SIEM

Readying for security incidents

ebook

An SC Magazine publication

Sponsored by

Contents

SIEM carries on, despite the odds

When it comes to security technologies, security information and event management tools have been frustrating to many – yet they are here to stay, reports Beth Schultz.

Depending on who you ask, security information and event management (SIEM) is either a boon or boondoggle, or maybe a little bit of both.

Done well, SIEM produces undeniable benefits – the ability to react in real time to threats and to meet compliance mandates rank at the top among them. However, the problem, many say, is that SIEM solutions can be difficult to tune to full effectiveness. In fact, sometimes the effort can be so overwhelming that companies leave their SIEM appliances in a corner collecting dust rather than deal with the time and effort required to make them useful.

"As much as I love SIEM – it's my favorite technology – I know there are a lot of people who are frustrated by it," says Anton Chuvakin, who worked within the SIEM vendor community for nearly 10 years and now heads SIEM consultancy Security Warrior Consulting. "This includes people who think they've been deceived by vendors and those who think they've been promised something that they haven't been given. That's a very powerful sentiment about SIEM."

But still, Chuvakin adds that SIEM's promise of combining security technologies together for better visibility across everything going on is an important goal. "We almost have to have this, and the fact that we cannot have it yet doesn't stop me."

From threat monitor to compliance checker

SIEM tools evolved out of the intrusion detection system (IDS) and intrusion prevention system (IPS) disciplines, upping the ante with the notion of real-time threat monitoring. Early SIEM tools – whether software or appliance – collected data from security devices, such as a firewall, IDS or IPsec, and searched for patterns indicative of threats. They used rules-based correlation to speed problem recognition.

Historically, SIEM represented the be-all and end-all of security management. It was the purview of only the largest enterprises – those with deep pockets and big IT security staffs manning multi-console security operations centers.

"The belief was that in order to be a serious security shop, you had to have a SIEM in place," says Richard Bejtlich, principal technologist and director of incident response at General Electric Co. "A lot of companies fell into this trap. 'OK, the next phase of our maturity is we have to have one of these things,' they said."

While Bejtlich says reality hasn't borne out the absolute necessity of SIEM, enterprises of all sizes flock to the technology today. Many enterprises, no matter the size, are drawn initially to SIEM for compliance rather than its original intent: threat monitoring.

Indeed, when new compliance mandates hit the enterprise – stemming from initiatives such as the *Health Insurance Portability and Accountability Act (HIPAA)*, the Payment Card Industry (PCI) Data Security Standard and the *Sarbanes-Oxley Act* – SIEM took on a new life. By feeding network device event logs into a SIEM, enterprises created a central repository for the logs they'd need for meeting compliance mandates. They could analyze and run reports on the logs, as well as archive them. Suddenly, SIEM data grew to colossal proportions at many companies.

SIEM on fire

Now, SIEM has reached the mainstream. "We're in the broad adoption phase," says Mark Nicolett, a vice president at Gartner Research who has been following the technology's development since its earliest days.

$1.4b

SIEM revenue expected to reach in 2013

– IDC

In 2009, Gartner fielded 40 percent more calls from clients with funded SIEM projects than it did in 2008, which had seen higher SIEM-related call volumes than the year prior, too. "Investment in SIEM projects carried right through the economic depression," he says.

SIEM has become a hugely popular security management technology, agrees Charles Kolodgy, research director of security products at IDC. In fact, SIEM is driving overall growth in the security and vulnerability management technology sector with a compound annual growth rate of 16 percent for the five-year period ending in 2013, he says. Led by ArcSight, EMC, Symantec, Attachmate and Q1 Labs, SIEM revenue for 2008 reached $663 million, IDC's research shows. That figure is expected to reach $873 million in 2010 and $1.4 billion in 2013.

But still, many industry watchers say SIEM evolution has been disappointing overall, and that in many instances the technology falls far short of its potential.

> "SIEM provides a smart system that can take data from all our different systems and make sense of it."
> *–Richard Bejtlich, General Electric Co.*

One wary SIEM watcher is Joel Snyder, senior partner with Opus One, an IT consulting firm. "Fundamentally, I haven't seen a huge evolution in the technology inside a SIEM" he says. "There has been change, so it's not as if we've sat still. But really innovative ideas, like using reputation services, haven't permeated throughout the marketplace. We see that sort of thing in one or two products, but more or less that's it. So it's been disappointing."

SIEM specialist Chuvakin agrees. "Basically, a lot of the technology is pretty much what was built by the early SIEM vendors in the late 1990s," he says. "There were a lot of ambitions put forth and a number of promises about what SIEM would do, ultimately providing a single pane of glass for viewing all security things across the corporation. But that hasn't really happened."

