UBM TechWeb

Network Computing

November 2010

For IT, By IT

AccelOps 2.1

SIEM Plus

AccelOps puts security information and event management and operations data in the same package

AccelOps, a relatively new entrant in the security information and event management market, combines SIEM functions with performance and availability monitoring features typically found only in network operations tools. The result is a platform that provides visibility for both security and network operations centers (NOCs). We tested AccelOps 2.1 and found it offers surprisingly rich functionality and usability while remaining cost competitive.

AccelOps was founded in 2007 and offers both SaaS and on-premises delivery models, which we believe is unique among SIEM vendors. In the cloud model, AccelOps hosts all of the infrastructure and functionality, a setup that security-sensitive companies may balk at since it requires them to send log data off-site. We tested the on-premises version, which was packaged as a VMware-based virtual appliance. AccelOps makes recommendations on hardware specifications based on the size of the environment, but the virtual appliance makes deployment very easy.

One of AccelOps' customizable security dashboards

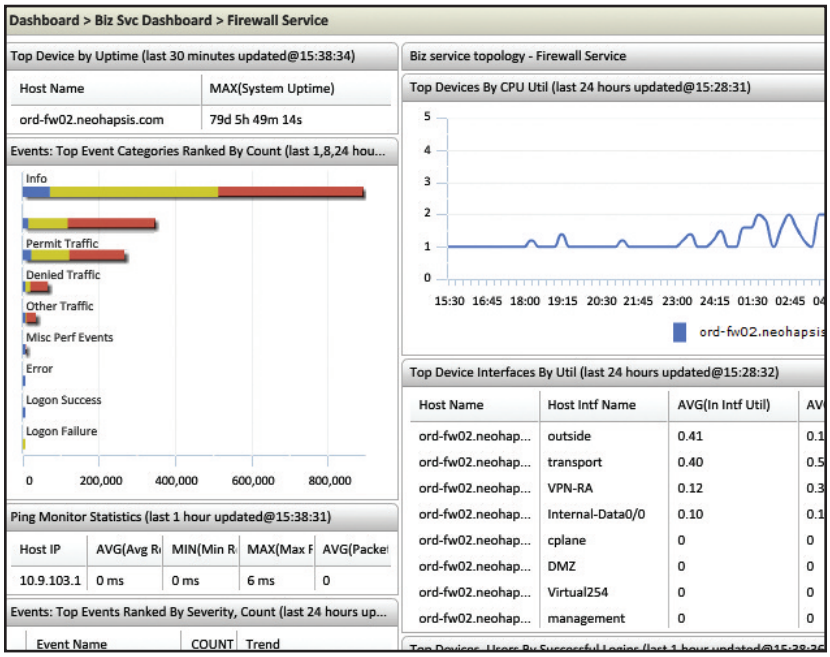
Our test environment is a mixed set of Windows and Linux systems, along with routers, switches, firewalls, intrusion-detection systems, Web servers, and VPN gateways. We found that the product offers an impressive array of features, including must-have SIEM capabilities: a reporting engine, a range of device-specific log parsers, a correlation engine, an alerting mechanism, and an impressive set of dashboards. The Flash-based UI is polished, responsive, makes good use of data visualization tools, and is downright slick compared with the "ho-hum" interfaces found in many legacy SIEM products. We found the UI's layout to be intuitive, with top-level navigation areas providing easy access to dashboards, reporting, configuration data, and alerts.

The only negative to the Flash-based UI—besides forcing security-conscious folks to use the security-challenged Flash player—is that there is no left-mouse-click option.

AccelOps does support syslog, which is the de facto communication method for transmitting event data to SIEM products. It gathers basic network session information via Netflow (versions 5 and 9). The product also supports the Windows Management Interface (WMI) for gathering Windows events, because Windows doesn't support syslog natively.

The downside of using WMI with AccelOps is that, unlike with syslog, you need a credentialed, admin-level user on the target system to pull logs. The company says it will research the feasibility of providing alternatives.

By Greg Shipley



AccelOps required that SNMP be enabled for the intrusion-prevention sensor module in our Cisco ASA for the initial device identification/device provisioning step. Is this a game ender? No; we enabled SNMP, performed the device discovery, then turned off SNMP. That said, the more devices you supply credentials for, the greater the visibility the AccelOps SIEM provides. We haven't tested a SIEM yet that matches AccelOps in terms of system health and security status.

As a SIEM, AccelOps delivers all of the features that one expects. It comes with a number of prebuilt dashboards for authentication; network-control devices like VPNs, firewalls, intrusion-prevention systems, and so on; system availability; and more. Some dashboards are more useful than others, but AccelOps let us reconfigure dashboards to our liking. The reporting engine also comes with a number of good canned reports and an ad hoc query mechanism for quick text searches.

