CorreLog

SIEM Correlation Server

One of our great rewards here in the SC Labs is seeing vendors take our reviews seriously enough to respond with better products, at least in part due to our review. Last year, we reviewed the CorreLog SIEM and, while we liked it a lot, we took it to task for its documentation. We are happy to report that the documentation has gotten better this year.

With the very small exception of a lack of clarity in a single piece of the installation process, this product installed faster and easier than any product of similar complexity that we've seen in our many years of doing product reviews. We probably could have given it to Dillon, the Lab Dog, and gotten similarly good results. We installed the server on a virtual MS Server 2008 R2 and stuck a Windows agent on a virtual Windows 7 machine. No sooner had we completed the agent install than the Correlation Server had started communicating with it.

The dashboard is simplicity itself. The home page – this a web page, the landing page actually is called out in the menu as "Home" – has something that we never have seen: the page consists of links to a variety of supplementary information and downloads. For example, it's easy to download the agent for the device you want to monitor. Simply browse to the Correlation Server from the device you want to monitor, in our case the Win7 VM, and download the agent. Once the file is on your device, all you need to do is execute it. The rest is automatic.

The main menu sports a series of dashboards, including a top-level view, a specific dashboard for PCI DSS, an overview of threats, and several others, including a way for you to create custom dashboards. These, like any dashboard, provide an overview with drilldown.

Generally, we found this an easy to use and very comprehensive product. It is supplied as software, which means that you will need a server – physical or virtual – to house it. However, access to the Correlation Server is via the web, so once it is installed you can access it from any browser that can reach the server over the enterprise. Even with the extra cost of a physical server, the overall cost of ownership is very reasonable.

The tool has its own ticketing system and reporting is extensive. In addition to supplied reports, there are templates so that you can create your reports. The included reports contain the usual compliance reports and there is an interesting capability for creating pivot log analyzers much like a spreadsheet pivot table.

Support is good with a year of basic aid included and a fee-based program as well. Documentation is extensive and much improved over our last look. The website is clear with such things as a support portal.

– Peter Stephenson, technology editor

DETAILS

Vendor CorreLog

Product SIEM Correlation Server

Website correlog.com

Price $5,000.

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

OVERALL RATING ★★★★★

Strengths The easiest product of its type to deploy, comprehensive feature set and a good price point – even if you need to add the cost of a physical server in-house.

Weaknesses None that we found.

Verdict We like this a lot, especially for SMBs, although larger organizations certainly should not rule it out as too small. It's not. For its value and feature set, as well as the efforts to improve and keep the product ahead of the curve, we make this our Best Buy.

CorreLog, Inc.
1004 Collier Center Way, 1st Floor
Naples, Florida 34110
+1-877-CorreLog (267-7356) - Toll-free (US only)
+1-239-514-3331 - Telephone (US, Int'l)
+1-239-687-3505 - Fax
info@CorreLog.com
www.CorreLog.com