The problem lies in the very nature of what SIEM tools aim to do. "You've got this massive pile of logs and the SIEM tools have to give you useful, actionable data from that," says Snyder. "The hardest thing is the rule writing. While SIEM companies have done a great job of providing rules or giving the ability to write rules, they haven't taken a quantum leap. It's easier, but fundamentally the same."

GE's Bejtlich echoes these concerns: "SIEM provides a smart system that can take data from all our different systems and make sense of it and tell us what's really going on. Only problem is, if you're starting with data that you couldn't operationalize – meaning, turn into an action – then it's pretty ambitious, to be polite, to think you could have a system that could make sense of that stuff."

Roll up your sleeves

All this is to say that SIEM requires hard work – a lot of it. "It's certainly not something you can buy, install and forget about," says Johannes Ullrich, chief research officer with the SANS Internet Storm Center.

Nor can you turn to an easy-to-use manual for guidance, he adds. "How you configure SIEM depends on your network, and then you need to make continual adjustments, going through the network device by device to figure out how best to collect and correlate event logs."

Jeff Dalton, technical operations officer for Regulus Group, a nationwide payment services provider in Napa, Calif., adds that when it comes to SIEM, he doesn't think there's such a thing as 100 percent deployed. After all, he says, "every time we add a new device to our network, we've got to add it into this wonderful world."

Dalton, for one, approaches SIEM with caution. He's been driven to SIEM with

$873m

What SIEM revenue is expected to be in 2010

– IDC

the goal of more efficiently and effectively handling the 1,700 special audit requests his company must handle yearly. "These requests could easily be one or 100 questions, but they are all mainly asking, 'Are your roles and controls surrounding governance adequate?'" he says.

For now, PCI remediation is his focus, for which he turned to Q1 Labs' QRadar SIEM tool. He's feeding logs from about 350 devices into the tool, roughly 40 percent of his production environment, and checking to make sure the reports he can pull from there pass PCI, the SAS 70 auditing standard and other requirements. "We're not going any further until we validate that the reports are coming through and doing what they're supposed to do," Dalton says.

So far, so good, and, he says, the benefits have been both organizational and personal. "I used to take at least an hour-and-a-half to two hours a week to make sure we could pass a quarterly audit for a specific customer, and now I'm down to about 20 minutes per week. That's saved me quite a bit of time, almost 60 percent, which is really important," Dalton says. "We don't have a whole lot of IT staff, and being an outsourcer we're trying to stay lean and mean in order to be competitive."

Size matters

While smaller and mid-sized enterprises might have just a single person keeping tabs on the SIEM data, a large organization might devote a team or more of security analysts to implement and then watch over SIEM. Such is the case at BNY Mellon, a leading asset management and securities services company based in New York. Created out of mergers and acquisitions, BNY Mellon has inherited multiple SIEM tools and has since consolidating on a single platform, says Daniel Conroy, the firm's managing director of information security.

"We have teams of analysts that look for internal and external threats, and a team that

Top priorities: Picking the right SIEM

Following the 2007 merger of Bank of New York and Mellon Financial of Pittsburgh into BNY Mellon, Daniel Conroy returned to the company after a brief hiatus. As managing director of information security, he faced the challenge of integrating two good-sized security operations. As part of this effort, he needed to decide on which of the multiple security information and event management (SIEM) platforms to standardize. Here he describes the top priorities he required:

Event throughput: BNY Mellon feeds data from upward of 70,000 devices into its SIEM. The tool needs to be able to handle roughly one million events per day without blinking.

Ability to receive data from any sources: Name a log type and chances are it's being fed into BNY Mellon's SIEM. Conroy says he doesn't want to mess around with layering in additional technologies owing to the fcact that a SIEM can't accept the feeds from the ones he already uses.

Scalability: "With certain SIEM tools you can put the technology into each data center, but that data is only local to that data center," Conroy says. "With our SIEM, we wanted to make sure someone in Europe, for example, could view the attack profile of the organization globally."

Adaptability: BNY Mellon needed a SIEM tool that provided flexibility in how the company handled alerts. "For example, we might specify, 'Hey, this alert should kick off an SMS, and if somebody doesn't access that within a certain period of time, then it should move on to the next level in our escalation procedure,'" he says. "Certain SIEMs don't have that technology."

– Beth Schultz

16%

compound annual growth rate for the five-year period ending in 2013: SIEM is driving overall growth in the security and vulnerability management technology sector

– IDC

does access privileges for database monitoring. Plus, automated alerts trigger off anything else that happens to be outside the environment for those teams. For example, our firewall managers might look at the logs sometimes if they're trying to diagnose a problem," Conroy says. "We use the SIEM across the organization for four or five different reasons – from debug to analysis to investigation."

