Recorded Future

Combining LogRhythm's Threat Intelligence Service for enterprise security with Recorded Future's actionable threat intelligence

Benefits

- Obtain real-time contextualization across multiple dimensions
- Leverage improved risk-based prioritization
- Gain forensic visibility into malware attack vectors and patterns
- Consolidate threat management via a tight integration

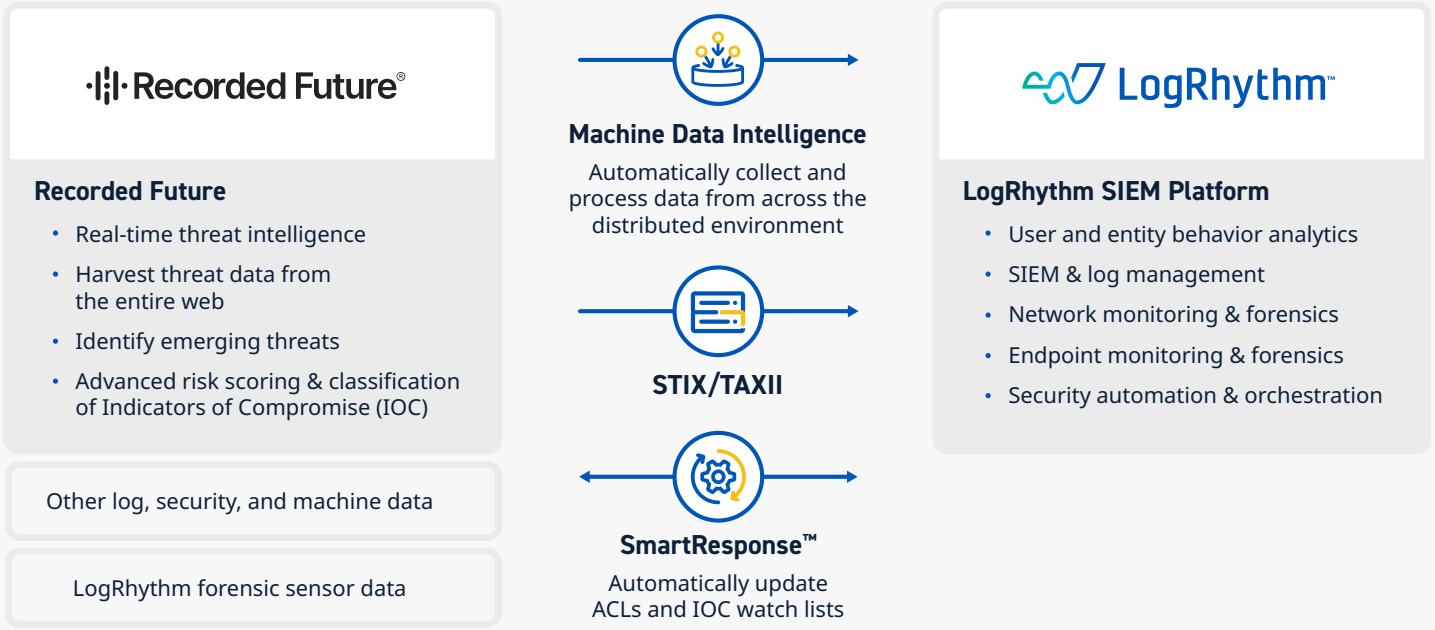
Solution overview

The LogRhythm SIEM Platform integrates Recorded Future's real-time threat intelligence into LogRhythm's Threat Intelligence Service (TIS) by automatically correlating machine data collected from the extended enterprise with actionable intelligence that Recorded Future analyzed from the web. The combined solution provides comprehensive, real-time threat detection.

By leveraging Recorded Future's instantaneous threat intelligence with LogRhythm's TIS, 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.

About LogRhythm and Recorded Future

LogRhythm and Recorded Future work together to help organizations around the globe increase network visibility and protect against modern cyberattacks. LogRhythm offers extensive support for and integration across Recorded Future's product portfolio. The combined solution empowers security teams to identify behavioral anomalies, internal, and external threats, and to prioritize their responses based on accurate enterprise security intelligence. LogRhythm and Recorded Future empower security teams to navigate a changing threat landscape with confidence. Together, LogRhythm and Recorded Future are ready to defend.



Cyberthreat intelligence collection

LogRhythm's TIS is a service that allows threat data feeds from third parties, such as Recorded Future, to be easily integrated into any LogRhythm deployment. TIS integrates with various open-source providers and supports custom Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) providers. When TIS is combined with LogRhythm's Threat Intelligence Module, data collected by Recorded Future is ingested and analyzed. Alerts ingested by LogRhythm become actionable, reducing detection and response times by alerting customers to threats in their environment.

How it works

Recorded Future Threat Intelligence is collected by scraping every recess of the internet to include the deep and dark webs. Recorded Future accomplishes this task by using a multitude of technical sources, applying advanced natural language processing, and ontology analysis. This provides context around IP addresses, domains, URLs, hashes, threat actors, and vulnerabilities.

Customers can configure alerts specific to their needs, providing real-time alerting, which is then ingested by LogRhythm's TIS. Based on the customer's configuration, risk lists are generated that include malicious indicators, such as IP addresses, domains, URLs, and hashes, which are used for correlation via AI Engine rules. These risk lists of malicious indicators can drastically improve detection in the LogRhythm SIEM Platform. With the Recorded Future browser plugin, LogRhythm users can enrich indicators anywhere in the platform and obtain valuable context around them.

How automated workflows work

IP reputation threat content is continually imported from Recorded Future into the LogRhythm SIEM for immediate recognition of user/entity, network, and endpoint behavior involving malicious sources, emerging threats, and indicators of compromise. This provides 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.

The correlation of network activity involving bad actors with other activity and behavioral changes to hosts and users is automated for more accurate prioritization of high-risk events. This allows for accelerated responses to threats identified by Recorded Future via LogRhythm's SmartResponse™ to automate remediation. SmartResponse is part of LogRhythm's security orchestration, automation, and response (SOAR) solution that can execute if an alarm rule triggers.

SmartResponse automated actions for Recorded Future

Action	Description	Use Case
Create Configuration File	Execute this action and rerun it before using the SmartResponse's other available actions when changes are made to the fixed-value parameter	This functionality must run first before other SmartResponse functions can execute
GetAlertById	Displays information regarding previously configured alerts	Retrieves a triggered Recorded Future alert by ID; information is provided via Recorded Future Alert API
GetDomainLookup	Displays domain information associated with configured alerts	Retrieves Recorded Future threat intelligence data on a given domain; not necessarily associated with a Recorded Future alerts
GetEntityLists	Displays list of entities associated with configured alerts	Retrieves user-configured Recorded Future Entity Lists; lists can be retrieved using optional free text keywords to match; not necessarily associated with Recorded Future alerts
GetHashLookup	Displays retrieved Recorded Future threat intel data on a given hash value associated with configured alerts	File Integrity Monitor (FIM) will alert when a new file was added to a monitored folder; SmartResponse is then triggered to validate hash value; information is provided via the Recorded Future Connect API
GetIpLookup	Displays IP address associated with configured alerts	Retrieves Recorded Future threat intelligence data on a given IPv4 address; information is provided via the Recorded Future Connect API
GetUrlLookup	Displays URL details associated with configured alerts	Retrieves Recorded Future threat intelligence data on a given; information is provided via the Recorded Future Connect API
GetAlertRules	Displays alert rules associated with configured alerts	Retrieves user-configured Recorded Future Alert Rules, optionally matching against free text keywords; information is provided via the Recorded Future Alert API