LogRhythm and Cisco Threat Grid for Integrated Enterprise Security

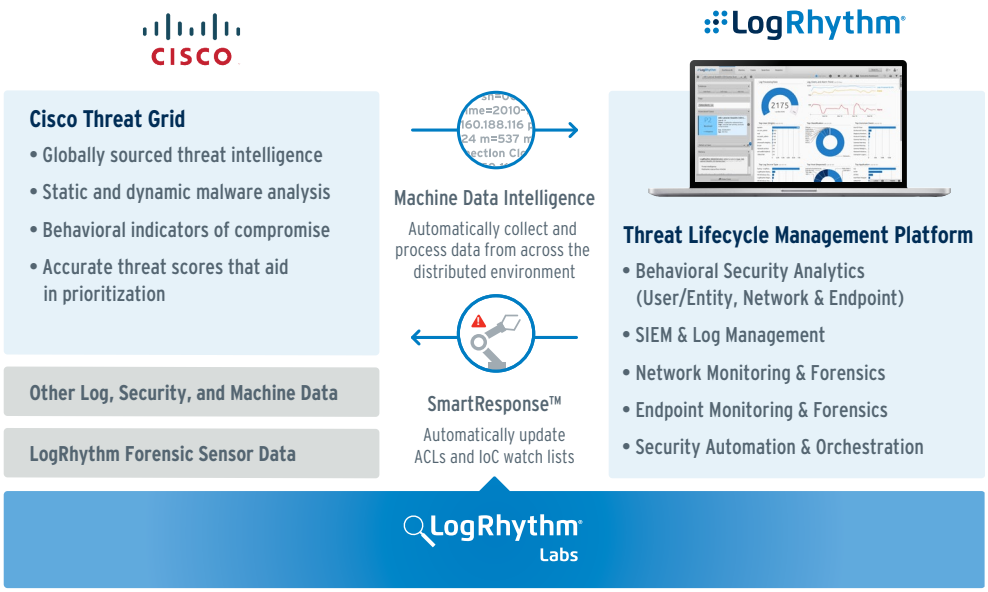
LogRhythm and Cisco have partnered to deliver mutual customers enterprise-wide threat detection and response by integrating Cisco's Threat Grid threat intelligence into LogRhythm's Threat Lifecycle Management Platform and automating the discovery of indicators of compromise relative to malware that has penetrated the network.

LogRhythm's platform continually consumes malware analysis and threat intelligence data provided by Threat Grid with other machine data collected from across the environment to accurately identify and prioritize high risk events. LogRhythm has developed a SmartResponse™ plugin that allows analysts to automatically submit potential indicators of comprise such as domain names, IP addresses, hashes, and file names detected within the LogRhythm platform to Threat Grid for analysis and threat scoring. Results from Threat Grid are quickly and seamlessly returned to the LogRhythm console to facilitate immediate protective action.

The integration allows mutual customers to:

- Streamline processes that were once significantly manual and turn them into an automated workflow to reduce detection and response times
- Correlate known threats with changes to the behavior of endpoints, users and networks to quickly alert on and take immediate action on high risk events
- Mature from logging and alerting to taking dynamic active defense actions

With the combined power of LogRhythm and Cisco, mutual customers can effectively capture and send potential indicators of compromise observed within their environment for additional context or enrichment by querying Cisco Threat Grid's expansive threat intelligence repository. Once examined, the indicators of compromise may be extracted and resubmitted to LogRhythm to help improve an organization's overall security posture.



About LogRhythm

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

About Cisco Threat Grid

- Cisco Threat Grid combines static and dynamic malware analysis with threat intelligence into one unified solution.
- It provides in-depth information customers need to protect their business from malware of all types.
- It integrates behavioral analysis and up-to-the-minute threat intelligence feeds with existing security technologies, protecting customers from both known and unknown attacks.
- Threat Grid's detailed reports, including the identification of important behavioral indicators and the assignment of threat scores, lets users quickly prioritize and recover from advanced attacks.

LogRhythm and Cisco Threat Grid are tightly integrated, bridging the value of Threat Grid's dynamic malware analysis and threat intelligence with the advanced analytics and incident response capabilities of LogRhythm's Threat Lifecycle Management Platform. The combined offering empowers customers to accurately identify malicious activity, detect advanced threats, mitigate attacks, and prioritize response based on accurate, highly contextualized security intelligence.

LogRhythm for Integrated Enterprise Security Intelligence

- Dynamic defense for detecting and stopping unauthorized network threats
- Multi-dimensional behavioral analytics to deliver real-time security intelligence
- Deep visibility into all aspects of user, network and endpoint behavior activity throughout the IT environment
- Tight integration for consolidated threat management

Use Case: Operationalizing Threat Intelligence

Challenge:
The volume of malicious activity and the speed at which it can propagate make it difficult for information security professionals to know which events pose the greatest risk to their organizations.

Solution:
Threat Grid dynamically analyzes key behavioral indicators and malware artifacts to provide a view of malware. LogRhythm consumes this intelligence in real time, performing advanced behavioral analysis to recognize when network activity with known bad actors is observed within the customer environment. This visibility enables administrators to quickly discover and qualify threats that represent real risk in their environment.

Additional Benefit:
LogRhythm SmartResponse plug-ins are designed to actively defend against attacks by initiating actions that offset the threat, such as automatically adding the attacking IPs to a firewall policy. This immediately stops all activity such as botnet command and control communication.

Use Case: Detecting Zero-Day Malware

Challenge:
Targeted attacks are designed to evade detection by traditional perimeter solutions. Once an intrusion gets through, organizations struggle to detect malicious activity and corroborate the presence of malware, which delays response times and increases risk to the organization.

Solution:
To help organizations proactively detect unknown malware in their environments, LogRhythm and Cisco Threat Grid have developed an integrated approach that combines extensive visibility and analysis of multiple attack vectors with globally sourced malware activity and analysis to detect malware. When LogRhythm's advanced analytics and behavioral profiling expose malicious activity, a SmartResponse alert can automatically send attack-related artifacts to Cisco Threat Grid for analysis against other known malicious samples. Results and a prioritized threat score are immediately returned to the LogRhythm console

Additional Benefit:
Analysts can quickly launch a forensic investigation into the results from the malware analysis to determine if malware resides in other parts of the network.