# LogRhythm SIEM

Secure your environment with a self-hosted SIEM purpose-built for organizations that need full control, visibility, and compliance support. With LogRhythm SIEM, you gain advanced analytics, synchronized threat intelligence, and automated response to improve threat detection, investigation, and response (TDIR).

Your team faces constant pressure from advanced threats, fragmented visibility, and a growing skills gap. Burnout and alert fatigue make it difficult to separate real threats from noise. LogRhythm SIEM reduces this burden by surfacing high-fidelity alerts, accelerating investigations, and strengthening resilience against modern cyberattacks.

No organization can afford visibility gaps. LogRhythm SIEM delivers broad coverage and the scalability required to manage massive log volumes. Open collection from more than 1,000 sources and patented Machine Data Intelligence (MDI) enrichment give you accurate analytics, automated workflows, and streamlined compliance. Contextual dashboards help you see the full security story, while guided workflows reduce noise and improve time to value.

Realize outcomes quickly with prebuilt integrations, rules, and compliance content. Over 1,000 correlation rules and 28 prepackaged frameworks enable faster detection, audit readiness, and reporting. Guided workflows and automated response help you assess threat severity and contain incidents faster.

LogRhythm SIEM also delivers long-term value. Transparent licensing and unlimited data ingestion eliminate hidden costs as your environment scales. You gain confidence knowing your team can close coverage gaps, meet compliance requirements, and maximize security investments while maintaining full control.

## Benefits

- → Gain Comprehensive Visibility
- → Quickly Reduce Detection
- → Streamline Compliance

## Includes:

- → 1,000+ Prebuilt Correlation Rules
- → 28 Compliance Frameworks
- → 1,000+ Third-Party Data Sources

