A capable SIEM needs to take vulnerabilities, threats and assets into account in order to give a credible picture of the enterprise, says Peter Stephenson.

Security information and event managers (SIEM) have pretty much reached their plateau in terms of product-type maturity. In terms of functionality, we did not see much that was new this year. However, the tools we looked at exhibited many improvements in the depth to which they analyze data and present findings to the administrator.

That said, there are some areas that are coming to the fore in this group. For example, compliance is a big deal.

Another development we saw this month is that SIEMs are beginning to lose their personalities. Whereas we are used to seeing appliances that are strong in log management or reporting or some other functionality, we now see all tools trying to be full-out SIEMs with all of the bells and whistles of a first-rate correlation and reporting system. And, for the most part, they are succeeding.

LogRhythm

Vendor	LogRhythm
Price	$25,000
Contact	www.logrhythm.com

The LogRhythm appliance features high-powered functionality to the enterprise in the way of log correlation and full, real-time event analysis with massive bells and whistles. Right out of the box, this appliance not only collects, analyzes and correlates log data, but also encompasses advanced functions, such as file integrity monitoring, network and user monitoring, and full-scale compliance reporting.

SC MAGAZINE RECOMMENDED

With all this power, one would think it would be complicated to deploy and manage, but this appliance can be up and running with very little effort. The true power comes by way of a solid dashboard that provides an easy and intuitive way to view data and drill down to see deep into events and get a clear picture of which events took place and how they happened.

This appliance also comes loaded with a full set of preconfigured rules ready to go, and can be easily modified to fit the specific needs of any environment. We also found this solution to offer a multitude of deployment flexibility with several install options.

Documentation included installation, configuration and administrator guides. All these are accessible from the LogRhythm console itself, so there is no need to fumble through several PDFs when looking for configuration information. We found all documentation to be clear and well-organized and to include many screen shots and easy-to-follow configuration examples.

LogRhythm offers standard 11-hours-a-day/five-days-a-week support, as well as platinum 24/7 phone and email technical support as part of an annual agreement. Customers also can access an online portal with other resources, including an online knowledge base.

At a price of $25,000, this appliance is an excellent value for the money. It comes packed with many advanced functions and features that are easy to use and intuitive to interpret.

SC MAGAZINE RATING

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths Advanced Intelligence engine provides more in-depth event correlation.
Weaknesses None that we found.
Verdict For its value and feature set, we make this offering our Recommended product.

LogRhythm®
COMPLY. SECURE. OPTIMIZE.

LogRhythm, Inc.
3195 Sterling Circle, Suite 100
Boulder, CO 80301
(303) 413-8745 office
(303) 245-9075 fax
www.logrhythm.com

It comes packed with many advanced functions and features that are easy to use and intuitive to interpret.

Peter Stephenson