LogRhythm SIEM

Easily secure your environment with the most accurate end-to-end self-hosted SIEM powered by synchronized threat intelligence, security analytics, and automated incident response for efficient threat detection, investigation, and response (TDIR).

There is a lot riding on the shoulders of a security operations team: protecting the organization's reputation, safeguarding sensitive client information, and ensuring the organization's ability to deliver products and services. But overtaxed security teams are stretched thin by the burden of managing the overwhelming amounts of disparate data, advanced threats due to digital weaponization, increase in cloud technologies, and the struggle to hire and retain talent. When security teams are stretched to the limit, LogRhythm SIEM quickly lightens the load to help focus on the threats that matter.

Quickly gain control of your environment with the most accurate end-to-end SIEM built for security teams that are overwhelmed by immense amounts of data and an ever-evolving threat landscape.

LogRhythm SIEM's ability to collect from anywhere and dynamic enrichment powers the most accurate machine analytics, automated incident response, and ability to easily comply with necessary mandates. See the entire security story by automatically gaining contextual insight into critical cybersecurity threats with dashboards, searches, and simplified workflows that quickly reduce noise to secure the environment. LogRhythm SIEM reduces the burden of managing threats, helping security teams prioritize and focus on the work that matters through the most efficient threat detection, investigation, and response (TDIR) solution.

Gain immediate return on investment with the ability to gather, normalize, and interpret data from over 1,000 third-party products and cloud services that are easily searchable. Instantaneously use over 1,000 pre-built rules to detect and remediate security incidents within days of implementation. 28 prepackaged compliance frameworks include lists, correlation rules, alerts, and reports that streamline necessary mandates without the need for manual processes. Enable analysts at all levels to quickly understand the severity of threats with built-in response capabilities that help eliminate threats quickly.

Benefits

- → **Gain Comprehensive Visibility**
- → **Quickly Reduce Detection and Response Time**
- → **Streamline Compliance**

Includes

- → **+1,000 Pre-Built Rules**
- → **28 Compliance Frameworks**
- → **+1,000 Third-Party Data Sources**

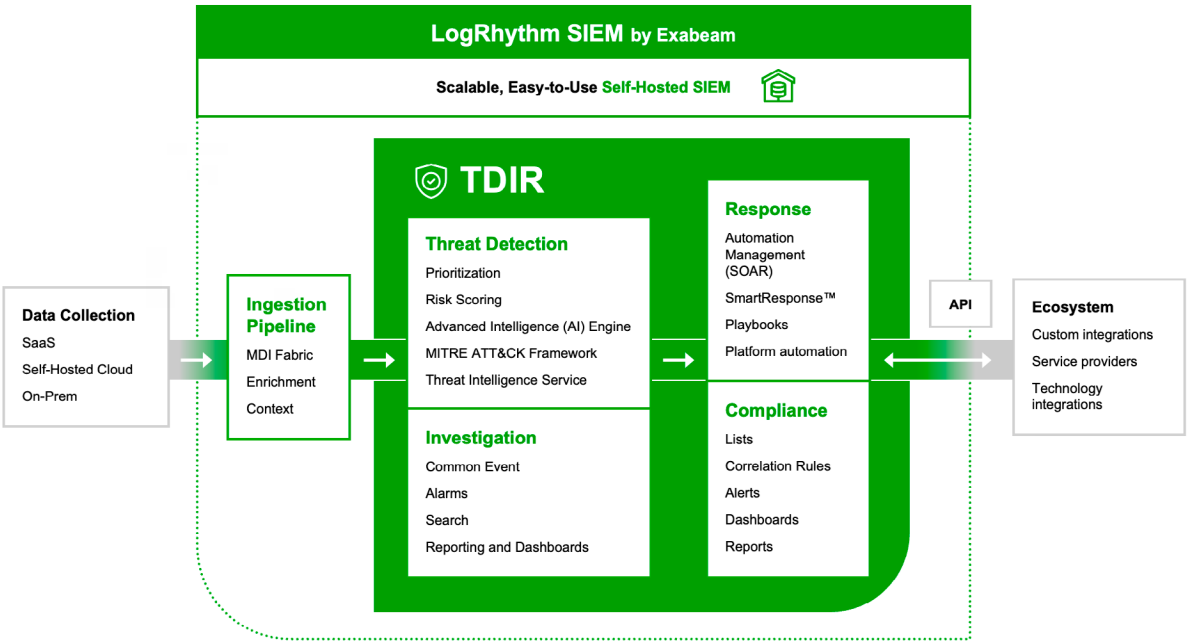

Figure 1.

LogRhythm SIEM

Features

Flexible Self-Hosted Platform

Scale smoothly as your security operations center (SOC) grows. LogRhythm SIEM is designed to easily integrate with other cloud services and on-prem applications.

Open Collection Architecture

Immediately collect from over 1,000 log sources, including software as a service (SaaS), self-hosted cloud, and on-prem. Integrations from cloud collectors, agents, and customizable API and Webhook connections ensure you have visibility into your environment.

JSON Parsing

The JSON Policy Builder feature only requires a few clicks. Guided workflows help build new policies to ensure future JSON logs can be easily searched and automatically fed into visualizations and detections.

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 machine 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

The Advanced Intelligence (AI) engine includes over 1,000 actionable prepackaged correlation rules including rules mapped to the MITRE ATT&CK® framework and compliance modules. Easily build your own custom threat detections based on criteria that matter to your organization.

Dashboards, Search, and Reporting Capabilities

Search the entire log store at any time and continuously monitor via dashboards to enhance visibility into investigations and security analytics. Search common events to find relevant security events across different vendors' 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.

Automatic Alerts

Risk-based alerts are automatically generated from machine analytics, allowing for prompt incident response and reduction in alert fatigue. Quickly investigate suspicious activity by 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. SmartResponse delivers automated playbook actions or semi-automated, approval-based response actions for streamlined efficiency across the incident response workflow.

Compliance

Streamline the compliance process with 28 prebuilt content that includes lists, AI Engine correlation rules and alerts, dashboards, searches, and reporting for regulation standards such as ISO 27001, PCI DDS, GDPR, NIST (800-53, 800-171, CSF), CMCC, CIS, etc. — helping your team comply with necessary mandates more efficiently and effectively than manual processes. Our in-house compliance experts develop these modules, providing you with the content specifically mapped to the individual controls of each regulation.

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 →