A global operation, BNY Mellon is feeding data into its SIEM from upwards of 70,000 devices. The SIEM tool handles some one million events per day, so far with aplomb. That's a pleasingly different experience than what Conroy says he has had with previous products. "We crushed other SIEMs with a lot less traffic than that," Conroy says.

> "We use the SIEM across the organization for four or five different reasons."
>
> – *Daniel Conroy, BNY Mellon*

And one million events per day is nothing, comparatively. Mark Evans, information security manager for Salt Lake County Information Services, in Salt Lake City, reports having had 600 million events in his SIEM database after only two months of use. While Evans has begun the finetuning that will help reduce that volume, he says he isn't worried about it. "I know I've got a long way to go before this thing is fully implemented," he says.

While other products he tested couldn't keep up with that volume, the tool he selected, NitroSecurity's NitroView Enterprise Security Manager, is doing so without a problem. "We can jump around in it like lightning," he says.

Plus, Evans already has cut the database in half just by turning off 95 percent of the signatures it had been feeding into the tool from its Websense web traffic monitors. "We left the juicy ones in, like who tried to download an .exe file or visit a keylogger site, and turned off the rest. Now we're only getting a few thousand signatures a day rather than a few million," he says. And, he adds, deleting the 300 million unnecessary signatures from the database only took five or so minutes."

Not all SIEM users experienced such ease of use. Brian Shellock, senior security analyst at Lehigh Valley Health Network, a large hospital system serving eastern Pennsylvania, says a sizable event-per-day volume flattened his first SIEM tool, essentially turning it into a security and compliance nonentity, he says.

"We were getting more than 100 million events per day from just half of our systems, and it couldn't handle the volume. It would chug along, freeze up and miss 22 hours of the day. It wasn't catching or storing the data," Shellock explains. "Plus, running even a short report would take hours."

For the past two years, however, Shellock has been using Prism Microsystem's EventTracker SIEM tool without any problems at the health care organization based in Allentown, Pa. "It doesn't miss a beat," he says.

This SIEM tool has changed the way Shellock approaches security and compliance management, he says. "It essentially gives me the eyes and ears going through the events, so I can be out doing other things, getting more information, figuring things out, setting more alerts and correlating behind the scenes."

Previously he had been limited by the ineffectiveness of that earlier SIEM tool, which he had brought in-house in large part to address *HIPAA* compliance mandates. "I spent all my time collecting events just so I could say, 'Well, I'm obeying *HIPAA* and storing my logs.' That's great, but what does it all mean? All this information was there, but I wasn't getting anything out of it."

Easing into SIEM

For many companies, the sense of ease they're expecting following a SIEM implementation never does materialize. This can especially be the case at smaller companies,

40%

more calls Gartner received from clients with funded SIEM projects than it did in 2008

which often rely on the SIEM tool vendor or other external experts for implementation help. Subsequently, they often feel swamped by event notifications.

Tom Franciosi, CIO at Covenant Dove, a national nursing home provider based in Memphis, Tenn., knows how critical, yet overwhelming, the initial SIEM experience can be. Franciosi joined Covenant Dove three years ago to help centralize IT operations as the company undertook an aggressive growth strategy.

"Given that health care is one of the most popular targets for nefarious hackers, I knew we needed some means of gaining real-time visibility about how the network was behaving, or not, and that was SIEM," he says.

Having evaluated SIEM products for use at a previous employer, Franciosi selected TriGeo Network Security's TriGeo Security Information Management product and set it up to collect information from almost 1,000 devices.

"When we first installed SIEM, our security guy did feel the danger of having too much information coming at him, so we tuned it down a bit – the first exposure to this type of product can be overwhelming," Franciosi says. "But once you're used to it and you know what you're looking for, like anything it becomes more manageable."

But this is not always the case. "One of the biggest problems with SIEM implementations is that most companies hire a consulting company for deployment," says Nathan LaFollette, CEO of iNet|Detect, a security consulting firm in Columbus, Ohio. "The consulting company will install it, throw every device at it and tell the owner, 'Hey, you've got all this great data here.' And the owner says, 'Oh, this is so valuable, all this visibility is great.'"

Problem is, the next day the contractor leaves the company to its own devices. And the IT security professional is stuck trying to make business sense of 15 million alerts a day. "That can be a daunting task for any company," says LaFollette.

"Most customers at this point weigh the cost of sifting through millions of events per day and tweaking the false-positives in hopes that at the end of the tunnel they will see business risk measurability," he says. Some decide the effort won't pay off or, perhaps, that they simply can't devote the necessary personnel hours to the ongoing task.