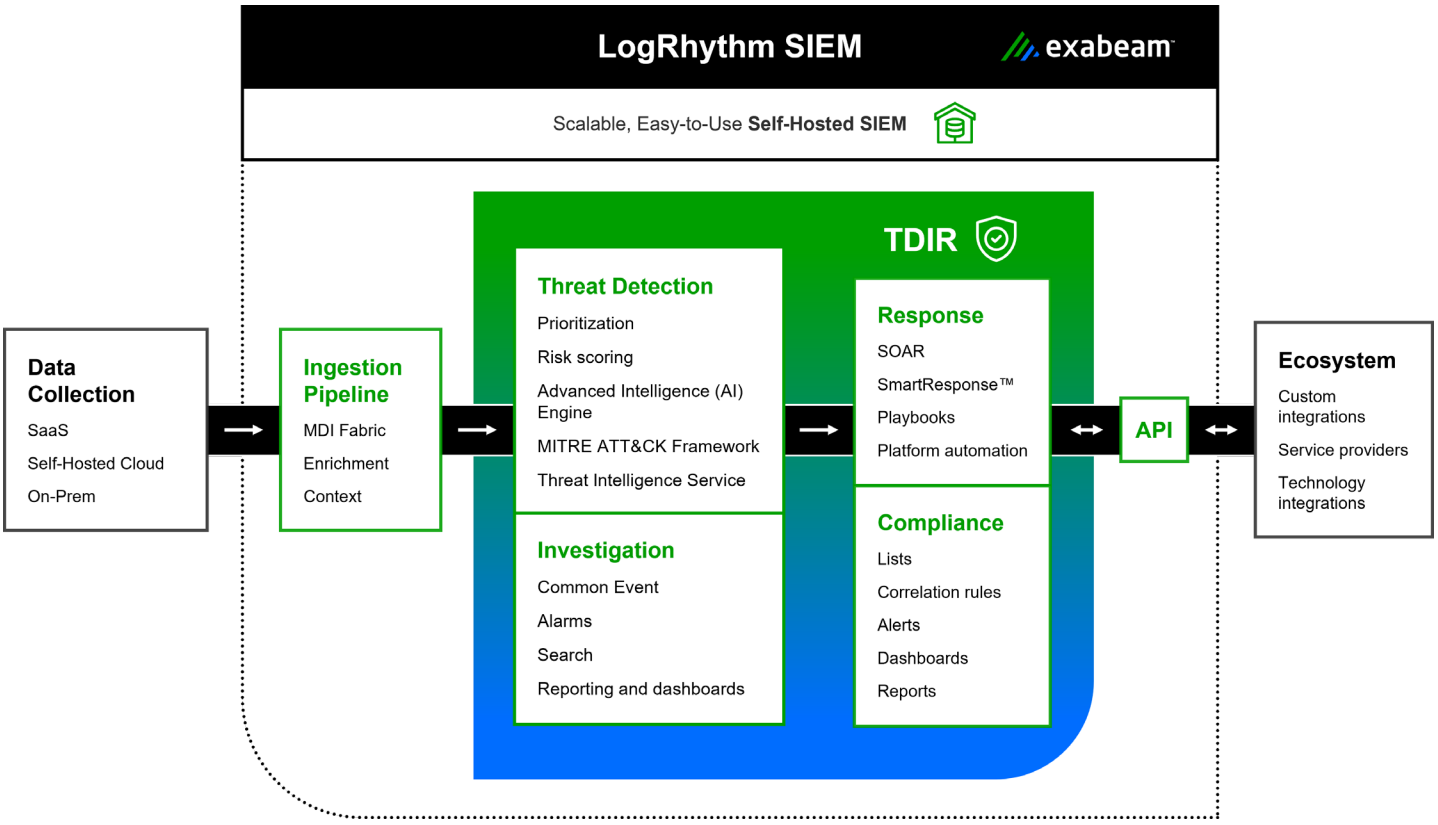


**Figure 1.** LogRhythm SIEM integrates data collection, analytics, compliance content, and automated response in a single self-hosted platform designed for full control and visibility.

## Features

### Flexible Self-Hosted Platform

Scale smoothly as your SOC grows, LogRhythm SIEM integrates with cloud services and on-prem applications, giving you deployment flexibility without sacrificing control.

### Open Collection Architecture

Collect logs immediately collect from more than 1,000 sources spanning SaaS, self-hosted cloud, and on-premises environments. Cloud collectors, lightweight agents, and customizable APIs and webhooks ensure you have visibility across large data volumes from day one.

### JSON Parsing Made Simple

The JSON Policy Builder lets you create parsing policies in just a few clicks. Guided workflows help you build new policies quickly, ensuring future JSON logs can be searched, visualized, and used for detections with minimal effort.

### Log Enrichment and Normalization

Patented MDI Fabric normalizes and enriches log data at ingestion. Metadata is automatically extracted and structured for search and analytics, improving accuracy across diverse log sources. Prebuilt processing rules eliminate manual tuning, helping analysts get to insight faster.

### Advanced Intelligence (AI) Engine

The AI Engine includes more than 1,100 prebuilt correlation rules, including rules mapped to the MITRE ATT&CK® framework and compliance modules. You can also build custom threat detections tailored to your environment, extending detection coverage to meet changing needs.

## Dashboards, Search, and Reporting Capabilities

Monitor activity with real-time dashboards and search across your entire log store. Save and schedule reports daily, monthly, or quarterly. Even without detailed knowledge of log formats, you can pivot across events and vendors to find what you need.

## Guided Workflows and Automatic Alerts

Consistent, intuitive workflows help analysts detect, investigate, and respond faster while reducing ramp time for new users. Risk-based alerts are generated automatically, highlighting suspicious activity with supporting evidence so your team can act immediately.

## Correlation Rules Testing

Fine-tune correlation rules for your environment. Built-in testing supports detection engineering, red team exercises, and penetration tests, all from within the LogRhythm SIEM interface.

## Automated Investigation and Response

Accelerate efficiency with embedded automation capabilities and integrations with more than 80 partner solutions. The AI Engine automatically generates cases from detections, centralizing investigations and ensuring the right incidents are prioritized. SmartResponse™ delivers automated or approval-based playbook actions to streamline repetitive tasks, while case management tracks progress and keeps your team focused on what requires immediate attention.

## Compliance Support

Meet audit and regulatory requirements faster with 28 prebuilt frameworks, including ISO 27001, PCI DDS, GDPR, NIST (800-53, 800-171, CSF), CMCC, and CIS. Each framework includes rules, dashboards, and reports mapped directly to individual controls, developed by in-house compliance experts.

## Knowledge Base

Access biweekly updates in the Knowledge Base with new modules that combine actionable intelligence and analytics to continuously strengthen your security posture.

## About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

**Learn more at www.exabeam.com →**