LogRhythm and Recorded Future

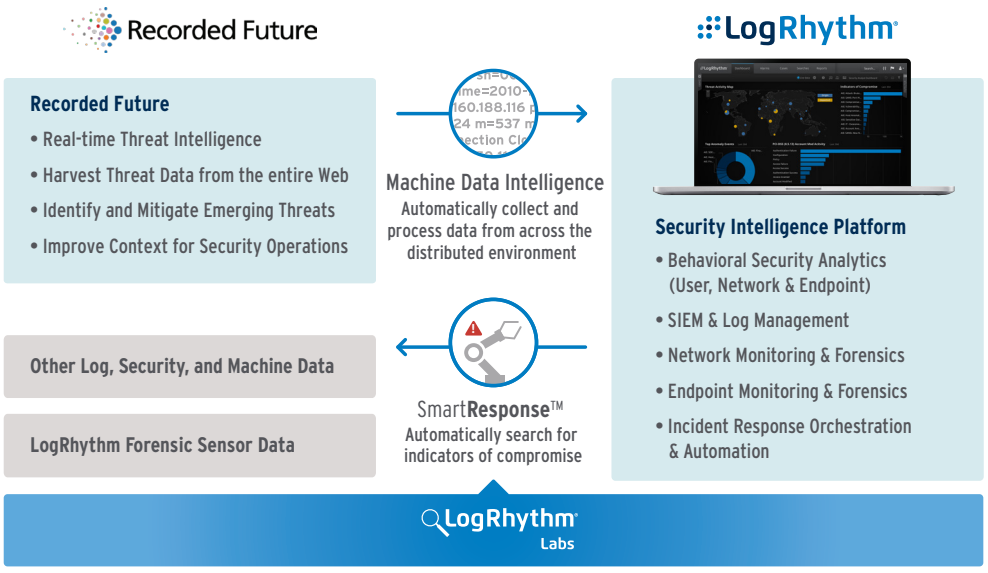
Combining actionable threat content with advanced behavioral analytics for enterprise security intelligence

LogRhythm has developed a solution which integrates Recorded Future's real-time threat intelligence into LogRhythm's Security Intelligence Platform. LogRhythm automatically correlates petabytes of machine data collected from across the extended enterprise with actionable intelligence that Recorded Future has analyzed from the entire web to provide comprehensive, real-time threat visibility and next-generation security analytics.

The integration allows customers to:

- Continually import IP Reputation threat content from Recorded Future into LogRhythm for immediate recognition of user, host and network behavior involving malicious sources, emerging threats and indicators of compromise.
- Provide deep forensic visibility into activity to and from threatening IPs, URLs, and domains that have been identified and validated by Recorded Future's Web Intelligence Engine.
- Automate the correlation of network activity involving bad actors with other activity and behavioral changes to hosts and users for more accurate prioritization of high risk events.
- Accelerate response to threats identified using Recorded Future by leveraging LogRhythm SmartResponse to orchestrate and automate remediation.

By leveraging Recorded Future's real-time threat intelligence with LogRhythm's Security Intelligence Platform, customers benefit from actionable insights and accurate risk management. The combined solution delivers the ability to rapidly detect, validate, and prioritize security events, resulting in streamlined and accelerated incident response.



About LogRhythm

- Empowers organizations to rapidly detect, respond to and neutralize cyber-threats
- Delivers rapid compliance automation and assurance, and enhanced IT intelligence
- Provides a holistic platform for end-to-end Threat Lifecycle Management, uniquely unifying next-gen SIEM, log management, network & endpoint forensics, advanced behavioral analytics & machine learning, and incident response orchestration & automation
- Delivers unparalleled compliance automation & assurance, and deep IT operational intelligence
- Consistently recognized market leadership, including being a Leader in Gartner's SIEM Magic Quadrant since 2012

Recorded Future

About Recorded Future

- Empowers customers with real-time threat intelligence, to defend against threats at the speed and scale of the Internet
- Web Intelligence Engine continuously analyzes the entire web to deliver unmatched insight into emerging threats
- Helps protect four of the top five companies in the world, and over 12,000 IT security professionals use Recorded Future every day

LogRhythm and Recorded Future are tightly integrated, combining the value of Recorded Future's actionable threat intelligence with LogRhythm's award winning Security Intelligence Platform. The combined offering empowers customers to quickly and accurately identify malicious activity, detect advanced threats, protect systems from application vulnerabilities and prioritize response activities.

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

Use Case: Optimizing Threat Intelligence

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

Solution:
Recorded Future's Web Intelligence Engine delivers real-time, actionable threat intelligence analyzed from the open, deep, and dark Web including TOR sites, IRC channels, forums, paste sites, social media and threat feeds. LogRhythm combines this data with advanced behavioral analytics to identify security events with minimal false positives and enhanced prioritization.

Additional Benefit:
LogRhythm Smart**Response**™ plugins are designed to actively defend against attacks by initiating actions in response to threats, such as automatically adding an attacking IP to a firewall ACL. This immediately stops all activity, such as botnet command and control communication. Additionally, Recorded Future Browser plugins make it easy to browse Recorded Future's intel summary pages on the following indicator types: IP address, file hashes, and domains.

Use Case: Detecting Zero-Day Attacks

Challenge:
Zero-day exploits are designed to evade detection by traditional IDS/IPS solutions, and once an intrusion gets through, organizations are unable to detect malicious behavior. Detecting these attacks requires extensive visibility and analysis of multiple attack vectors with a focus on identifying behavior patterns tied to malicious activity.

Solution:
Recorded Future analyzes the open, deep, and dark web to identify indicators related to zero-day attacks such as IP addresses. LogRhythm's advanced machine analytics engine performs statistical and behavioral modeling using data provided by Recorded Future to detect and alert analysts to the first signs of compromise within their organizations. This helps reduce response times and minimize the impact of a successful Zero Day attack.

Additional Benefit:
If a Zero Day attack has successfully compromised a host, a LogRhythm SmartResponse plugin can be initiated to automatically lock down the impacted endpoint to isolate the attack and prevent further harm.