> "The first exposure to this type of product can be overwhelming."
>
> *–Tom Franciosi, CIO, Covenant Dove*

Those who decide to proceed with the fine-tuning ought to be prepared to spend six to 12 months tweaking the tool before seeing any business risk value, LaFollette says. "Those who don't will continue to use the SIEM technology as a glorified syslog server that cost way too much."

Taking the fast track

GE's Bejtlich says he's talked to many peers who essentially do just that. "They use it sort of as a giant bucket. They dump everything into the bucket and use it to do simple things, like searching. That's not SIEM. Correlation is missing."

Still, this works for some. "What's nice about this approach is the amount of information you need to do something useful upfront is low, as opposed to the SIEM idea which involves deep knowledge of your environment," Bejtlich says."

It's a fast-track approach, Bejtlich adds. "You put everything in one place and then search it once you know what to look for. I call that 'retrospective security analysis.'"

True SIEM implementations are far more time-consuming, even more so than LaFollette's six months-to-a-year projection, especially for large enterprises. "Anybody who tells you they've got a successful SIEM deployment has generally taken two, three or maybe even four years to get there," Bejtlich

$2m

per year is the average cost an enterprise suffers as the result of a cyberattack

– Symantec, 2010 State of Enterprise Security study

THE ESSENTIALS: What makes a SIEM?

The ability to correlate data is a defining characteristic of a security information and event management system (SIEM). But sometimes, users confuse other necessary SIEM elements with correlation, says Richard Bejtlich, principal technologist and director of incident response at General Electric Co. To Bejtlich, the top SIEM essentials are the ability to:

- Collect data sources in a central location;
- Normalize data sources, which means converting log sources into a common format;
- Prioritize events;
- Suppress certain events;
- Accumulate events via simple incremental counters;
- Centralize policies;
- Summarize via reports; and
- Configure software.

Bejtlich adds it is necessary to correlate data, which he defines as the process of applying criteria to data inputs, generally of a conditional ("if-then") nature, in order to generate actionable data outputs.

– Beth Schultz

says. "What you're doing is using the knowledge of your own environment that you've built over the years and you're encoding that into a tool. That's the key lesson from the whole SIEM idea – it ends up being more about what you learn about your environment and less about the tool."

In and of itself, that's not a bad thing, Bejtlich adds. "Anything you can learn about your environment is definitely worthwhile. The question is, Are you willing to spend six figures, potentially seven, for a premiere product to get to that? Or is there another way?"

At GE, the security team uses SIEM as yet another source of indicators rather than as a universal system for pooling events and tracking incidents. "We put a select feed of data into SIEM and have the SIEM correlation engine tell us, as Chris Matthews would say, 'Tell me something I didn't know,'" says Bejtlich, referring to the host of MSNBC's *Hardball with Chris Matthews*.

The SIEM reveals to the GE security team something it didn't know by culling through and normalizing the log data, sending an alert when it comes up with something fishy. The team treats that alert just as it would any other data received from its systems, Bejtlich says.

"We have a dozen or so generic ways to find activity, and SIEM is just one of them. That's a quick way to SIEM, taking a period of months instead of years to implement – and it's flexible, realistic and doesn't cost as much money as when using SIEM for everything," he adds.

While Bejtlich declines to name the SIEM tool in use at GE, he notes that the company looked for a product that met its needs, but intentionally stayed away from the premiere wares. "We didn't feel the money for a Cadillac was justified by the extra features we would have gotten. We were more interested in the correlation engine piece," he says, noting that GE has been using its tool in a meaningful way for more than a year, having installed it in the fall of 2008.

SIEM of the future

A critically important part of the story, Bejtlich says, is enterprise log management. "If you get that as part of your SIEM, that's great. If you integrate a standalone product into your SIEM, that's great, too. I can't recommend this highly enough," he says. "You've got to have a repository that allows quick searches and accommodates a huge variety of data types."

When GE began its SIEM project, log management wasn't a common request. That meant that integrating the company's standalone log manager was a bit of chore,

75%

of enterprises experienced cyberattacks in the past 12 months

– Symantec, 2010 State of Enterprise Security study

Bejtlich says. If he had to make the SIEM decision now, a top question he'd ask potential vendors would be whether they offer log management functionality as part of their SIEM and, if not, with which log management systems they integrate.

Integration with an ever-increasing array of network devices is a common theme among SIEM providers and users – as well it should be, says Gartner's Nicolett. "We have companies that are three-plus years into this, and they're still expanding the scope. That's a sensible way to tackle this," he says.

Sustaining the effort makes the difference between good and great, he adds. "It's a basic decision that a company makes. If it is just interested in solving the compliance issue, it basically stops expanding the leverage of the technology and doesn't get the full benefit from it – and mostly it's a security benefit. Security benefits accrue for companies that keep moving forward with it after the initial install."

