Partner Data Sheet

LogRhythm

Industry

SIEM

Website

www.logrhythm.com

Company Overview

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats.

Product Overview

LogRhythm delivers solutions for next-generation SIEM, log management, endpoint/ network monitoring and forensics, security analytics, and threat lifecycle management in a unified Security Intelligence Platform.

Solution Highlights

LogRhythm's patented machine analytics technology continually performs real-time analysis on machine data collected from across the customer environment, enabling security analysts to identify, investigate and respond to previously unknown threats.

ANOMALI™

LogRhythm and Anomali's ThreatStream Product: Integrated Security and Threat Intelligence Solutions

The threat landscape is continually expanding and organizations are under continuous attack and overwhelmed with alerts. Thousands of incidents occur each day and security professionals only have time to deal with dozens. This creates operational chaos. Security teams need next-generation security solutions to help them respond faster, defend proactively and invest smarter.

LogRhythm for Integrated Enterprise Security Intelligence

- Real-time event contextualization across multiple dimensions
- Improved risk-based prioritization
- Forensic visibility into malware attack vectors and patterns
- Tight integration for consolidated threat management

Just-in-Time Intelligence

Threat intelligence is continuously gathered, categorized and ranked (for severity and confidence) in Anomali's ThreatStream platform and then delivered in real-time to your LogRhythm instance for detection of security threats in your enterprise infrastructure. This enables your security and threat intelligence teams to quickly see high priority threats to your business. Each of the selected IOCs for integration into your LogRhythm instance is enriched with factors such as risk score to add context and relevance to the delivered information

Benefits of the Joint Offering

LogRhythm and Anomali have developed an integrated solution for comprehensive security intelligence and threat management. LogRhythm automatically integrates actionable intelligence from the ThreatStream Platform with other machine data collected throughout the enterprise for comprehensive, real-time threat visibility and next generation security analytics.

By leveraging ThreatStream with LogRhythm's Security Intelligence Platform, customers benefit from increased threat intelligence and accurate risk management. The combined solution delivers the ability to rapidly detect, validate, and streamline incident response time to cyber-attacks.

Benefits of Anomali

- Easy-to-use interface to view threat information received through STIX/TAXII feeds.
- Analyze and correlate data into actionable information: SIEM rules, reports, and dashboards.
- Pinpoint IOCs - quickly search for a specific indicator, search for an indicator type over a time range, and drill-down into details.
- Eliminate unnecessary, duplicative and irrelevant indicators - before they enter your infrastructure.
- Identify and prioritize the events that matter now - without DIY scripting.
- Machine-to-Machine learning algorithms scale to accommodate thousands of IOCs per minute across your environment.

Benefits of LogRhythm

- Next Generation SIEM and Log Management.
- Endpoint forensics, with registry and file integrity monitoring.
- Network Forensics with Application ID and Full Packet Capture.
- Behavioral analytics for holistic threat detection (users, networks and endpoints).
- Rapid unstructured and contextual search.
- End-to-end incident response orchestration workflows to support team collaboration.
- SmartResponse™ automation framework.
- Integrated Case Management.

Analytics

Anomali threat intelligence can be easily configured within LogRhythm allowing threat data to be correlated with other activity in the user environment. When communication with an identified bad actor is detected, an alarm is triggered within LogRhythm's console, allowing organizations to rapidly detect, validate, and streamline incident response time to cyber-attacks.

Seamless Integration

The Anomali Link connection with LogRhythm provide seamless, automatic integration of indicator data to deliver real-time threat intelligence to your LogRhythm deployment. With the ThreatStream platform you are ready to start using IOCs in meaningful ways more efficiently and more effectively than ever before.

About Anomali

Anomali® is the pioneer of an enterprise class threat intelligence platform, combining comprehensive threat data collection, prioritization, and analytics with secure collaboration in a vetted community. Offering the broadest enterprise security infrastructure integration available, the ThreatStream platform enables organizations to proactively identify and combat cyber threats targeting their operations. www.anomali.com

About LogRhythm

LogRhythm empowers organizations to detect, respond to and neutralize cyber threats early in the threat lifecycle to prevent damaging data breaches and cyber incidents. LogRhythm solutions also deliver rapid compliance automation and assurance, and enhanced IT intelligence.

LogRhythm's award-winning Security Intelligence Platform integrates next-gen SIEM and log management with network forensics, endpoint monitoring and multidimensional security analytics. Its collaborative incident response orchestration and patented SmartResponse automation framework help security teams perform end-to-end threat lifecycle management. LogRhythm's unified solution powers the next-gen SOC, accelerating the detection and response to emergent threats across the holistic attack surface.

For more information contact Anomali sales at info@anomali.com or LogRhythm sales at info@logrhythm.com.

ANOMALI™

2317 Broadway, 3rd Floor, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com