



Going to School On Intruders

The University of Tennessee didn't have enough manpower to see who was trying to attack its systems. The answer: installing a centralized software product to analyze intrusion logs and warn of danger ahead.

BY DEBORAH GAGE

Like many research universities, the University of Tennessee is a prime target for hackers and other Internet miscreants. It manages Oak Ridge National Laboratory, which conducts research on national security for the Department of Energy. It runs health-care facilities that collect patient data. It supports an inter-campus computing grid for researchers, who routinely transfer 40-gigabyte data files using unorthodox protocols that may escape detection by ordinary security programs. And it acts as an Internet service provider for students, who occasionally "get crazy" with the high bandwidth and swap multimedia files that can transmit viruses and worms, says senior security analyst A.J. Wright. Each network needs to be locked down as tight as a drum.

In addition, as part of a push to tighten information security, the school recently took on projects to upgrade old network switches, secure wireless networks, and redesign the university's firewall to group systems with sensitive information, among other things.

There's plenty to do.

Like all security managers, Wright would like more people to help him do his job, which he says is unlikely given the university's budget.

One particular challenge was finding a way to monitor intrusion logs for all the devices—firewalls, intrusion detection systems, intrusion prevention systems and more—that protect the campus against hackers and may be subject to attack.

At the main campus in Knoxville, which has 26,000 students, Wright had five people to watch over more than 20 devices, all of which worked differently because they came from different vendors. And any one of the devices could log millions of connections per day—more data than any human being can absorb.

To centralize all the information coming in from the logs, the university in February installed a product from ArcSight of Cupertino, Calif., called ArcSight Enterprise Security Manager (ESM). ArcSight ESM places sensors on Linux boxes around the network that monitor devices or applications that customers choose—including physical security systems like badge readers. Data is put into a single format

by the ArcSight Manager, which has configurable rules that can parse data by vendor, type of device, time of day, likelihood of threat and so on. Customers can graphically view and analyze data through an ArcSight console or over the Web. For example, with graphs users can quickly identify the "top talkers" on the network; these talkers may be infected.

Wright says his biggest challenge has been learning everything that the ArcSight product can do. "We thought we were buying a sedan, and we ended up with a 4x4," he says. For example, the university had turned off many of the rules for sending alerts on its individual intrusion detection systems because they sent too many. Now the rules are back on, and ArcSight can help eliminate false positives.

His only real quibble is that ArcSight's documentation was not always in sync with its product. For example, installation failed on Red Hat Linux version 3.6 even though the documentation said that version was supported. But Wright says the company provided excellent support, which more than made up for any problems. According to ArcSight senior vice president Steve Sommer, the company sends a person to each site to help with implementation.

The university chose ArcSight ESM over four or five other products because it works across Windows, Macintosh and Linux operating systems and with other university equipment, such as software made by Tripwire that audits changes made to information-technology systems. It also understands DHCP, or dynamic host configuration protocol, which the university uses to assign students Internet Protocol addresses when they log on to the network. And it is configurable enough that Wright was able to write code to connect ArcSight with IP Audit, an open-source tool similar to Cisco's NetFlow that shows relationships between network devices. That data now feeds into ArcSight, which looks for patterns to show what those relationships might mean. If ArcSight finds that machine A talked to B and B talked to C, for example, maybe a worm has spread from A to C.

Wright declines to say what the university has spent on ArcSight, although Sommer says deployments start at around \$50,000. ◀

Reprinted from Baseline, September 2006 with permission from Ziff Davis Media Inc.

©2006 Ziff Davis Publishing Holdings Inc. All rights reserved.



ArcSight, a leader in Enterprise Security Management, provides solutions that serve as the mission control center for real-time threat management, compliance reporting and automated network response. By comprehensively collecting, analyzing and managing security data, ArcSight solutions centrally manage and mitigate information risk for security, insider threat and compliance. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs.