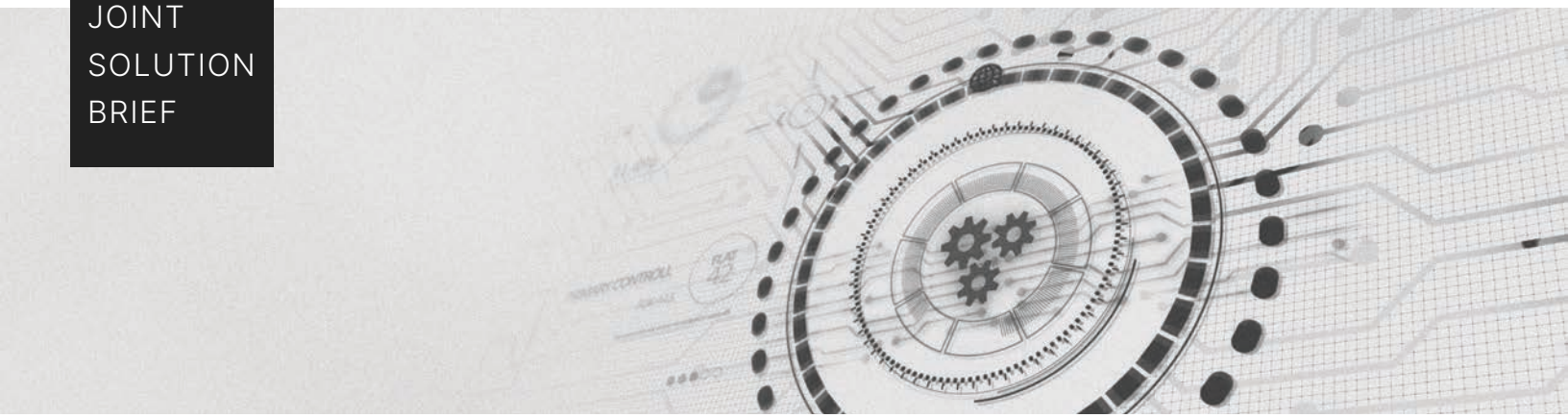
Recorded Future®

JOINT SOLUTION BRIEF



LogRhythm and Recorded Future

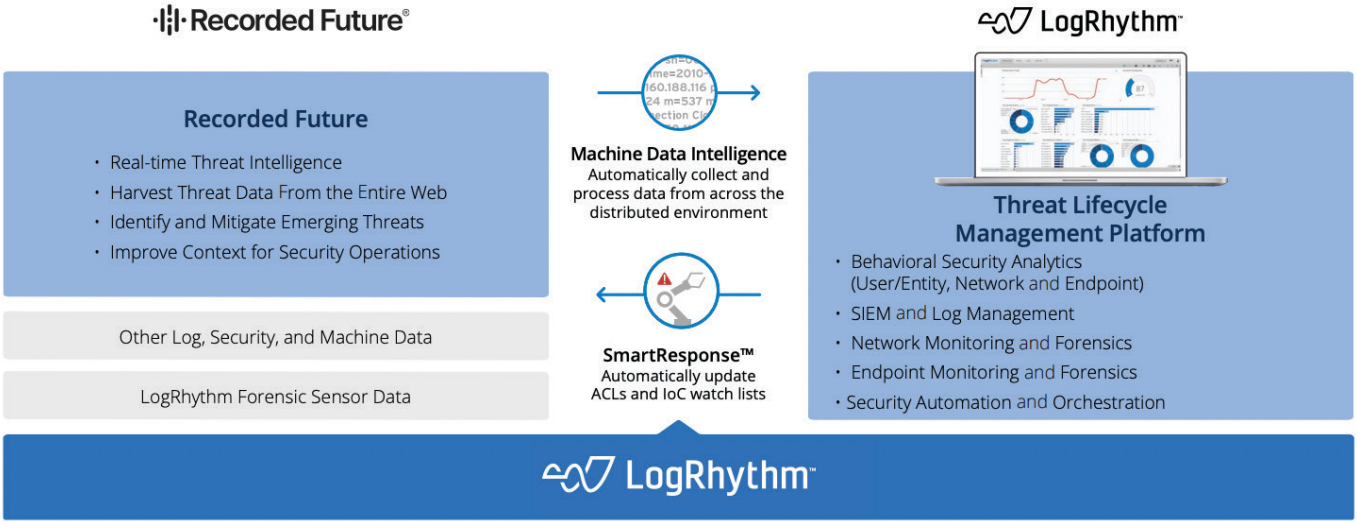
Combining Actionable Threat Content with Advanced Behavioral Analytics for Enterprise Security Intelligence

LogRhythm™

LogRhythm automatically integrates Recorded Future's real-time threat intelligence into LogRhythm's Threat Lifecycle Management Platform. LogRhythm automatically correlates machine data collected from across the extended enterprise with actionable intelligence that Recorded Future has analyzed from the entire web. The combined solution provides comprehensive, real-time threat detection.

The Integration Allows Customers To:

- Continually import IP reputation threat content from Recorded Future into LogRhythm for immediate recognition of user/entity, network and endpoint 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 by Recorded Future by using LogRhythm SmartResponse™ to automate remediation. By leveraging Recorded Future's real-time threat intelligence with LogRhythm's Threat Lifecycle Management Platform, customers benefit from actionable insights and accurate risk management. The combined solution provides the ability to rapidly detect, validate, and prioritize security events, accelerating incident response.



LogRhythm and Recorded Future are tightly integrated, combining the value of Recorded Future's actionable threat intelligence with LogRhythm's award-winning Threat Lifecycle Management 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 Unified Threat Lifecycle Management

- 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 spreads 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 SmartResponse 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 indicators such as IP addresses, file hashes, and domains.

Use Case: Detecting Zero-Day Attacks

Challenge: Zero-day exploits are designed to evade detection by traditional perimeter-based technologies, and when it gets through, organizations must detect and respond before it does damage. 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 machine analytics perform statistical and behavioral modeling using data provided by Recorded Future to detect and alert analysts on 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.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries. Learn more at recordedfuture.com.

ABOUT LOGRHYTHM

LogRhythm is the world leader in NextGen SIEM, empowering organizations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm platform combines user and entity behavior analytics (UEBA), network traffic and behavior analytics (NTBA) and Security Orchestration, Automation, and Response (SOAR) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations center (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant. For more information, visit logrhythm.com