PRODUCT OVERVIEW

LogRhythm Threat Intelligence Ecosystem

LogRhythm
The Security Intelligence Company

LogRhythm's Threat Intelligence Ecosystem for detecting high-risk cyber threats

LogRhythm's Threat Intelligence Ecosystem is the industry's first collective of threat intelligence partners and open source providers focused on delivering security intelligence via a next-generation Security Intelligence Platform. By integrating the massive amount of threat data provided by ecosystem partners and open source providers with the machine data collected from throughout the enterprise, LogRhythm generates highly contextualized security intelligence, enabling quick and accurate threat detection and response.

Detecting and responding to today's increasingly sophisticated cyber threats requires:

- Pervasive, enterprise-wide visibility
- Advanced machine analytics
- Rich external context in the form of relevant, accurate and actionable threat intelligence.

The LogRhythm Threat Intelligence Ecosystem allows customers to seamlessly incorporate threat context into their LogRhythm implementations from industry-leading commercial and open source providers of threat intelligence, enabling faster detection of and response to:

- Dangerous IPs accessing internal infrastructure
- Users visiting risky URLs
- Phishing attempts
- Malware propagation
- Other high impact activities

LogRhythm's Threat Intelligence Ecosystem enables its award-winning Security Intelligence Platform to consume and leverage threat intelligence from commercial and open source providers. This threat intelligence includes data such as low reputation IP addresses and URLs, nefarious email addresses, file names, processes and user agent strings. Customers can easily select which feeds to integrate from within the Threat Intelligence Service Manager. This includes any feed that belongs to the Threat Intelligence Ecosystem, including open source feeds and commercial feeds that require their own subscriptions. Information from threat intelligence feeds can be used to more accurately detect a broad range of malicious behavior, including dangerous IPs accessing internal infrastructure, inappropriate URL usage, phishing attempts, malware propagation, and other highly suspicious activities.

LogRhythm Labs maintains a Threat Intelligence Security Analytics Module which ensures that threat data unique to each ecosystem partner and open source provider is accurately captured and recognized by LogRhythm's platform, allowing customers to leverage intelligence from one or multiple vendors. Customers benefit from LogRhythm's ability to collect and process all of an organization's log, flow, event and other machine data, as well as endpoint, server and network forensic data, to not only identify activities associated with threat intel, but automatically prioritize incidents corroborated with other high risk events recognized across the IT environment. This pervasive visibility, combined with the rich context provided by Threat Intelligence Ecosystem partners, enables LogRhythm's Security Intelligence Platform to deliver even faster detection of and response to cyber threats, driving down false positives and reducing mean time to remediation.

LogRhythm provides an integrated solution for each partner, offering:

- Quick setup and consumption of partner threat feeds
- Capture of live threat activity
- Corroboration of threat intel with other enterprise sources for rapid and precise event recognition and prioritization

Examples of threat data provided by Ecosystem partners:

Known Attacks	Botnets	Associated with Fraud	Associated with Malware	Used for Phishing	Suspicious
• IP Addresses • URLS • User Agents	• IP Addresses • URLS	• IP Addresses • URLS	• IP Addresses • URLS • User Agents • Processes • File Paths • File Names	• IP Addresses • URLS • Email Addresses • Email Subjects	• IP Addresses • URLS

Data is automatically propagated to Lists within LogRhythm based on the threat feeds enabled within the platform. Vendor-specific lists are nested in common lists, allowing saved searches, reports, and analytical rules from AI Engine to easily leverage content provided by one or multiple providers.

LogRhythm has created a tightly integrated Threat Intelligence Ecosystem, combining the value of partners' actionable threat intelligence with LogRhythm's award winning Security Intelligence Platform. The integrated offering empowers customers to identify malicious activity, detect advanced threats, protect systems from application vulnerabilities and prioritize responses based on accurate, highly contextualized security intelligence.

Prioritized Threat Intelligence

Challenge The volume of malicious activity on the Internet and the speed with which it propagates makes it difficult for information security professionals to know which events pose the greatest risk to their organizations.

Solution LogRhythm's ecosystem partners provide rich, external context regarding IP addresses, URLs, and other data points associated with known threats. LogRhythm automatically populates its common lists with this threat data to facilitate rapid identification of threats and attack types, including known attacks, botnets, fraud, malware, phishing and suspicious. LogRhythm not only instantly recognizes when there are activities linked to threats, but can leverage this data using advanced behavioral analytics to better corroborate threats and events and limit false positives.

Additional Benefit Smart**Response**™ Plug-ins are designed to actively defend against attacks by initiating actions that offset the threat, like automatically adding an attacking IP to a firewall ACL. This advanced countermeasure immediately stops all activity to and from adversary groups to immediately halt an attack.

Preventing Data Breaches

Challenge Many organizations struggle with a lack of visibility into the activity of internal users. This makes it difficult to protect the network from outbound threats, such as communication from internal resources to an external adversary group, command-and-control server or anonymous proxy network such as TOR. Administrators need to differentiate legitimate employee activity from suspicious employee activity and identify the threat level posed by the latter.

Solution LogRhythm separates threat data based on vendor categories and severity scores, providing additional context to better recognize the nature and priority of observed events. Domains and URLs identified as malicious by threat intelligence vendors can be added to a blacklist within LogRhythm to identify and prioritize dangerous outbound or inbound communication.

Additional Benefit LogRhythm's Network Monitor can automatically initiate a targeted packet capture of all outbound data being sent to a malicious domain or URL for in-depth forensic analysis and potential law enforcement purposes.

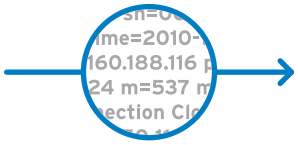
Commercial and Open Source Threat Intelligence Providers

ANOMALI™
CROWDSTRIKE
Symantec.
ThreatGRID
WEBROOT

Abuse.ch
AutoShun
HailATaxii
Malware Domains
Phish Tank
SANS-ISC
SpamHaus
STIX/TAXII
TOR Network

Other Log, Security, and Machine Data

LogRhythm Forensic Sensor Data



Threat Intelligence

Automatically consume and leverage threaet intelligence

SmartResponse™

Automatically take action and respond to events and alarms

LogRhythm

Security Intelligence Platform

- Next Generation Security Operations Center
- Security Analytics
- SIEM & Log Management
- Network Monitoring and Forensics
- Endpoint Monitoring and Forensics
- Behavioral Analytics (e.g. UBA, NBAD, EDR)

LogRhythm Labs