And companies should not expect to reap cost-savings out of those efforts, Nicolett notes. It's not possible to justify the technology on potential cost reductions. What he tells clients instead is this: "If you don't have the technology in place, then you're flying blind and you don't know what's happening in your environment. This technology represents work that has not yet been done. You install the technology, and if you're using it properly, you'll discover issues that were unknown to you. When those issues are discovered, you'll have to do some project work to resolve them. So this is not about cost-reduction. It's an improve-your-security-capabilities type of technology."

As Bejtlich says, "Before SIEM, we had terabytes of logs available, but we weren't really actively doing anything with them. Once we put in SIEM, not only did those become available for searching, but SIEM goes through and finds things we didn't know were there – and that's what it's all about. There's just no way a human can do that." ■

What's next for the SIEM market?

Business analytics must become part and parcel of next-generation security information and event management, experts say. Beth Schultz reports.

Expectations surrounding security information and event management (SIEM) technology have always been grand. After all, what enterprise IT security executive could resist the thought of gaining visibility across all security domains – application, database and network?

As much frustration as this ambitious SIEM vision has fostered, however, industry watchers and participants still expect big things of the technology in the future.

"The future SIEM will have to be able to find, in real time, the needle-in-the-haystack security event out of a pool of hundreds of thousands of events per second and, at the same time, be able to run a query over terabytes of data and deliver results in a matter of seconds or minutes, not hours," says Jon Oltsik, principal analyst with Enterprise Strategy Group, based in Milford, Mass.

That's a tall order, indeed, he says. But several trends inside and outside the SIEM arena will ease the way to that inevitably, he adds. For one, the intelligence associated with event filtering and correlation from multiple data sources is continuing to improve. Ultimately, Oltsik says, the data collection and storage processing part of SIEM will go away and instead be handled by a log management tier.

Secondly, SIEM tools will become better and better at doing complex queries for investigations, forensics and analysis, he says.

The BNY Mellon, a leading asset management and securities services company based in New York, could use just such improvements, says Daniel Conroy, managing director of

29%

of enterprises reported attacks have increased in the last 12 months

– Symantec, 2010 State of Enterprise Security study

information technology at the firm. "You're always going to have a certain noise level across the network, but no SIEM platform today really provides an understanding of that activity and its spikes," he says.

What he hopes for in all SIEM technologies is trending and behavior analysis. Say, for example, a database administrator logs in at 4 p.m. till 4 p.m. the next day, and all of a sudden at 2 a.m., activity under his account begins happening.

"The technology should be able to detect that as unusual based on trending of people with that sort of data linked to the IP address and user account information," says Conroy. "That's where we're going to have to be in two or three years. We need that type of behavior analysis built into these toolsets."

For now, security analysts must scour log data and search for indicators. "But these are mathematical patterns that should be built into the toolsets," Conroy adds.

With the continual improvements in processing, such goals should be attainable, Oltsik says. "It's certainly possible, but it will take focus. Some of the legacy SIEM folks may not be able to manage through the changes as we move from data collection and all-in-one packaging for security and compliance to really deep event detection and analysis skills." ■

For more information, please contact Illena Armstrong, editor-in-chief, SC Magazine, *at illena.armstrong@haymarketmedia.com.*

SPONSORS

Tripwire

Headquartered in Portland, Ore., Tripwire has operations in 15 countries around the world. Tripwire's powerful IT security and compliance automation solutions help businesses and government agencies take control of their entire IT infrastructure.
For more information, visit www.tripwire.com.

LogRhythm

LogRhythm provides enterprise-class log management and SIEM 2.0 solutions that empower organizations to comply with regulations, secure their networks and optimize IT operations. LogRhythm's rapidly growing customer base includes Fortune 500 corporations and mid-sized enterprises spanning a variety of industries, including retail, financial services, utilities, health care and higher education, as well as military and civilian government agencies and MSSPs.
For more information, visit www.logrhythm.com.

ArcSight

ArcSight 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 cyberthreats 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 cybertheft, cyberfraud, cyberwarfare and cyberespionage.
For more information, visit www.arcsight.com.

NitroSecurity

NitroSecurity is the leader in high-performance, content-aware security information and compliance management solutions. NitroSecurity's integrated solutions provide "single pane of glass" visibility into events and logs and monitor networks, databases and application payload information. Utilizing the industry's fastest analytical tools, NitroSecurity identifies, correlates and remediates threats in minutes instead of hours.
For more information, visit www.nitrosecurity.com.

