PRODUCT OVERVIEW

LogRhythm and Symantec: Integrated Security and Threat Intelligence

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

LogRhythm has developed a solution which integrates Symantec's DeepSight Threat Intelligence into LogRhythm's Security Intelligence Platform. LogRhythm automatically correlates actionable intelligence from Symantec's DeepSight™ Intelligence DataFeeds with other machine data collected throughout the enterprise for comprehensive, real-time threat visibility and next generation security analytics.

The integration allows customers to:

- Continually import IP Reputation threat data from Symantec DeepSight™ Intelligence DataFeeds into LogRhythm for immediate recognition of user, host, and network behavior involving malicious activity sources, emerging threats and indicators of compromise.
- Provide drill-down and deep forensic visibility into activity to and from threatening IPS, URLs and Domains that have been identified and validated by over 41.5 million attack sensors around the world.
- Automate the corroboration of network activity to or from bad actors with other behavioral changes to hosts and users for more accurate prioritization of high risk events
- Automate the remediation of attacks from bad actors by blocking communication with compromised domains to prevent data theft, block malware and terminate APT communication with a command and control infrastructure.

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

By leveraging Symantec's DeepSight Intelligence with LogRhythm's Security Intelligence Platform, customers benefit from increased threat intelligence and accurate risk management. The combined solution delivers the ability to rapidly detect, validate, and streamline incident response time to cyber-attacks.

LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's award-winning Security Intelligence Platform unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence. LogRhythm delivers:

- Next Generation SIEM and Log Management
- Independent Host Forensics and File Integrity Monitoring
- Network Forensics with Application ID and Full Packet Capture
- State-of-the art Machine Analytics
- Advanced Correlation and Pattern Recognition
- Multi-dimensional User / Host / Network Behavior Anomaly Detection
- Rapid, Intelligent Search
- Large data set analysis via visual analytics, pivot, and drill down
- Workflow enabled automatic response via LogRhythm's Smart**Response**™
- Integrated Case Management

Symantec

Symantec DeepSight™ Intelligence provides actionable data about malicious activity sources, emerging threats, and vulnerabilities. This intelligence can reduce exposure to threats through automated integration with existing security solutions. This integration into existing processes and tools allows businesses to act appropriately and quickly, preventing security incidents before they happen.

DeepSight Intelligence DataFeeds are derived from deep, proprietary analysis of billions of events from the Symantec™ Global Intelligence Network. The Global Intelligence Network provides global visibility into the threat landscape, including:

- More than 41.5 million attack sensors in 157 countries producing 660 billion log lines per month
- 60,000 products from more than 19,000 vendors
- More than 8 billion emails per month
- Over 13 billion web requests a day

LogRhythm and Symantec are tightly integrated, combining the value of actionable threat intelligence with LogRhythm's award winning Security Intelligence Platform. The combined 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.

Optimizing 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 Symantec's DeepSight Intelligence IP Reputation DataFeed delivers up-to-date, actionable intelligence with important context, including the type of activity (attacks, malware distribution, bot activity, etc.), a hostility and confidence rating based on proprietary algorithms that weigh activity types, consecutive appearances in the sensor network, and other factors for accuracy. LogRhythm combines this data with advanced behavioral analytics for real-time threat intelligence with minimal false positives.

Additional Benefit Smart**Response**™ 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 ACL. This immediately stops all activity such as botnet command and control communication.

Preventing Data Breaches

Challenge Many organizations struggle with a lack of visibility into activity from their internal users. This makes it difficult to protect the network from outbound threats, such as communication with compromised domains and URLs.

Solution The Symantec DeepSight Intelligence Domain and URL Reputation DataSheet provides detailed threat data with a focus on domains and URLs, allowing organizations to better define security policies for outbound communication. LogRhythm leverages this data for highly accurate threat detection related to outbound activity.

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 deep understanding of what data is being targeted by an attacker.