

University of Tennessee Achieves Expert Protection

A.J. Wright

With more than 45,000 students and 12,000 faculty and staff, and five campuses, the University of Tennessee (UT) prides itself on educating its students, doing research and creative work that improves quality of life, and reaching out to share expertise with Tennesseans. The university stands in a class by itself as Tennessee's flagship institution and one of the United States' great public research universities.

Like most major educational institutions, UT is a prime target for hackers and the insider threat. Past security incidents involving university systems attacking military sites resulted in all access from the university being blocked. Because our institution has been awarded millions of dollars through various grants, not having the ability to communicate or continue research efforts has a detrimental effect on the university.

To protect our network, we installed a variety of security devices, including multiple intrusion prevention systems, firewalls and vulnerability assessment tools. Our IT staff soon discovered that these devices were generating around 20 million events per day. We did not have the manpower or the budget to manually sift through these logs. Neither could we waste time and money babysitting security devices 24x7.

We needed an expert system that

could interface with our many security devices and act as a central place to collect log data — and could automatically and intelligently correlate the information.

Our university engaged in a pilot project to better understand what it wanted to accomplish and to more accurately gauge the features and capabilities it most required. We conducted a thorough evaluation of the security information and event management market, running a number of competing systems through their paces, before

"We needed a solution that could interface with many security devices and automatically and intelligently correlate the data."

ultimately selecting ArcSight Event Security Manager. We realized that on the surface many of these offerings purport to do the same things, but they don't. Based on this evaluation, ArcSight was the clear choice.

ArcSight allows us to find the proverbial needle in the haystack by enabling us to filter out the things we don't really care about and immediately alerts us to suspicions events that we are truly concerned about. ArcSight can also automate the escalation of those events,

either via email, pager or mobile device, to ensure the right people are notified at the right time.

SIEM turned us from a reactive security organization to a proactive one. Advice for other organizations looking to do the same thing would be to make good use of filters to make sure you're catching data that isn't an incident now, but may become a problem soon, i.e., make sure the trash you're filtering out is really trash.

Also, set up a vulnerability management system to make proactive action part of the regular process. Begin with collection, then analysis, follow with remediation for incidents and finally reporting.

When searching for a SIEM solution, we found the following qualities to be paramount:

Ability to connect to all the various devices we need to collect data from,

- Asset modeling/rules/lists,
- Quality of correlation engine,
- Reporting power and
- Ability to integrate with our existing workflow.

We've greatly improved our visibility into threats that seek to harm our network. Using ArcSight ESM, we can quickly spot emerging worms and worm variants before signature detection is available. Moreover, our staff can review new patterns daily and automatically create new rules for

identifying these threats in the future.

Whenever a new worm or virus propagates across the network, we can quickly locate any infected machine based on ArcSight's correlations rules. ArcSight then automatically feeds that information back to our campus management system, which will disable that particular machine on the network.

If it is 2:00 a.m. in the morning and a worm starts spreading, we don't have to log into 10 different devices or look at 10 different sets of logs to under-

stand what is happening. The flexibility of ArcSight even allows us to create an automated response for such events. If a

"ArcSight allows us to reduce response times, improve performance and be a much more responsive organization."

machine gets compromised, there is no need for worry. We can come to work

in the morning and know that the situation has been resolved.

Overall, ArcSight plays a critical role in helping our staff reduce response times and improve performance. With ArcSight, we are turning the corner from being a reactive organization when it comes to security to becoming a much more proactive one.

AJ Wright, chief technology officer and chief information security officer, University of Tennessee.



ArcSight (NASDAQ: ARST) is a leading global provider of security and compliance management solutions that protect businesses and government agencies. ArcSight identifies, assesses, and mitigates both internal and external cyber threats and risks across the organization for activities associated with critical assets and processes. With the market-leading ArcSight SIEM platform, organizations can proactively safeguard their assets, comply with corporate and regulatory policy and control the risks associated with cyber-theft, cyber-fraud, cyber-warfare and cyber-espionage. For more information, visit www.arcsight.com.