TriGeo Network Security

TriGeo Network Security delivers enterprise security information and event management designed specifically for the mid-market. TriGeo combines real-time log management, event correlation and end-point security with unique active response technology. This award-winning product delivers an "audit-proven" compliance solution that meets security requirements imposed by PCI, *GLBA*, *HIPAA* and more.
For more information, visit www.trigeo.com.

tripwire TAKE CONTROL.

tripwire LOG CENTER

Take Control with Tripwire Log Center

Tripwire Log Center offers next-generation SIEM—log and event management designed and built in a single solution without the complexity and bloat of traditional SIEM solutions. Tripwire Log Center offers:

Log Management Capabilities
- High-speed log archiving
- Google-like log indexing
- Fast log data searching
- Intelligent reporting

Event Management Capabilities
- Visibility to events of interest
- Structured data for data correlation
- Threat pattern identification with data visualization
- Complex reporting of correlated data

Customer quote:

Terremark Worldwide Inc.

At Terremark, we needed a single, intelligent solution that could manage massive amounts of logs from multiple customers, servers and security devices and from locations all around the world. We needed to analyze this activity in real time and report and act upon events of interest.

With Tripwire Log Center, we have a central console from which we can quickly take action on the suspicious activity: We find the important needle for our clients among the many massive haystacks of possible suspicious needles.

Pete Nicoletti
Vice President of Security Engineering
Terremark

Next-generation Security Information and Event Management (SIEM)

The number of annual security incidents continues to rise and hackers continue to get more sophisticated. Yet the average breach-to-detection gap is weeks to months. As IT infrastructure increases in complexity, with virtual infrastructure and more servers, devices and applications, IT faces a seemingly impossible task of identifying just what went wrong. Did the attack come from outside, or did the security hole open as a result of an internal change? How do we fix it? Does it impact our compliance status with PCI, NERC or other critical regulations or standards?

Tripwire VIA Solutions
Ideally, nothing goes wrong. But for that to happen, IT needs increased visibility to the entire IT infrastructure, intelligence to make better decisions faster, and automation to reduce the IT workload and error associated with repetitive, manual tasks. IT needs the Tripwire® VIA™ suite of solutions.

Tripwire, the leading provider of IT security and compliance automation solutions, has helped over 7,000 organizations worldwide meet their IT security and compliance needs. Tripwire has done this with its growing suite of Tripwire VIA solutions, which include Tripwire Log Center, a complete log and event management solution, and Tripwire Enterprise, the industry-recognized solution for configuration control.

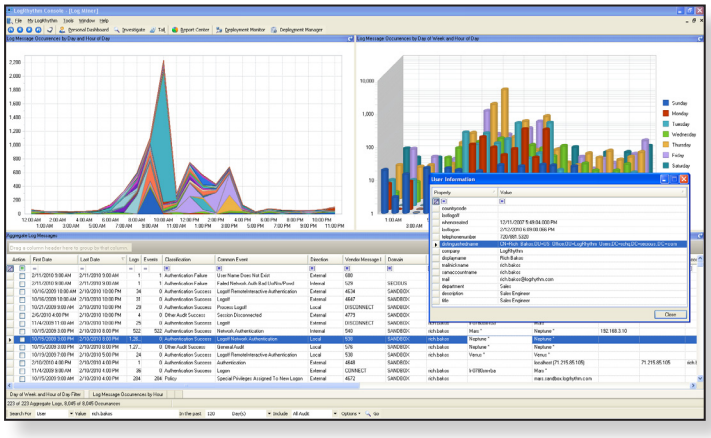
A New Approach to SIEM
Traditional log and event management solutions were either originally built to address log management or security event management, but not both. To offer a more complete SIEM solution, these traditional solutions later added the other component. On paper, these SIEM solutions look complete, but in reality, one half of the solution never measures up.

Complete Visibility and Control with Tripwire
Tripwire Log Center also integrates with Tripwire Enterprise, providing total visibility to all events of interest, including log and change events. The result? Tripwire VIA solutions reduce the breach-to-detection gap from weeks or months to just minutes. So when something does go wrong, IT has what it needs to take control—immediately.

PRIVILEGED USER MONITORING

AN EFFECTIVE APPROACH USING SIEM 2.0

When it comes to protecting a network from insider threats, organizations need to be able to keep a watchful eye on privileged users. This includes systems and networks administrators with the ability to create and modify permissions, privileges and access to any device, as well as business users with extended access to confidential data.



The challenge is finding a way to effectively and independently monitor and audit the activities of privileged users to detect malicious and/or anomalous use of privileged credentials as well as demonstrate segregation of duties through impartial observation.

LogRhythm's SIEM 2.0 technology, delivering comprehensive, integrated log and event management, file integrity monitoring, and network and user monitoring, provides enterprise customers with maximum functionality while monitoring the activities of privileged users.

