

NETWORKWORLD

T R E N D W A T C H

SECURITY

SECURITY LEVEL 02



ERROR!!
PLEASE START AGAIN

How information protection, identity-centric access control, security event management and managed services are shaping new defenses



SIEM: Finding the proverbial needle

We're getting closer to the day when making sense of and taking action on disparate security events gets quick and easy

BY SANDRA GITTLEN

Matt Roedell, vice president of infrastructure and information security at TruMark Financial Credit Union in Trevoze, Pa., has a big dream for his layered security network: One day, his antivirus protection, firewall, intrusion-detection system and other security tools will use integrated, intelligent [security-information and event-management](#) techniques to stop fraudulent transactions.

An early adopter and big believer in SIEM (also called security event management or security information management), Roedell believes the technology will reach its full potential only when it's integrated into application and network security tools. Today SIEM comes in the form of stand-alone tools that collect, correlate and analyze event logs across a security infrastructure. ([Compare SIEM products.](#))

Roedell's wish is on its way to being granted, says Kelly Kavanagh, research analyst at Gartner. SIEM providers are making creative strides, moving from mere log collection to intelligent analysis, he says. As an example, he points to SIEM's newest use case: application-layer monitoring for fraud detection or internal threat management. Companies are putting SIEM alongside their traditional security tools to collect and analyze application-level events or transaction logs for the purpose of discovering transaction combinations that are indicators of fraud or misuse, he says.

Roedell calls SIEM, which has more than 20 competing vendors, one of the fastest-growing security markets, having a growth rate of more than 50% in 2006 and 30% in 2007, when estimated revenue topped \$800 million. Large enterprise companies, such as CA, Cisco, EMC (its RSA security division), IBM, Novell and Symantec, have SIEM products, as do a host of smaller companies. These include ArcSight, High Tower Software, Intellitactics, LogRhythm, netForensics, Prism Microsystems, Q1 Labs, SenSage and TriGeo.

The first indications of the full integration that Roedell wants are starting to show up, too, Kavanagh says. Such companies as CA, IBM and Novell have started to bundle or integrate SIEM with other pieces of their portfolios, including identity-based access management; systems management; and IT governance, risk and compliance management offerings.

"I can prove to auditors that [the SIM appliance is monitoring] just about anything with an IP address."

MATT ROEDELL,
vice president of infrastructure
and information security,
TruMark Financial Credit Union

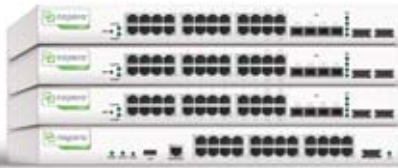
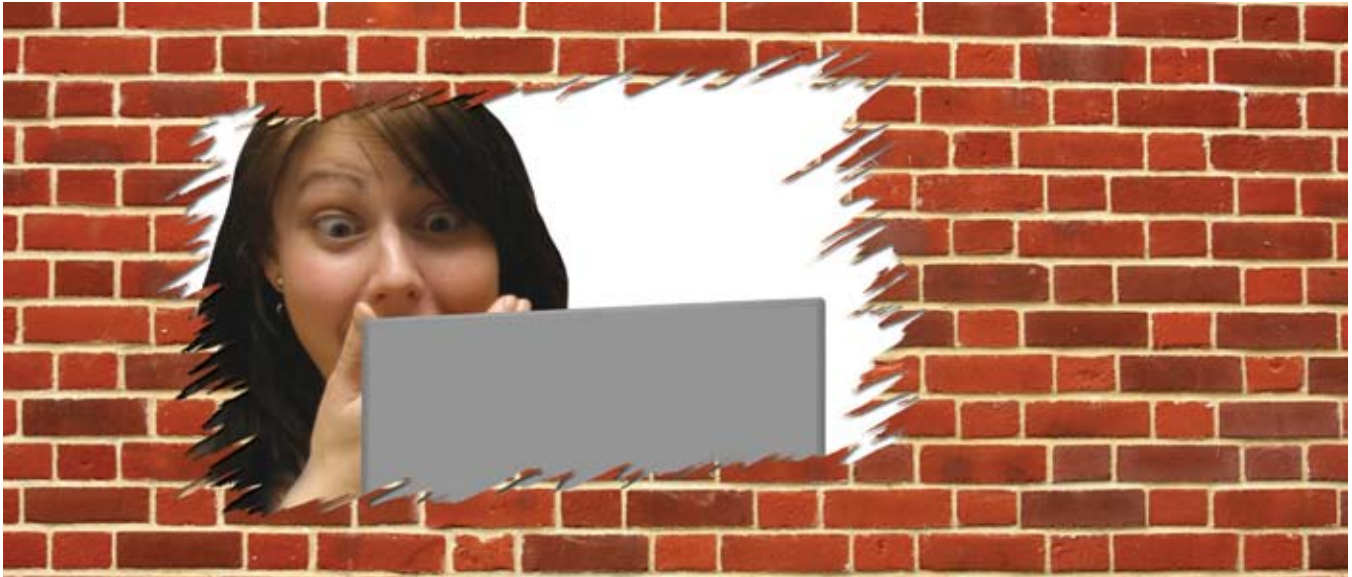
Agents on the loose

Roedell uses TriGeo's [TriGeo Security Information Manager](#) (SIM) appliance to determine the severity of threats to his company's security infrastructure. The agent-based TriGeo SIM correlates events, such as alerts about TCP port scans on the firewall or intrusion-detection system (IDS) anomalies, and sends a ticket to IT or mitigates the problem based on preset thresholds. For instance, it can end PC processes, shut down switch ports, add access lists to routers or make firewall configuration changes — actions that otherwise would require someone to log on to each device and manually update it.

Using the SIM appliance to keep such close tabs on his security network not only has made vulnerability management much easier but also has improved compliance initiatives, Roedell says. "I can prove to auditors that [the SIM appliance is monitoring] just about anything with an IP

B. PROUD

Your employees just blew up your firewall!



The Napera N24 is an appliance and integrated Web-based management service that makes sure only authorized users and secure computers access your systems.

It is the only practical network access control solution built for the small and medium enterprise. In just ten minutes, you can deploy Napera and start taking back control of your network!



Find out if your network is at risk by taking the Napera Network Test, and you could **win a free iPod nano!**

www.napera.com/products_test.php

In today's mobile computing world, laptops move in and out of your network and your users walk right around your firewall, bringing unknown threats with them.

A virus, Trojan horse, or hacker is like dynamite to your business, with just one attack costing hundreds of thousands of dollars in lost revenues, productivity and corporate reputation.

Napera plugs those holes in your firewall by:

- Making sure computers are updated and patched before access
- Quarantining unhealthy devices
- Enforcing identity
- Providing real-time visibility and reporting

address," he says.

Compliance, nevertheless, is only one factor leading to enterprises' increased awareness and adoption of SIEM tools, Gartner's Kavanagh says. Their interest also can be attributed to the technology's maturity, the decrease in its deployment and management complexity, and the availability of affordable, easy-to-deploy SIEM appliances.

Although SIEM tools have improved since earlier versions, they still can be too complicated, cautions Ted Ritter, research analyst at Nemertes Research. This is especially the case for large enterprises: "The complexity of the SIEM implementation goes up dramatically with the size and complexity of the infrastructure," he says. In a 2007 "Security and Information Protection" benchmark study, Nemertes found that 64% of 54 participants at 49 companies collected logs, but only 25% had implemented SIEM. "They said the main reason they hadn't is that it's still too complex and difficult to configure to catch the things they want to catch," he says.

Millions and billions of events

When SIEM is done well, however, threat management becomes so much easier, says Denis Hein, senior information security engineer at Wells Fargo Bank in Chandler, Ariz. He describes security management before he deployed SIEM: "We had processes in place, but they weren't enough to handle the tens of millions of events we receive daily. Four or five people were logging into separate security tools looking at information in different ways. There was no common view or correlation," he says.

