LogRhythm and Cisco: Integrated Enterprise Security

LogRhythm provides a best-of-breed unified Threat Lifecycle Management Platform, uniquely combining enterprise-class SIEM, Log Management, File Integrity Monitoring and Machine Analytics, with Host and Network Forensics. Designed to help prevent breaches before they happen, LogRhythm accurately detects an extensive range of early indicators of compromise and provides an integrated response workflow, enabling end-to-end threat lifecycle management. The deep visibility and understanding delivered by LogRhythm's Threat Lifecycle Management Platform empowers enterprises to secure their networks, comply with regulatory requirements, and increase operational productivity.

LogRhythm and Cisco have formed a strategic partnership to help organizations around the globe increase network visibility and secure their IT environments. LogRhythm offers extensive support for and integration across Cisco's product portfolio, automatically incorporating, normalizing, and contextualizing log, flow and event data captured from over two dozen Cisco products. LogRhythm's Threat Lifecycle Management Platform performs advanced analytics across these data sets, as well as all other machine data collected across an organization, to deliver real-time detection of advanced threats. In addition to being recognized in Cisco's Solution Partner Program (SPP), LogRhythm is a member of the cyber security-focused Cisco Security Technical Alliances (CSTA) program, which is dedicated to bringing together best-of-breed technologies to enable secure and resilient network environments.

Together, LogRhythm and Cisco deliver complementary solutions that combine the visibility and enforcement mechanisms of Cisco's portfolio of leading security and networking solutions with the advanced security analytics and actionable intelligence of LogRhythm's Threat Lifecycle Management Platform. The LogRhythm-Cisco partnership empowers customers to detect internal and external threats, identify behavioral anomalies, enhance security, and enforce compliance. Highlights of the integration include:

Cisco Adaptive Security Appliance (ASA)

LogRhythm collects and continuously analyzes firewall, malware, intrusion prevention and VPN data from Cisco's FireSIGHT Management Center and ASA platforms and applies advanced analytics and correlation against both this data and other machine data collected from devices and systems throughout the IT environment. The integration between LogRhythm's Threat Lifecycle Management Platform and nextgeneration ASA firewalls provides unprecedented visibility and control into client-side applications, operating systems, virtual machines and mobile devices to meet a variety of use cases and strengthen end-to-end threat lifecycle management. LogRhythm also currently supports the eStreamer API, which ensures granular and secure transport of ASA platform telemetry as Cisco transitions to the FireSIGHT Management Center as the optimal integration point for these solutions.

Sample Supported Device List

- Cisco Adaptive Security Appliance (ASA)
- Cisco Cloud Security (Umbrella and Cloudlock)
- Cisco eStreamer
- Cisco Identity Services Engine (ISE)
- Cisco Network Access Control (NAC)
- Cisco Secure Access Control Servers (ACS)
- Cisco Sourcefire Intrusion Detection System (IDS)
- Cisco Routers & Switches
- Cisco VPN Concentrator
- Cisco Wireless Access Point (Meraki)

Customer Use Case: Violating Corporate Policy

Problem: An insurance vendor needs to know when users have multiple concurrent VPN connections.

Solution: LogRhythm collects Cisco ASA firewall logs that provide detail on all VPN connections. LogRhythm's advanced analytics engine looks for two or more Cisco ASA firewall logs from the same origin user in a limited time frame.

Enforcement: If a VPN connection is not terminated within one minute of the second VPN connection being established, an alarm is triggered and the user account is added to a watch list.

Cisco FireSIGHT Management Center

LogRhythm leverages Cisco's eStreamer API to collect network security and flow data from the Cisco FireSIGHT Management Center (formerly Sourcefire), including information generated by Cisco's next generation firewall,

Cisco ASA with FirePOWER services, and by Cisco's next-generation Intrusion Prevention System (NGIPS), Cisco FirePOWER NGIPS. Relative to other collection methodologies, such as syslog and CEF, Cisco's eStreamer API provides more reliable transport and more granular data to third-party systems. Consequently, LogRhythm can ingest and optimize FireSIGHT data in real-time, and correlate threat activity and known vulnerabilities with other network data to deliver advanced security analytics, extended visibility, and continuous monitoring for real-time threat detection and response.

Use Case: Zero Day Attacks

Monitor: Sourcefire's FireAMP leverages a cloud-based antimalware model that pushes real-time security updates to identify malicious files on the wire.

Detect: LogRhythm performs advanced correlation and behavioral analytics on FireAMP events and machine data from other sources to help identify which devices, hosts, applications and users have been targeted and/or impacted, sending all relevant context in a high-priority alarm for immediate action.

Response: A LogRhythm SmartResponse™ plugin can initiate immediate protective action such as terminating communications with command-and-control servers or adding the malicious IPs to a Cisco firewall policy to prevent critical applications and servers from exposure.

Cisco Identity Services Engine (ISE)

LogRhythm and Cisco have developed an integrated solution around Cisco's Identity Services Engine (ISE) that allows users to monitor and secure the entire range of endpoints, systems, and applications across the organization. LogRhythm's Threat Lifecycle Management Platform automatically incorporates identity, access and activity telemetry from Cisco ISE, performing advanced analytics and pattern recognition across the expanded data set to deliver real-time cyber threat protection and compliance enforcement based on up-to-date situational awareness. LogRhythm was the first SIEM vendor to join Cisco ISE's partner ecosystem and continues to invest in the integration to help organizations detect attacks and gain greater visibility across their networks.

Use Case: Compromised Credentials

Monitor: LogRhythm incorporates telemetry from Cisco ISE and applies advanced analytics and correlation against all other log and event data to provide deep visibility into devices and users accessing the network. LogRhythm also creates baselines for logical groupings such as device type, authentication location, number of connections typically made, etc. and thereby establishes a profile for "normal" behavior.

Detect: LogRhythm can trigger a high-priority alert when a user or device violates policy or deviates in a threatening or concerning way from an established behavior pattern based on type, peer group or identity.

Respond: A LogRhythm SmartResponse plugin can initiate an automated response by instructing ISE to quarantine a user or device.

Cisco Threat Grid

LogRhythm continually consumes and analyzes malware and threat intelligence data provided by Threat Grid and combines this with other machine data collected from across the environment to help organizations proactively identify and defend against attacks targeting their network. By correlating the malware artifacts discovered by Threat Grid and changes to the behavior of endpoints and users, LogRhythm enables organizations to quickly prioritize high risk events and take immediate action. Additionally, LogRhythm has developed an out-of-the- box SmartResponse plugin that allows analysts to automatically submit potential indicators of compromise such as domain names, IP addresses, hashes, and file names detected within the LogRhythm platform to Cisco 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.

Use Case: Optimizing Threat Intelligence

Monitor: 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.

Detect: 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.

Respond: A LogRhythm SmartResponse plugin can initiate immediate protective action such as adding malicious IPs to a Cisco firewall policy to prevent critical applications and servers from exposure.