	Watching the Watchers	Securing the Bread Crumbs	Finding the Needle
CHALLENGE	Because they are the only people with access to the information, privileged users are most often the group that is tasked with providing information on privileged user actions and behavior patterns.	Many privileged users have permissions that not only give them access to data recording user activity, they also have the means to change that data and hide activity.	Even with the means to access recorded data on privileged user activity, that activity can be enterprise-wide. Identifying significant events among a lot of recorded activity across a large number of data sources is incredibly time consuming and leaves a lot of room for human error.
SOLUTION	LogRhythm's automated, centralized, and secure collection of log data provides independent access to privileged user activity logs without relying on the privileged user for collection.	Immediate collection by LogRhythm with cryptographic hashing provides a digital chain-of-custody that eliminates the ability for privileged users to tamper with activity records and conceal nefarious activity.	LogRhythm has Quick Search capabilities for rapid, user-level investigations, displays aggregate and trending visualization to identify behavior-based patterns, and provides automated alerting on specific privileged user activity.
BENEFIT	Using the Alarming tool, LogRhythm users can set up alerts to send out notifications any time a privileged user account is added or modified, including information about who created the account. And, because these alerts are automated, they are not initiated by a privileged user, maintaining segregation of duties.	LogRhythm's Second Look archive restoration wizard allows administrators to immediately query against any archived data, which is automatically validated to maintain the digital chain-of-custody, making it ideal for compliance purposes.	LogRhythm users can quickly Investigate on all activity performed by a newly created user, using a combination of detailed forensic views and interactive graphical analyses. A simple, wizard-based GUI makes investigations quick-to-run and easy to save for future use.

"Powerful product with plenty of easy-to-use features, this one is our Best Buy."

SC MAGAZINE BEST BUY

READER TRUST AWARD
"Best SIEM"
INNOVATOR OF THE YEAR

OVERALL RATING
★★★★★

LogRhythm
COMPLY SECURE OPTIMIZE

LogRhythm provides enterprise-class Log Management and SIEM 2.0 solutions that empower organizations to comply with regulations, secure their networks, and optimize IT operations. LogRhythm's rapidly growing customer base includes Fortune 500 corporations and mid-size enterprises spanning a variety of industries including retail, financial services, utilities, healthcare, and higher education, as well as military and civilian government agencies and managed security service providers.

See an in-depth, self-paced demo of LogRhythm given by Chris Petersen, Co-Founder & CTO.

Customer Case Study:

IWCO Direct

"ArcSight Express is very intuitive and easy to use. It is a perfect fit for the size and scope of our business and has allowed us to expand into new markets."

– Chris Van Houtte, Vice President of Information Technology, IWCO Direct

Impact Highlights:

- IWCO Direct is able to quickly analyze log data and conduct forensic investigations if and when an incident arises
- ArcSight Express enhances security by providing IWCO Direct with greater control over its own policies and procedures
- With ArcSight Express, IWCO Direct has been better able to expand their customer base and stay competitive

About ArcSight:

ArcSight (NASDAQ: ARST) is a leading global provider of security and compliance management solutions that protect businesses and government agencies. For more information, visit www.arcsight.com.

IWCO Direct's Challenge

While security has always been important to IWCO Direct, the company did not have an efficient way to analyze event data or conduct forensic investigations if and when an incident arose. For instance, if a piece of customer data was altered somewhere along the line, IWCO Direct would want to see where the information was changed and who touched it last. "If something were to occur, it might have taken us weeks to sift through the data, with the possibility of not being able to conduct the investigation at all," says Chris Van Houtte, Vice President of Information Technology at IWCO Direct.

The ArcSight Solution

With ArcSight Express, IWCO Direct is able to make full use of its log data and ensure the highest level of security for its customers. ArcSight Express provides the company with the ability to correlate events across multiple systems and automatically generate security alerts for any suspicious activity.

IWCO Direct has also been able to take full advantage of ArcSight Express without stretching their resources. They were especially impressed with the ease of use of the product, and how simple the graphical user interface is to navigate. If a troubling event or alert pops up on the screen, they can drill down and investigate the issue with a single click.

ArcSight Express is also providing IWCO Direct with greater control and accountability over its own security policies. Soon after ArcSight Express was implemented, the system alerted Van Houtte to a policy violation: a new employee was adding people to an Active Directory involving a critical asset without management approval. "We started receiving emails in plain English explaining the problem," explains Van Houtte. "That's when we realized we could use ArcSight Express to make sure all of our policies and procedures are enforced. As a result, we've greatly enhanced our own security posture."

Learn more about the market-leading SIEM platform for cybersecurity and compliance monitoring.

