The state of SIEM

Implementing a SIEM takes planning, but the rewards can make the tool worthwhile.

ebook

An SC Magazine publication

The state of SIEM

The technology is capable of providing all of the data organizations need for compliance, but managing the log activity to make sense of it can be a challenge, reports Alan R. Earls.

Used to collect, aggregate and correlate log data for analysis and reporting, security incident and event management tools (SIEMs) are today's must-have security product, say a number of industry observers. But the fact that SIEM solutions are a combination of once distinct product categories – namely SIM (security information management) and SEM (security event management) – is important to both selection and implementation.

Modern SIEM technology can deliver real-time analysis of security alerts generated by network hardware and applications, and it is also used to log security data and generate reports for compliance requirements. Determining what SIEM solution to deploy, and how, isn't a trivial task. In fact, it can often be complex and require considerable research and planning. Still, those who have put the tool to use say the advantages of getting modern SIEM technology in place compensates for the effort.

> "You must have logs and the ability to bring them together."
>
> – Charles Kolodgy, research vice president at IDC

C. Matthew Curtin, a computer scientist, litigation consultant and founder of Interhack, a Columbus, Ohio-based consulting firm, says organizations always need to remember the context in which they're operating and ensure that they understand the requirements of their business from beginning to end. "SIEMs can be very helpful for the purpose of identifying and correlating activity," he says. "By their nature, they can identify high-impact events that demand responses that are more than technical in nature."

For example, a report from a computer system is typically insufficient in assessing security incidents. "How do we know that the SIEM isn't issuing a false alarm?" he says. "Getting to the original log data with the ability to show what was happening is critical."

But, before one thinks about purchasing something, it helps to have a clearly defined purpose behind adopting SIEM, says Charles Kolodgy, a research vice president in the security products services department of Framingham, Mass.-based IDC, a global advisory services firm. For most organizations, he says, that means compliance.

"If that is your general purpose, you want to see what kind of reporting you need and whether the tool you are considering will make it easy to report and combine materials," he says. Ease of use and how much data can be easily imported into reports are important considerations.

On the other hand, he says, if one is looking at SIEM purely from the standpoint of enhancing security, customers may want to make sure it covers all the log and security product types with which they work. That's because most SIEM solutions will have, or will need, connectors to help receive and integrate data, Kolodgy says.

In fact, he says there are a wide range of security devices, logs, identities and applications – all of which need to be integrated in order to provide a full picture. "The big term that is coming into vogue is 'situational awareness,'" says Kolodgy. But that concept builds on analytics and fundamentals, like log management.

"You must have logs and the ability to bring them together in order to implement a SIEM," he says. "That is why so many SIEM vendors have log management as one of the first things included in their product."

Choosing among SIEM products isn't

98%

of data breaches in 2011 were instigated by external agents.

– Verizon "2012 Data Breach Investigations Report"

SIEM: Bank on it

Pete Boergermann has come to depend on SIEM and, he says, there is no going back.

"We do a lot of IT work ourselves," says Boergermann, the IT security officer for Citizens & Northern Bank, a community institution in Pennsylania with 26 branches and 1.3 million customers. One recent project was helping the company deploy a basic SIEM product that provides log management and other security functions. Boergermann says the IT staff has come to rely heavily on the tool to help identify and corral malware attacks and to maintain compliance. Using the tool, Citizens & Northern is able to review its logs faithfully and has become more cognizant of actual and potential security issues, he says.

The SIEM pulls log data automatically from across the organization. "The fact that it does it automatically is a huge help and a great time saving," says Boergermann.

The bank's SIEM tool is accessible through a web interface, from which queries can be initiated and reports run. "We have automated logging set up now so that when certain kinds of things happen in the system, we get an email – we don't have to go look," says Boergermann. In particular, due to *Sarbanes-Oxley* requirements, the company has to monitor virtual private network (VPN) connections to vendors and maintain an awareness of what they are doing. "The tool helps us to do that," he says.

Even comparatively routine issues can be helped by a SIEM, says Boergermann. "We recently discovered that a router in one of our locations was misconfigured and that generated an alert, allowing us to fix the problem before anything bad happened," he says.

Boergermann says that to select a SIEM that is the right fit, it helps to get as much information as possible from the web about competing products and then set guidelines early on for what features and capabilities one thinks will be needed.

"I was looking for a tool that was more of an appliance," Boergermann says. "I didn't want to manage another service. I wanted something that would work with multiple vendors and hardware. Other considerations included trying to find low maintenance costs and ease of use. In fact, for Citizens & Northern, initial costs turned out to be higher than expected, but ongoing costs were lower."

Boergermann says another good starting point for those seeking a SIEM solution is to consider the regulations and other issues that govern one's industry and determine through a discussion with auditors and examiners what they really mean in practice. Only then can one try to find a way to have a SIEM tool automate as many tasks as possible.

