PRODUCT OVERVIEW

LogRhythm and Norse: Integrated Security and Attack Intelligence

Connecting internal network events with external contextual live attack data for rapid detection of advanced attacks

LogRhythm and Norse have developed an integrated solution for comprehensive security intelligence and threat management. LogRhythm's advanced correlation and pattern recognition automatically incorporates live attack intelligence from Norse's Darklist and DarkViking solutions to deliver live threat protection based on up-to-date attack vectors and comprehensive security analytics.

The integration allows customers to:

- Continually import threat data from Norse's live attack intelligence into LogRhythm for immediate recognition of an internal resource communicating with identified bad actors.
- 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
- Provide drill-down and deep forensic visibility into activity from known bad actors, including who, what, where, when, how, etc.
- Automate the remediation of attacks from bad actors by blocking communication from malicious IP addresses from the network

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 Norse's live attack 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 uniquely combines enterprise-class SIEM, Log Management, File Integrity Monitoring and Machine Analytics, with Host and Network Forensics, in a fully integrated 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

Norse

Norse's live attack intelligence combined with LogRhythm's advanced correlation and pattern recognition delivers a complete and actionable security intelligence solution. Norse provides contextual, risk-weighted, and continuously updated attack intelligence collected from its global infrastructure, including the darknets, deep web, and anonymous proxies from where many bad actors operate. The integration adds critical external context to internal security events enabling rapid detection of advanced threats, risk-prioritized incident response, and faster time to resolution.

Norse provides threat intelligence via two complementary methods:

Darklist, a continuously updated list of the Internet's highest risk IPs with basic context. Darklist is integrated within LogRhythm, and users can always look up any single IP for a wealth of information about that IP. Norse threat intelligence includes a 0-100 risk score for each IP, the risk category (such as "botnet" or "Tor proxy") to provide context to the score, and highly accurate geolocation.

DarkViking, a live IP lookup solution that queries the Norse Dark Matter platform to provide deeper threat context and years of history for individual IP addresses.

LogRhythm and Norse are tightly integrated, combining the value of next-generation IP blocklists and live attack intelligence with LogRhythm's award winning Security Intelligence Platform. The combined offering empowers customers to identify inbound and outbound malicious activity, detect advanced threats, and prioritize responses based on accurate, highly contextualized security intelligence.

Optimizing Threat Intelligence

Challenge The sheer volume of potentially malicious events in an enterprise IT environment makes it difficult for Information Security professional to prioritize which events pose the most significant risk to an organization

Solution Norse Darklist is a continuously updated list of list of over 3 million high risk IPs with important event context, including risk potential and accurate geolocation. LogRhythm combines this data with advanced behavioral analytics to recognize when network activity with known bad actors is related to other malicious activity, alerting administrators to high risk attacks with greater accuracy.

Additional Benefit Smart**Response**™ Plug-ins are designed to actively defend against attacks by initiating actions that offset the threat, such as automatically add the attacking IPs to a firewall ACL. This immediately stops all activity to or from a known high risk IP, preventing the attack from being successful.

Preventing Data Breaches

Challenge Many organizations struggle with a lack of visibility into activity from their internal users. This includes communication with high-risk areas of the internet, such as IRC chat rooms and anonymous proxy networks such as TOR.

Solution Norse DarkViking provides important context around suspicious activity such as communication with destinations recognized as TOR exit nodes, via a live, SaaS-based threat intelligence feed. LogRhythm correlates this data with advanced behavioral analytics to accurately determine whether or not the activity is malicious for highly accurate threat detection and response.

Additional Benefit LogRhythm provides out-of-the box Smart**Response**™ Plug-ins that can automatically quarantine the endpoint in response to an alarm indicating malicious activity or a potentially compromised host, halting data breaches before damage can occur.