Download now:

- *Demonstrating the ROI for SIEM: Tales from the Trenches*
- IWCO Direct full case study

ArcSight Headquarters: 1-888-415-ARST

The Emergence of Content Aware SIEM

Content Aware SIEM represents a new generation of Security Information and Event Management (SIEM) capabilities that extend the value and benefits of SIEM by providing visibility into the contents of applications, documents and protocols. Without content awareness, SIEM is only able to act upon the surface details provided by event logs. This limits the effectiveness of key SIEM functionalities—including threat detection, incident response, and compliance reporting—because the data being used for analysis lacks sufficient context and content to make informed, relevant decisions.

As a result, SIEM systems have started to evolve, adding context information from add-on systems such as Identity Management, Vulnerability Assessment, Configuration Management systems, and others to enhance the security events collected and correlated by the SIEM. While these systems provide a great deal of value to SIEM, the events themselves are still myopic, limited to the summary data provided by the source log files.

What is Content?

We define content as it relates to SIEM as the payload of an application, i.e., what is actually being communicated, transferred, and shared over the network. Logs describe the fact that an activity has taken place on a system or network. Content is what defines the actual nature of the activity: email contents, including attachments, social network communication, document contents, and database queries and the size and/or subject matter of their responses. Learning these details becomes more important as threats become more complex and as they "move up the stack," exploiting vulnerabilities at the application and session layers as well as business logic flaws.

Content Aware Correlation

This content data can be analyzed using Content Aware SIEM. In addition to correlating, summarizing, filtering and reporting on events, we can now also filter email contents, correlate SQL keywords with others information and perform other analysis tasks.

Examples of how content data can add value to correlation rules are shown below:

- **Event correlation rule:** if 1,000 emails originating from within the company are sent, raise an alert "anomalous email activity."
- **Content rule:** if 1,000 emails originating from a non-SMTP host within the company, with a 'reply to' address in an outside domain, are sent to 1,000 unique addresses with the words 'account' and 'password' in the body of the email, raise a critical alert "possible spam bot," with maximum severity.

Such rules allow much more comprehensive security monitoring, compared to current SIEMs. This level of visibility also brings us one step closer to a true "single pane of glass" CISO dashboard, where the views can include the actual contents of network communication and application activity, adding new tools to the arsenal of a SOC analyst, security manager and CSO.

Performance Considerations

However, by extending visibility into the actual payload of applications and protocols on the network, this generates a massive increase in event load translating directly to a performance impact on current SIEMs. Query responses from most SQL-based data stores begin to slow rapidly after just a few million rows of stored data, and content information can quickly generate billions of rows. Even with highly optimized databases or flat-file data stores, current systems lack the scale and performance to deliver the real-time results needed to be valuable as rapid response operations systems.

Only SIEM tools built from the start to handle massive volumes of diverse data, logs and content, can evolve to the next level, and become Content Aware. Luckily, while content awareness represents architectural challenges to most SIEM platforms, it is a technology that is available today. NitroSecurity's NitroView Enterprise Security Manager — which was built from the start on a patented, high performance database architecture designed to handle massive volumes of diverse data, logs and content — is the first commercially available Content Aware SIEM.

TriGeo®
Network Security

REAL-TIME LOG ANALYSIS - WHY SETTLE FOR JUST FORENSICS?

"The recent intrusions...are a wake-up call to those who have not taken this problem seriously. New cyber security approaches must continually be developed, tested, and implemented to respond to new threat technologies and strategies" - Dennis C. Blair, Director of National Intelligence 2/2/10

Real-Time Log Analysis for Proactive Network Defense

Logs have to be analyzed. Regulations such as PCI, HIPAA, NERC CIP, SOX and GLBA require it, but let's face it - traditional log analysis is **reactive**. You have a choice: You can pick a product that is ***forensically focused***: gathering logs, storing them in a database and offering search and reporting, **OR** you can choose TriGeo SIM.

TriGeo SIM is the ONLY log analysis solution that combines real-time log analysis with active response for true Proactive Network Defense.

Real-time, in memory, analysis is the key. TriGeo's enterprise-wide view of the network makes it possible to capture, correlate and actively respond to network attacks and insider threats - at network speed.

For proactive network defense, there is only one choice.

GET TRIGEO. GAIN VISIBILITY.™

SC MAGAZINE AWARDS 2007 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2008 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2009 WINNER Honored in the U.S.

Seeing is believing...

Find out why this award-winning technology is so highly rated by reviewers and loved by customers.

Join us for a live webinar where you'll see TriGeo SIM in action under real-world conditions. Watch as we capture, correlate and respond to network attacks and policy violations - all in real-time. Register today at www.TriGeo.com or call 1-866-664-9292.

Come see us @ RSA Booth #817 and Interop Booth #715