PRODUCT OVERVIEW

LogRhythm and CrowdStrike: Integrated Security and Threat Intelligence

LogRhythm

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

LogRhythm and CrowdStrike have developed an integrated solution for comprehensive security intelligence and next generation threat protection. LogRhythm automatically correlates actionable, adversary-based cyber threat intelligence from CrowdStrike Falcon Intelligence 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 actionable threat intelligence feeds from CrowdStrike Falcon Intelligence into LogRhythm for immediate recognition of malicious activity tied to targeted attacks, malware and advanced adversaries.
- Provide drill-down and deep forensic visibility into activity to and from 40+ specific adversary groups.
- Automate the corroboration of activity tied to threatening adversary groups with other behavioral changes to hosts and users for more accurate prioritization of high risk events.
- Automate the mitigation of targeted attacks by blocking communication tied to known adversary groups.

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 CrowdStrike's Falcon 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 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

CrowdStrike

CrowdStrike is a global provider of security technology and services focused on identifying advanced threats and targeted attacks. Using big-data technologies, CrowdStrike's next-generation threat protection platform leverages real-time Stateful Execution Inspection (SEI) at the endpoint and Machine Learning in the cloud, instead of solely focusing on malware signatures, indicators of compromise, exploits, and vulnerabilities.

Falcon Intelligence is the cutting-edge cyber threat intelligence application of the CrowdStrike Falcon Platform. It provides endpoint threat detection and response endpoint activity monitoring and real-time forensics intelligence and attribution proactive and incident response services enterprises with strategic analysis, organization-specific, tailored intelligence, and customized views of advanced attacker activity. With unprecedented insight into adversary tools, tactics, and procedures (TTPs) and multi-source information channels, analysts can identify pending attacks and automatically feed threat intelligence via API to SIEM and third-party tools.

LogRhythm and CrowdStrike 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 resources based on accurate, highly contextualized security intelligence.

Streamlining Threat Intelligence

Challenge The volume of malicious IPs and URLs has grown to such an extent that it is difficult for organizations to accurately assess and prioritize risk associated with communication to and from potentially threatening locations.

Solution CrowdStrike's Falcon Platform leverages extensive research to deliver highly targeted, adversary-based threat intelligence feeds with industry-leading awareness of the highest priority attackers and adversary groups. 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 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.

Solution CrowdStrike Falcon Intelligence provides highly focused lists of malicious URLs and IPs tied to specific adversary groups, allowing organizations to define streamlined security policies for outbound communication. LogRhythm leverages this data for highly accurate threat detection related to outbound communication with adversary groups.

Additional Benefit LogRhythm's Network Monitor can automatically initiate a targeted packet capture of all outbound data being sent to malicious URLs and IPs identified by CrowdStrike for in-depth forensic analysis and deep understanding of what data is being targeted by an adversary group.