

Protecting Patient and Healthcare Provider Data with LogRhythm SIEM

Detect and Remediate Attacks with LogRhythm SIEM

As the proliferation of patient and provider data continues to grow, your organization faces the task of continuously protecting that information and keeping it secure. With a growing cyberattack landscape and new technologies that transfer, process, store, and interact with patient data, LogRhythm SIEM helps you stay on top of patient data safety while quickly navigating threats and intrusions across endpoints.

By leveraging a security information and event management (SIEM) solution, customers have the visibility and tools to quickly detect threats and keep patient and provider data, biomedical devices, and healthcare systems secure.

Monitoring the Network — Not Just Data

NetMon provides real-time visibility to monitor your organization's entire network. Rich data and deep insights delivered by NetMon help organizations detect and respond to advanced threats, including nation-state espionage, zero-day malware, and data exfiltration.

Simplify and Demonstrate Health Insurance Portability and Accountability Act Compliance

LogRhythm SIEM helps healthcare organizations address their security concerns. Healthcare security teams rely on LogRhythm SIEM solutions to:

- Improve detection, mitigation and response capabilities with LogRhythm SIEM that includes user and entity behavior analytics (UEBA) and network analysis.
- Maximize patient data protection by integrating with electronic health record systems such as Epic, eClinicalWorks, Cerner, and AllScripts
- Demonstrate Health Insurance Portability and Accountability Act (HIPAA) and Health Information Trust Alliance (HITRUST) compliance with fact-based evidence easily accessed and exported for audit reports
- Reduce time and the cost of compliance with prepackaged content
- Obtain real-time visibility into events with preconfigured alarms, reports, rules, and dashboards
- Bridge technology including IT, IS, and OT that support the healthcare business with systems and infrastructure that enable the industry

LogRhythm SIEM Features and Benefits for Healthcare

Smart Security

- Flag weaknesses in authorizations that could put hospital and laboratory management systems and patient data at risk.
- Save time and effort in complying with HIPAA and HITECH using the Health Care Compliance Automation Module.
- Detect malicious activity and meet compliance regulations using the LogRhythm's prebuilt security analytics content and visualizations.
- Discover and identify devices on the network to help determine normal states for different device types and manufacturers with LogRhythm SIEM's integration with MedScan and Ordr.
- Protect data on disconnected devices with passive network monitoring.
- Identify suspicious activity with EHR system alerts and alarms.
- Use customizable and flexible dashboard visualizations to fit IT environment and policies.

Automation to Reduce SOC Team Effort

- Streamline workflows to help security teams combat evolving threats using SOAR features, including case management, case metrics, playbooks, and contextualization.
- Gain real-time visibility to understand what's occurring in your environment.
- Reduce manual security tasks and platform switching.
- Enrich data with contextual details and translate obscure log syntaxes to a consistent and predictable structure.
- Eliminate time spent writing scripts, building rules, and creating reports with automation.
- Manage specific threats and reduce time to detect and respond to threats with repeatable processes and guides.
- Document evidence of compliance with predefined reports.

Threat Intelligence

- Comprehend "normal" in IT and operational technology (OT) to help detect behavioral anomalies that might indicate an attack in progress.
- Access a library of prebuilt compliance, threat, and operational risk-based content.
- Obtain continuously updated data processing content and threat scenarios.
- Identify malicious activity, detect advanced threats, and protect systems from application vulnerabilities.

Integrations

- Accelerate medical device and system data monitoring with seamless integrations with top providers:
- Medical device integrations: Ordra and MedScan
- Healthcare software system integrations: AllScripts, Cerner, eClinical Works, and Epic
- Simplify deployment and maintenance with fully tested and certified prebuilt integrations.
- Aggregate information from physical, virtual, and cloud sources using a flexible data collection.
- Protect EHR with real-time visibility.
- Integrate with existing EHR software, and map prebuilt Analytics Engine rules and alerts to HIPAA and HITECH controls.

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.



Learn more at
www.exabeam.com →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.

2024 Exabeam, LLC. All rights reserved.