With a new crop of competent security information and event management tools, the choice of which to choose depends on users' needs, says Peter Stephenson.

This month we took a look at some of the top players in the security information and event management (SIEM) market.

Although all of the products we tested had the same core capabilities – correlating data from multiple sources, giving a consolidated report, and more – some products had a strong forensic focus. However, as we know, any good SIEM is a very useful network forensic tool in the context of incident response. There are some purely forensic requirements when legal issues come into play, though. Not all SIEMs can cover those. We saw some in our crop of products that covered all of the forensic bases well. So, even though we considered them SIEMs, these had a strong focus on forensics.

As well, all SIEMs do some log management. Some products we looked at have a legacy of log management, and that legacy shone brightly this month.

LogRhythm v5.1

Vendor	LogRhythm
Price	$25,000
Contact	logrhythm.com

The LogRhythm appliance offers some very powerful functionality for log management and security event management. This product is designed for the large enterprise and distributed environments. With features that include log management and analysis, file integrity monitoring, event management, network and user monitoring, and geolocation tracking, this product can provide the detail needed for in-depth security event analysis.

The appliance comes preloaded with all the necessary software for the LogRhythm platform, including Microsoft SQL Server, and all the LogRhythm components, so there is no actual installation that has to be done. Just a short Windows setup wizard, and the appliance is ready to go. After the appliance is set up, all management and configuration is done through the management console. We found this console to be easy to navigate with a well-organized layout. The dashboard itself includes a wealth of information that is quite easy to drill down into and view.

This product is all about detail. Every alert, chart or graph can be clicked on and drilled into. This appliance provides a great amount of depth and allows for going all the way into the source log data. To get a closer look for analysis, there is also the ability to use replay to go back and analyze past events as they happened.

Documentation includes a short quick-start guide, which outlines how to get the appliance up and running, and a much larger PDF administrator guide.

LogRhythm offers 11-hours-a-day./five-days-a-week phone and email support at a cost of 20 percent of the purchase price of the appliance annually. There is also 24/7 support available at a cost of 30 percent.

At a price of $25,000, this product may seem quite pricey, but we find it to be a great value for the money. The LogRhythm appliance offers a solid feature set with a lot of granular analysis capability.

SC MAGAZINE RATING

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

Strengths Provides granular analysis features, such as replay and geolocation to track events.
Weaknesses None that we found.
Verdict For its excellent functionality, we make this 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

Designed for large enterprise and distributed environments, and delivered with excellent functionality, we give LogRhythm our 5-Star "Recommended" rating.

Peter Stephenson