and entity behavior analytics (UEBA)."
>
> **– Nick Forster, Head of Security Operations, The Missing Link**

LogRhythm SIEM ingests logs, and then normalizes and enriches the data utilizing its unique Machine Data Intelligence (MDI) Fabric. MDI Fabric provides data enrichment with unique, rich metadata, and contextual information that feeds from LogRhythm Intelligence back into LogRhythm SIEM. Insights generated by 795 behavioral models are uniquely applied to every user and device to measure normal and abnormal behavior and is complemented by over 2,800 fact-based rules. Analysts become more efficient as they can focus on the threats that that matter instead of creating complex queries for investigation.

The results are greater visibility into sophisticated attacks and techniques resulting in faster, more accurate TDIR within LogRhythm SIEM.

LogRhythm Intelligence functions as an advanced user entity and behavior log source within LogRhythm SIEM.

Includes

- → 795 Behavioral Models
- → 2,800 Fact-Based rules

As with any other log in LogRhythm SIEM, you can build customizable dashboards, run and save searches, leverage Advanced Intelligence (AI) Engine rules for setting alarms, and using SmartResponse™ automated actions when desired. LogRhythm Intelligence seamlessly integrates into the LogRhythm SIEM user interface (UI), enabling analysts the ability to incorporate behavior analytics into their current operating procedure.

Features

Flexible Cloud-Native Add-On

Cloud-native architecture, built on Google Cloud, provides rapid data ingestion and powerful behavioral analytics into LogRhythm SIEM.

Collection

Immediately collect from over 1,000 logs from software as a service (SaaS), self-hosted cloud, and on-prem sources that give you visibility as soon as possible. Automatic collection of Authentication logs (AD/Entra, IdP), Windows, EDR, DLP, and M365 enables immediate results.

Behavior Analytics

Includes more than 2,800 fact-based rules, including cloud infrastructure security, and more than 735 behavioral model histograms that automatically establish a baseline of normal behavior for users and devices to detect, prioritize, and respond to anomalies based on risk.

Enrichment and Normalization of Logs

Log data is normalized and enriched into LogRhythm SIEM with our patented Machine Data Intelligence (MDI) Fabric to improve searchability and behavior analytics across disparate log sources. With deep intelligence into common and unique data source types and pre-built processing rules, MDI Fabric ensures that metadata is automatically and accurately extracted at the point of ingestion.

Advanced Intelligence (AI) Engine

LogRhythm's AI Engine provides correlation rules with predefined relationships between entities to escalate events and alerts. Write, test, publish, and monitor your own rules for your most critical business entities and assets.

Dashboards, Search, and Reporting Capabilities

Search user and entity log sources at any time and continuously monitor via dashboards to enhance visibility into investigations and behavior analytics. Search common events to find relevant events across log sources without having prior knowledge of the underlying log structure. Save dashboards and searches and schedule specific reports daily, monthly, and/or quarterly.

Guided and Intuitive Workflows

Detect, investigate, and respond to threats more easily with workflows that are consistent across the platform, which additionally reduces ramp time on the platform.

Automatic Alerts

Risk-based alerts are automatically generated from behavior analytics, allowing for prompt incident response and reduction in alert fatigue. Quickly investigate suspicious activity by easily drilling down into evidence associated with each alert.

AI Engine Correlation Rules Testing

Enable threat detection engineering with the ability to test that correlation rules are fine-tuned for your environment. Easily conduct red team exercises and penetration tests to check for exploitable vulnerabilities within the LogRhythm SIEM user interface (UI).

Security Orchestration Automation and Response (SOAR)

Accelerate your team's efficiency and productivity with embedded SOAR capabilities and integration with over 80 partner solutions. Automate incident response and investigation workflows by automatically creating cases from the AI Engine for faster response times. LogRhythm's case management centralizes investigations to help prioritize workflows across the security team while tracking which cases require immediate attention. LogRhythm's SmartResponse delivers automated playbook actions or semi-automated, approval-based response actions for streamlined efficiency across the incident response workflow.

Knowledge Base

Obtain bi-weekly updates in our Knowledge Base with modules that combine actionable intelligence with advanced analytics to help improve your security posture.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

exabeam™

Learn more at
www.exabeam.com →