LogRhythm

Threat Lifecycle Management Platform

DETAILS

Vendor LogRhythm

Product Threat Lifecycle Management Platform

Website logrhythm.com

Price $35,000 appliance (software-only option available for $27,000).

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Diverse and well-thought-out operational feature set. User configurable dashboards. Easy to use and deploy.

Weaknesses None that we found.

Verdict This is an important contender for your SOC SIEM. It will take data from just about anything you need to monitor and it includes solid third-party threat feed access. This is our Recommended product.

Of all of the tools we examined this month, this one seems to be the one most at home in the SOC. LogRhythm has a long history of log management and analysis. In today's threatscape, the product has evolved into a full-featured SIEM with a bit of a twist. The SIEM world can be a bit complex so a big piece of what makes a SIEM successful is visualization. For LogRhythm that's the twist.

The tool is next generation in that it uses some advanced AI for managing complex issues such as advanced intrusions or complicated compliance issues. The platform manager is a database that receives data either directly from the data process/indexer or via the AI engine. Everything starts with the agents, though.

At the end of the day the Platform receives events through the agents, assigns them to a log type (logs that match up with a common event), pulls out the metadata, then follows its rules to dispose of the event in the most appropriate manner. Perhaps that means an alert or some other action, such as beginning remediation. This is traditional SIEM activity with the addition that today's analysis is far more sophisticated than in the past, but the fundamental process is similar: receive the data, parse it, analyze it and take some action.

The tool uses ElasticSearch to speed up searches through large quantities of data. There are databases within the SIEM that include such things as the user preferences, case management, alarms and so on. There are two types of consoles as well: client console and web console. The consoles are laid out conventionally with a top-level navigation bar that sends you to the dashboards, alarms, cases, searches and reports.

The dashboard gives an overview of activity on the enterprise from different perspectives, such as analysts, executives and operations. The alarms page summarizes the alarms showing risk levels. Cases shows summaries of the current cases and searches is a straightforward columnar page, while searches shows the searches performed. You can separate out your own searches.

When you drill down or look at results of a search, you can bring up an analyze page that gives a lot of details and you always can drill down for more. One of the more useful features is the ability to configure custom dashboards using widgets that perform certain specific functions.

This is a solid SOC tool and is straightforward to use and deploy giving SOC engineers the most flexibility. This clearly is an operational tool. There is basic no-cost support through the customer community which, while very useful, we don't consider an official support channel. Other support is by subscription.

– Peter Stephenson, technology editor