EventTracker

SIEMphonic

The folks at EventTracker take a rather unique approach to the SIEM market: SIEMs are likely to become shelfware. While we are not sure that we agree completely, it is true that for some organizations the rigors of deploying and using a SIEM effectively can be challenging. EventTracker's answer is a co-managed SIEM.

The company characterizes SIEMphonic as an "iSOC" - intelligent security operations center. This is an interesting set of concepts and we dug in with not a small amount of skepticism given the marketing sound of this terminology. It turns out that there is quite a bit of method to this apparent madness and we were impressed.

First, core credentials of SIEMphonic are quite good. The capabilities of the tool are right where they ought to be. A server sits at the customer's site and acts as a collector along with some analysis, but the real threat intelligence work is done in the cloud managed by EventTracker experts and fed back to the customer. This is a mutable arrangement. Depending on the customer's internal capabilities, more or less of the EventTracker SOC team's side of the co-manage equation may be used. Certainly, the customer gets a very comprehensive dashboard.

The SIEMphonic model is what one would expect from a capable defense tool: predict, prevent, respond and detect. The product provides functionality for each of these parts of the model. For example, to prevent there is vulnerability scanning, 24/7 coverage addresses detection, the company offers forensics and remediation recommendations to assist in response, and all of the threat analysis capability of the Threat Center fills in the prediction piece.

SIEMs are aggregators and correlators. SIEMphonic takes data from the enterprise and from external threat feeds. Devices on the enterprise can be any of the 2500-plus manufacturers that EventTracker supports. These include such log types as Windows event logs, syslogs in several flavors, snmp, IIS, Exchange, Sharepoint and many others.

One facet that we found important is the use of STIX files for threat intelligence updating. SIEMphonic uses STIX as a source of threat intelligence input. The product uses a customized and internally maintained version of Soltra Edge. We saw some other analytics here that impressed us. For example, endpoint sensors can run a quick on-the-fly analysis of files to determine if they are known malicious or, if not, if they have been compromised. This is based on a trust list determined by known/seen-before files, as well as the National Software Reference Library. Another related endpoint capability is USB monitoring. USBs can be allowed or blocked and files exfiltrated by USBs can be monitored.

The tool supports 4,000 to 8,000 events per second out of the box, and logs are forensically preserved. Vulnerability scans can be scheduled and reporting is detailed, including trending. The system has its own honeynet based on an embedded deception network with virtual decoys spread around the enterprise and, of course, alerting is automated.

Reporting is substantial and we especially liked the Critical Observations Report, which gives only those events that are of importance. It actually learns over time so it is one of the few examples of a "smart" report that we have seen.

– Peter Stephenson, technology editor

DETAILS

Vendor EventTracker

Product SIEMphonic

Website eventtracker.com

Price Starts from $2,900 per month.

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★
Value for money	★★★★¾

OVERALL RATING ★★★★★

Strengths Comprehensive SIEM with a lot of new concepts, well-integrated into the overall product/service combination. Superior documentation.

Weaknesses Support is too tightly coupled to the co-manage model.

Verdict This product is a must-see. Any size organization can benefit by considering this as part of its security stack.