In addition, Hein was frustrated with each vendor's threat taxonomy, he says. "What one firewall vendor might call critical, an IDS vendor might ignore. Although we had all these tools and were monitoring a lot more, we were still missing things," he says.

Now Hein uses [ArcSight's SIEM](#) platform to develop and apply his own logic for identifying, prioritizing and mitigating threats. "The tool has better information, so it is generating better information on threats. [That] means we can take better action," he says.

Team members can tailor their own views of the data, Hein adds. "Although we all have access to the same information, it enables us to be far more focused. For instance, one person looks only at events and information pertaining to credit-card processing, while another can focus on a virus issue, all from within the same console," he says.

Like Hein, Arlan McMillan, global head of information security operations at ABN AMRO, a Chicago financial services giant with 110,000 employees, has tapped into advanced SIEM features. "You have to get out of the narrow focus of threat vectors and get into the range of behavioral analysis. Let your point solutions worry about Trojans and viruses. [SIEM] tools take you to the next step," he says.

For example, McMillan uses the [collection and correlation features](#) of his Intellitactics Security Manager appliance to identify patterns that indicate what he calls "low and slow" attacks. "Viruses and worms like 'I Love You' and Slammer are really easy to see. What we need to get are the more sophisticated attacks," he says.

All of ABN AMRO's security endpoint data — more than a billion events a month — passes through the centralized appliance. In turn, it correlates the data and filters out such faulty information as IDS false-positives, which can be as high as 80%, and mistaken firewall patterns, McMillan says. "We then present a 'washed' version of the data to a human analyst for further investigation. If we were to give him the raw data, there would be zero expectation for consistency, reliability or repeatable processes. And if you don't have these three things, you can't set rules or check the validity of your systems," he says.

Behavioral analysis is just the beginning of what SIEM tools will be able to do in the near future, says Julio Casal, CEO of AlienVault, a support and certification provider and contributor to an open source version of SIEM. The Open Source Security Information Management project is working on advanced versions of SIEM tools in conjunction with universities.

"This market is growing so fast," Casal says. "Soon these tools will use artificial intelligence, neural networks and fuzzy logic to spot potential problems with the network based on changes, and carry out quick remediation."

Gittlen, a freelance technology editor in the greater Boston area, can be reached at sgittlen@verizon.net.

Four tips for SIEM success

1. Start with a baseline understanding of your security events.

"You have to do a risk assessment before choosing a tool to know what you need. Look at every event in your environment, ask if it's normal and then what the threshold is within a certain time frame," says Matt Roedell, vice president of infrastructure and information security at TruMark Financial Credit Union in Trevose, Pa. In addition, be sure you understand your alert and mitigation strategies, he says. Skipping this step will render your security information and event management (SIEM) product useless, he adds. ([Compare SIEM products.](#))



2. Don't bite off more than you can chew.

The "start slowly" advice for IT deployments definitely [applies to SIEM](#), says Denis Hein, senior information security engineer for Wells Fargo Bank in Chandler, Ariz. "First, bring the product in-house and test it. How it looks on paper can be quite different than how it runs in your environment," he says. Next, tackle perimeter security, he advises: "Stay conservative to make sure it holds up as you scale and add in more endpoints."



3. Establish a system for dealing with alerts.

"If you don't already have processes in place for dealing with logs, then SIEM will not improve your security posture," says Kelly Kavanagh, principal research analyst at Gartner. Unless you have a plan in place before deployment, you're sure to waste your SIEM investment, he adds.



4. Make sure executives are onboard.

"Properly define your mandate and have your executives endorse it," says Arlan McMillan, global head of information security operations at ABN AMRO, a Chicago financial services giant. "IT teams will have to cross internal organizational borders to secure logs that might be sensitive or confidential, so you need all your governance issues clearly laid out before you start deployment."



— Sandra Gittlen

