With honeypots and threat intelligence ecosystems, LogRhythm expands capabilities

Analyst: Javvad Malik

6 Nov, 2014

Security information and event management (SIEM) products provide a plethora of data that can be enriched to the nth degree. However, this data is of little value unless it can be converted into meaningful information that organizations can use to proactively detect and respond to threats in an acceptable timeframe.

Threat intelligence can also be viewed in the same light, which in isolation may not provide much useful information. But relevant feeds that can be easily consumed and analyzed can help an organization adopt a proactive security posture. With this in mind, LogRhythm released its Honeypot Security Analytics, Threat Intelligence Ecosystem and Threat Intelligence Security Analytics.

The 451 Take

We've followed LogRhythm's progress closely over the years as it continues to succeed in both midmarket and very large enterprise segments, while continually adding functionality to its offering in order to differentiate itself in the competitive SIEM space. Threat intelligence has recently come to be the flavor of the moment, and LogRhythm is looking to capitalize on it – not just by including threat feeds, but by building out capabilities to best utilize the external intelligence with internal data. This move is likely to not only add additional value for its existing customers, but also help fuel its continued rapid growth.

Context

Founded in 2003 by Chris Petersen and Phillip Villella, LogRhythm initially focused on midmarket players; over time, it achieved success in the large enterprise market. Petersen serves as the CTO, and Villella is chief scientist. Andy Grolnick is president and CEO.

In July, LogRhythm closed a $40m funding round led by Riverwood Capital that included current investors Adams Street Partners, Access Venture Partners, as well as a new investor Piper Jaffray Merchant Banking. This adds to the previously raised $32m, and could possibly be the last funding round before the company makes the move to an IPO. The company states the cash will be used to accelerate product development, as well as grow sales, global marketing and customer care.

The 325-strong employee company has been actively ramping up its channel partnerships both internationally and within North America to build on its base of about 2,000 direct customers.

Products

The Honeypot Security Analytics Suite monitors honeypots in order to track attackers. The information garnered can be used by customers to examine attack patterns and tactics, and generate specific threat intelligence to facilitate the defense posture.

Honeypots are a widely utilized technique in which attackers are lured into attacking a fake network. LogRhythm's Honeypot Security Analytics Suite allows organizations to deploy honeypots to attract would-be attackers. The suite then captures network and log activity related to the honeypots, helping organizations detect attacks including zero-day malware and other emerging payloads.

LogRhythm's Security Intelligence Platform, in turn, prioritizes the intelligence derived from the honeypot to create blacklists and other defensive measures on the production network. Additionally, LogRhythm announced its Threat Intelligence Ecosystem and related security analytics suite to detect high-risk threats. The ecosystem of intelligence providers was initiated with partners CrowdStrike, Norse, Symantec, ThreatStream and Webroot. The threat intelligence delivered can be automatically consumed by LogRhythm's security analytics platform.

In conjunction with the Threat Intelligence Ecosystem, LogRhythm also released a corresponding Threat Intelligence Security Analytics Suite to ensure accuracy of partner intelligence. LogRhythm customers that are existing customers of one of the partner threat intelligence providers get the benefit of automated collaboration of the external threat intelligence with internally collected information from log, flow, event and machine data, as well as LogRhythm's endpoint, server and network-forensic sensor data.

Competition

LogRhythm's core competition in large enterprises has been and will remain other SIEM vendors such as HP ArcSight, RSA Analytics, IBM (QRadar), Splunk, Tripwire, Tier 3 and McAfee (Nitro), with AlienVault, SolarWinds and others competing for the business in SMBs. LogRhythm's Security Intelligence suite expands beyond traditional SIEM into network forensics, endpoint forensics and advanced security analytics. Other vendors in these areas include RSA, Blue Coat Systems and Tripwire among others.

SIEMs all benefit from threat intelligence, something we've seen work well for AlienVault's Open Threat Exchange. And owing to its large footprint, HP ArcSight is usually the first product that threat intelligence and analytics vendors want to integrate with. By creating a threat intelligence ecosystem and partnering with providers, LogRhythm is looking to tip the odds in its favor. That being said, the threat intelligence space is in a state of flux, with M&A activities and partnerships always seemingly on the horizon, which could cause LogRhythm to consider acquiring a threat intelligence vendor or two for itself.

SWOT Analysis

Strengths

With its network forensics release, LogRhythm showed it could bring specialist technology to the wider market, putting it in a good position to replicate the process with honeypots and threat intelligence.

Weaknesses

Threat intelligence is an often overused term that encompasses a wide range of capabilities. LogRhythm may need to educate customers on the benefits of its offering to get extensive traction.

Opportunities

With information security buyers increasingly focused on reducing mean time to detect and mean time to respond, LogRhythm's focus on delivering improved efficiencies in identifying and managing incidents could offer additional differentiation for the company.

Threats

The emergence of standalone security analytics vendors focused on specific use cases could impact SIEM buying patterns. Although material evidence of such a shift has yet to surface, it is an area that LogRhythm will likely be keeping an eye on.