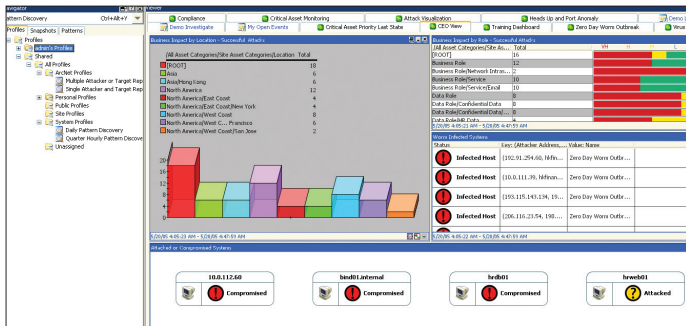


« Security event management

ArcSight ESM



Version	3.0
Supplier	ArcSight
Price	from \$50,000
Contact	www.arcsight.com

ArcSight's flagship product, the ArcSight Enterprise Security Manager, is a security event management (SEM) tool capable of analyzing large amounts of network data in real time. The IDS model fell down because the flood of unfiltered alerts overwhelmed the resources of security teams, but SEM provides correlation, filtering and analysis to allow the few real threats to be picked out of the blizzard of less important alerts and false positives.

As ArcSight's real strength is analyzing huge volumes of data, we took only a cursory tour through the product sent into the labs.

For serious testing, we stepped into the security center at an ISP which provides managed security for many corporate clients, generating millions of events a day. If that is not enough to stress test any SEM tool, nothing is. Because the data was live from corporate networks, testing was under strict NDA and we have kept the service provider and its customers anonymous.

Although we tested the product at one extreme end of the spectrum in terms of the network, the product can scale right from middling-size enterprises up to the top end.

The ArcSight architecture comprises several components. At the lowest level are the data collection "SmartAgents." These reside either on remote systems feed-

ing information back to the database, or on a separate layer taking syslog or SNMP feeds from a device such as an IDS, firewall, or log server.

Our environment included IDS products from several different vendors and multiple data feeds from remote networks. Some of these were fed through an intermediate stage of filtering – many vendors supply correlation engines of their own to reduce the overhead of redundant alerts.

The final stage brings all the event data into a central database, which is where a substantial chunk of cost will lie in any SEM implementation.

In our case, with a very high volume of traffic, this was a beefy cluster of Sun servers running an Oracle database and even then we observed the ArcSight interface having to wait for queries to return.

With more complex analysis, the system slowed even more, but despite this we never waited more than a couple of seconds for data to update. In the context of a security manager taking decisions in real time, we considered that to be perfectly acceptable.

At the heart of the ArcSight suite is the ArcSight Manager, the server component which drives the management console. Usually, this will be the ArcSight Console software or a web browser – we used the former. While we usually prefer web interfaces from a portability perspective, the ArcSight Console is very slick and makes a real difference.

The console interface is not easy to describe, because it is flexible

in the extreme. Essentially, the console provides a canvas into which numerous small modal windows are available, all of which offer some custom view on a dataset queried from the server and its database.

Every component, dashboard, list and graph can be customized to each administrator's particular role, with compartmentalized delegated privileges. And within the established bounds of each administrator's role, that user can rearrange the interface and data in many other ways.

The end result is no two ArcSight user consoles will look alike – everyone has their preferences to get their job done fastest, and getting the job done fast is what ArcSight is about.

There is a fair amount of initial work done to create zones, configure data sets and set up some automation, but once complete, it is easy to navigate what is in effect the calm surface of a turbulent sea of data.

We liked the ability to replay correlated sequences of events to analyze an incident – a handy tool from the forensics perspective, too.

Although we were pleasantly surprised at how easy the interface was to grasp, it is still quite complex and clearly takes some mastering. Watching experienced ArcSight users at work is a lesson in security administration – of the thousands of events flagging up in the system, the security staff in our ISP test environment were able to track and react to incidents within moments, slicing the data so it could be categorized, logged and then set aside as low risk or escalated for immediate action.

With all the interaction with raw network data, ArcSight has not forgotten the interface upwards, into business management.



A reporting system provides a set of standard reports covering the common information required, although it is easy to roll your own reports, too, including reports which compare the current results to the previous run. This is ideal for auditing and tracking progress, as well as for measuring service level agreements and identifying anomalies.

We were impressed with ArcSight ESM. It is well-designed for the heavy lifting job of event management, which might put it out of reach of some enterprises in terms of complexity and cost.

But the benefits to the security operation on any large or complex network will be well worth the effort, as well as the outlay.

Jon Tullett

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★☆
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★★
Value for money	★★★★☆
OVERALL RATING	★★★★★
<p>For Scalability and analysis features are both exceptional. Against Database requirements are high, but not unexpected. Verdict Heavy-duty toolset to accomplish a full range of SEM analysis.</p>	

ArcSight, Inc.
email: info@arcsight.com
Phone: 408 864 2600

ArcSight, the recognized leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM™ enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently. ArcSight's customer base includes leading worldwide companies across all verticals—and more than 20 of the top 30 U.S. federal agencies.