LogRhythm: understanding 'normal' with multidimensional behavioral analytics for big data

Analyst: Javvad Malik

19 Dec, 2012

Large enterprises have historically faced the challenge of being able to collect data from all their assets. However, as technologies evolved, particularly with SIEM offerings, organizations solved this original problem only to be faced with another. The big-data conundrum: how to sort through the masses of data to find the actionable information.

In light of growing targeted threats, this identification of key events needs to occur not just post-incident, but as close to real time as possible to allow action to be taken to minimize potential impact. In order to address these ever-increasing needs, Boulder, Colorado-based LogRhythm has bolstered its SIEM 2.0 technology with what it describes as multidimensional behavioral analytics for big data that allows organizations to bolster advanced threat and real-time breach detection – quite the mouthful. In simpler terms, it means LogRhythm can now baseline 'normal behavior' against a wide range of enterprise activity such as logs, flow and machine data – therefore increasing its chances of detecting any potentially malicious activity.

The 451 Take

We like how LogRhythm has continued to improve and add capabilities to its platform. The latest release feels like a significant shift up in gear, expanding beyond SIEM into areas where it will find itself stepping on the toes of vendors of 'anti-malware' and determined-attacker prevention, as well as forensics and analytics providers, with the potential to extend its scope beyond security into wider IT operations. In essence, LogRhythm is seeking to fulfill the role of security intelligence for the enterprise encompassing protection against cyber-threats,

big-data security analytics, compliance automation and assurance. However, the SIEM landscape remains a competitive one, and LogRhythm will find itself up against a laundry list of well-funded competitors.

Context

Founded in 2003 by Chris Petersen and Phillip Villella, LogRhythm has raised $31m in venture capital from Siemens Venture Capital, Adams Street Partners, Grotech Ventures, Access Venture Partners and Colorado Fund I. Initially focused on midmarket players, over time it carved out a space in large enterprises. Petersen serves as the CTO, and Villella is chief scientist; Andy Grolnick is the president and CEO.

LogRhythm has grown to more than 230 employees, and claims over 1,400 customers globally with offices in Europe, North America, Australia and Hong Kong among others. It has reported impressive growth figures, as well as high customer retention, and claims to be on target to increase sales by 50% in 2012, fueled in most part by strong channel growth.

Products

LogRhythm's SIEM 2.0 platform has been bolstered with the addition of 'multidimensional' analytics that collect data sets throughout the environment in which it is deployed, and analyze relevant information patterns to provide real-time threat information.

The primary data that is collected by log managers includes user and identity data, network data, host data and application data. This information is normalized and immediately fed into the LogRhythm Advanced Intelligence Engine that forms the heart of the real-time analytics. All log, flow and activity data is processed in memory for speed, and undertakes the necessary correlation, pattern recognition and behavioral analysis.

Using this information, LogRhythm builds up a picture of what constitutes normal behavior across each cross-section of user, network, host and application behavior, and uses this as a baseline against which it can analyze potentially suspicious behavior by taking a combined view. That is to say, being aware of a spike in application-authentication attempts provides one view of an activity. But combine this with knowledge of how many active users are on the network at that time, and a much richer picture can be built as to whether the activity is potentially malicious. In effect, baselining the normal behavior creates a whitelist of normal and acceptable activities.

This can be beneficial because LogRhythm comes with the ability to terminate any non-whitelisted processes in the event of an incident, thus allowing normal activity to continue while root-cause analysis is undertaken and threat mitigated. Furthermore, LogRhythm utilizes internal and external context to provide a better understanding to reduce false positives and negatives. Internal context is built up from multiple internal data sources such as vulnerability data, asset classification, business entity data, content management systems, identity and access management products and the like. The external context data comes from its LogRhythm Labs group as well as data feeds such as IP reputation services, threat intelligence feeds, geolocation service and other third-party sources. The intent is to provide enough context of the external threat environment that when internal activities match certain conditions, notifications can be sent to system administrators to determine whether it is indeed an active threat.

Competition

There is certainly no shortage of rivals for LogRhythm in the SIEM arena, Hewlett-Packard (ArcSight), IBM (Q1 Labs), McAfee (NitroSecurity), RSA (enVision), Alert Logic, eIQnetworks, BlackStratus (formerly netForensics), NetIQ (Sentinel), Trustwave, Tripwire, S21Sec, Tenable Network Security, AlienVault, Sensage, Red Lambda and many others will all be battling in the same arena, each putting greater emphasis on real-time analytics and threat intelligence.

SWOT Analysis

Strengths

Real-time analysis, in addition to being able to baseline normal activity within the enterprise, is a big step forward and keeps LogRhythm very well aligned to market needs.

Weaknesses

We think LogRhythm could do better than referring to its product features with phrases such as 'multidimensional behavior analytics for big data.' Granted it sells to security teams, but better clarity would help.

Opportunities

LogRhythm has the opportunity to take the 'S' out of SIEM, and expand its product beyond security departments to assist capacity planning, networking ops and IT departments as a whole, although regulatory-compliance needs will keep security at its core for the foreseeable future.

Threats

The SIEM market is a crowded and competitive landscape with well-funded competitors all vying for dominance. LogRhythm, as others, will need to continually innovate and demonstrate value to its customers to remain relevant.