PRODUCT OVERVIEW

LogRhythm and ThreatStream: Integrated Security and Threat Intelligence

LogRhythm

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

LogRhythm and ThreatStream have developed an integrated solution for comprehensive security intelligence and threat management. LogRhythm automatically integrates actionable intelligence from ThreatStream's Optic Platform with other machine data collected throughout the enterprise for comprehensive, real-time threat visibility and next generation security analytics.

The integration allows customers to:

- Dynamically sync threat data from ThreatStream's Optic Platform into LogRhythm for immediate recognition of internal resources communicating with identified bad actors.
- Automate the corroboration of network activity to or from threat indicators with other behavioral changes to hosts and users for more accurate prioritization of high risk events.
- Continually share and receive relevant threat data within the existing security infrastructure to optimize work-flows and enable real-time countermeasures.
- Automate the remediation of attacks recognized from prioritized IOCs 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 ThreatStream's Optic Platform 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 uniquely combines enterprise-class SIEM, Log Management, File Integrity Monitoring and Machine Analytics, with Host and Network Forensics, in a fully integrated Security Intelligence Platform. The LogRhythm solution gives customers profound visibility into threats and risks in areas that were previously exposed. Designed to help prevent breaches before they happen, LogRhythm's Security Intelligence Platform accurately detects an extensive range of early indicators of compromise, enabling rapid response and mitigation. The deep visibility and understanding delivered by LogRhythm empowers enterprises to secure their networks and comply with regulatory requirements. 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

ThreatStream

ThreatStream is a security company that offers a SaaS-based cyber security intelligence platform. The company's Optic Platform is the first ever community-vetted cyber security intelligence platform that integrates directly with an organization's existing security infrastructure. In real-time, Optic aggregates and analyzes threat intelligence from hundreds of sources, including open source intelligence, global honey net sensor farms, social media and private sources. That's in addition to the hundreds of organizations that contribute to the Optic community. Each individual indicator of compromise is categorized and risk ranked for severity and relevance using data analytics to identify relationships with known threats. A risk score is then assigned to each indicator before it is delivered to your security infrastructure.

The Optic Platform enables seamless integration into the enterprise by utilizing Opticlink, a lightweight connector. Opticlink allows organizations to dynamically sync threat intelligence from the cloud into their current security devices where it becomes immediately available for correlation. Beyond just syncing, Optic also delivers purpose built content or correlation instructions so that correlation becomes instantaneous. With Optic there's no need for lengthy professional services engagements or costly aftermarket configurations. Finally, Optic allows organizations to add and manage custom intelligence feeds, enabling automated risk ranking and distribution for correlation.

LogRhythm and ThreatStream 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 and proactively defend against attacks and to prioritize response efforts based on accurate, highly contextualized security intelligence.

Actionable Threat Intelligence

Challenge: The sheer volume of potentially malicious events in an enterprise IT environment makes it difficult for Information Security professionals to prioritize indicators of compromise that pose the most significant risk to an organization.

Solution: ThreatStream's Optic Platform collects, normalizes and risk ranks indicators of compromise from hundreds of sources including open source intelligence, global honeypots, social media, private sources and the Optic community. LogRhythm combines this data with advanced behavioral analytics for real-time threat detection 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 to and from adversary groups to immediately halt an attack.

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 from internal resources to a known adversary group and anonymous proxy networks such as TOR. Administrators need to differentiate legitimate employee activity from suspicious employee activity.

Solution: ThreatStream's Optic Platform ranks and normalizes high risk indicators of compromise, allowing organizations to better define security policies for outbound communication. LogRhythm leverages this data for highly accurate threat detection, identifying users associated with suspicious outbound communication.

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.