When it comes to the real heart of a SIEM product—the correlation engine that effectively reduces millions of raw device events into meaningful alerts—AccelOps met our needs. It offers the standard complement of prebuilt correlation rules, along with the ability to edit or add rules as needed. The system boiled down raw event data into alerts that pointed us to suspicious activity, such as large volumes of failed logins, advanced levels of network probing, and intrusion-prevention activity that warranted further investigation.

We received a lot of false positives related to Windows Kerberos authentication events. We tuned out the noise with some adjustments to the default rules, but we hope AccelOps will provide more-accurate rule baselines as the product matures. That gripe aside, the combination of a reasonable correlation engine, a solid reporting engine, and ad hoc query tools provides the foundation for a solid SIEM offering that will meet the needs of most companies.

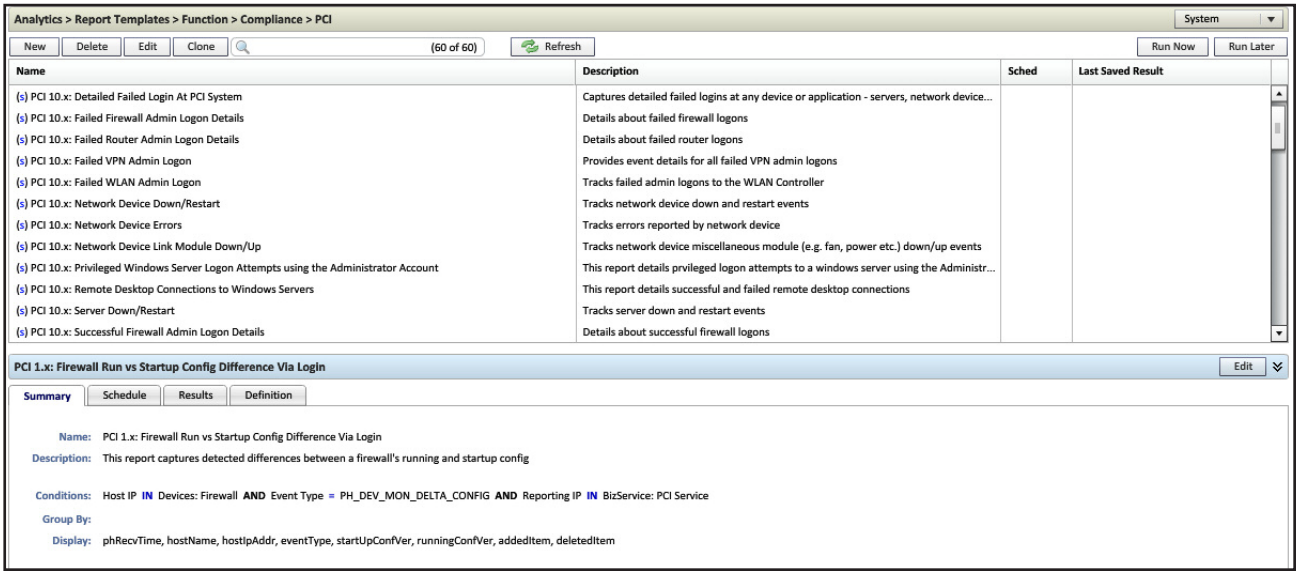
While this review is about SIEM, we couldn't help but notice (and play with) the NOC features, including processor- and memory-use levels, network bandwidth utilization, storage availability, and performance thresholds. We found them quite useful. For example, we set up SNMP v3 on our Cisco ASAs and were able to monitor not just firewall activity but general firewall health. We did the same for our Windows servers, and we were pleased to be alerted when one of our file servers hit 99% disk space consumption.

AccelOps' Flash-based UI is responsive and slick, with easy access to dashboards, configuration information, and more.

Final Analysis

AccelOps' target audience has been small and midsize companies, but in September the company released a version of its software aimed at large enterprises and service providers. Its general feature set is good, and the dashboard and correlation engine are on par with many established SIEM players.

We recommend taking a look at AccelOps. Given that the product is less than 3 years old, the 2.1 version is stable and feature-rich, a dream for companies that are looking to affordably improve their security and network



AccelOps maps rules and reports to compliance specifications

operations centers, and a contender for small and large SIEM deployments alike. AccelOps offers on-premises and SaaS-based pricing models, and also licenses features based on security operations center and NOC functionality. Support for 250 devices and approximately 1,500 events per second is priced at $45,000 for a perpetual license or $18,000 for a subscription license.

Greg Shipley is a security consultant and a former CTO. Write to us at comments@nwc.com.

Our Take -AccelOps 2.1

PROS

The platform combines security information and event management (SIEM) and network performance monitoring

Customers can choose SaaS or on-premises deployment, including a virtual appliance

The product offers a strong set of SIEM features and functions

CONS

The product has to store admin-level credentials to get logs from Windows systems

accelops

www.accelops.net
2905 Stender Way, Ste 48
Santa Clara, CA 95054
sales@accelops.net
408-490-0903