



SIMs security information/event management systems

GOLD | ArcSight ESM

Organizations looking for a security information management (SIM) solution have a lot of vendors to choose from, but ArcSight Enterprise Security Manager stood out from the crowd, according to readers. The product won a gold medal in the SIM category, scoring high marks for its event correlation capabilities, effective management interface and compatibility with existing systems.

ArcSight ESM also scored well in its ability to map information to security policy or compliance regulations, and its granular and flexible policy definitions.

The biggest benefit of ArcSight ESM is its dashboard graphics for analysis of security events, says Tim Maletic, manager of information security at Priority Health, a Michigan-based health insurance company.

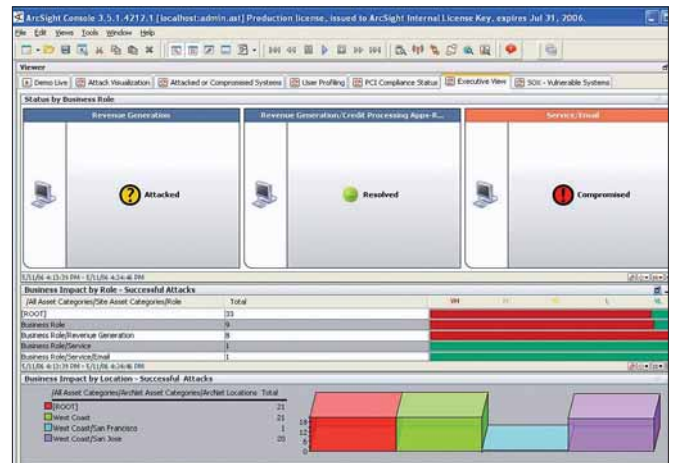
The product allows him to easily view events, drill down through various displays and pull data to research events.

In addition to using ArcSight ESM for incident detection and response, Priority Health uses the product to help with various compliance efforts. "It does a good job of recording what you do with the tool," Maletic says.

"I can use that data to back up my incident response policy and other policies we get audited on, and prove we're doing what we say we're doing," he adds.

Maletic says the list of devices ArcSight ESM supports is impressive. Priority Health uses the product to integrate data from IDSes, firewalls, Windows, UNIX and Linux servers, antivirus, and vulnerability assessment systems. The company also is writing customized agents for homegrown applications.

The fine-grained policies ArcSight ESM provides for user management can be a little daunting to set up, but provide valuable flexibility, he says.



Last year, ArcSight bolstered ESM with the release of its Compliance Insight Packages. The packages bundle rules and reports based on ISO 17799 and NIST 800-53 standards to help organizations meet regulatory requirements such as SOX, HIPAA, and the Payment Card Industry (PCI) Data Security Standard.

Also in 2006, ArcSight expanded beyond its core capabilities in security management with its acquisition of ENIRA Technologies, a supplier of technology for automating network management tasks. After the acquisition, ArcSight released Network Response Manager, which automates network responses in order to block worm outbreaks, hacker attacks or other security events, and Network Configuration Manager for automated network discovery and configuration management. ▶

Information Security and searchsecurity.com presented 1,595 readers with a survey of 341 security products, divided into 15 categories. The categories and product lists were determined by Information Security and searchsecurity.com editors, in consultation with recognized information security experts.

Reprinted with permission from Information Security Magazine, April 2007.
© 2007 TechTarget. All Rights Reserved. FosteReprints: 1-866-879-9144



For more information visit www.arcsight.com.

ArcSight is a leading provider of security and compliance solutions that intelligently identify and mitigate business risk and deliver a centralized view of enterprise-wide events across heterogeneous infrastructures. This real time and historic view into external attacks, insider threats and regulatory compliance provides enterprises, MSSPs, and government agencies with the intelligence and response capabilities required to effectively protect and manage their networks and their businesses.