"If the regulations require you to monitor all your VPN connections, find a tool that will make that simple," says Boergermann.

easy, so Kolodgy recommends developing well-thought-out and clear selection criteria. "SIEM is one of those things that would be hard to bring into your lab and test," he says. However, if the organization is large enough, it might be able to set up spaces in different locales and evaluate the data-gathering capabilities. No matter what the other criteria, Kolodgy recommends making sure a SIEM tool can provide a clear, centralized view of the organization's security situation.

But, he adds, even with a selection based on well-defined criteria, don't expect SIEM to be trouble free. "One of the big problems with SIEM tools is false positives," says Kolodgy. SIEM systems can provide too much information, making search-and-filtering functions especially valuable. Beyond those technical is-

81%

of data breaches in 2011 used some form of hacking.

– Verizon "2012 Data Breach Investigations Report"

sues, Kolodgy says the biggest challenge with SIEM is its cost of implementation. "There is a large services component involved, and to move ahead, one needs to develop a good understanding of what the total cost will be. That means the software and hardware component, as well as the professional services needed to get it set up," he says.

To make sure one gets a product that is a good fit, Kolodgy recommends obtaining a vendor's customer list and then contacting someone in one of those organizations who can provide objective feedback about cost, ease of use and effectiveness.

Watch for implementation challenges

John Verry, principal enterprise security consultant at Pivot Point Security, a Hamilton, N.J.-based security assessment firm, cautions that even with all their seductive bells and whistles, many SIEM implementations fail to achieve their objectives. One challenge can be the high levels of events-per-second (EPS) generated across the infrastructure that can overwhelm a SIEM's capabilities.

> "...developing good requirements definitions helps one see where one needs to be..."
>
> *– John Verry, principal enterprise security consultant at Pivot Point Security*

SIEM and traditional log management overlap, says Verry. SIEM solutions tend to write that kind of information into databases and the databases sometimes aren't adequately architected to handle those kinds of transaction rates. "If you have an issue with SIEM, whether or not it is a database issue, the challenge is catching back up [with that data rate]," he says.

However, a positive development over the last few years has been the movement of SIEM vendors toward adding log consolidation into their capabilities, Verry says. These work seamlessly with the SIEM and help digest events on the edge of the enterprise so that only key incidents filter up to the central SIEM itself. "It puts one in a better position to handle higher and higher data levels – like 750 million events a day," he says. If one's requirement is just to be able to do compliance reporting, onemay opt for log consolidation alone because it will prove to the auditor that logs are kept, and user accounts are rotated at a certain frequency, he says.

There are dozens of major SIEM players with few differences in core functionality, says Verry. The key differences may just be related to specific features that fit one's needs. He says another unique capability available with some SIEMs is increasing integration with other critical sources of data in the environment.

For example, if someone tries to access files by account group, that might prompt an alert, but it could also trigger an action to allow or prevent access, he says. Then, if the SIEM tool sees some kind of pattern it didn't approve of, it might deprovision. "Those more advanced, high-end features are unique to the SIEM world," says Verry. "That is where differences in developing good requirements definitions helps one see where one needs to be relative to sophisticated SIEM or just log-based tools."

Another strategy Verry recommends is the consolidation box, a custom, flat-file-based database designed to handle high event rates. The information these gather can then be forwarded back to a SIEM console. The idea, he says, is to keep the event rate at the main SIEM console to manageable levels, namely "under a few thousand events per second." Using a consolidation box approach, one can still handle massive event rates across an enterprise-class infrastructure. "A consolidation box is more relevant to compliance, but may not be so relevant to security incident detection," he says. However, he adds, "If I were a big company, in every data center I would set

94%

of all data compromised in 2011 involved servers.

– Verizon "2012 Data Breach Investigations Report"

Drill down: The technology

Some of the specific features and functionality in SIEM solutions can be worth understanding in more detail. Based on feedback from technical end-users, some SIEM systems do not provide robust and full-featured ticketing systems, says Bob Dooling, an independent consultant at Dooling Information Security Defenders, based in Austin, Texas.

He explains that this refers to a database that contains "tickets" or "issues" for support or for security staff to address. "In the case of SIEM, this is often issues like a desktop infected with malware, or an external attacker that should be blocked at the firewall," he says. Also, in order to facilitate efficient escalation of alerts, as well as automated emailing and content pushes to the customer portal, ticketing systems should integrate with a contact directory, backend email server and – in the case of a managed security service provider – a customer web portal. "Integration with external software may be necessary," Dooling says. "Check which third-party software is supported to avoid disappointment."

He says the ability to view full, raw-packet data for security incidents being investigated is crucial to make an informed assessment of an incident. This might include a valid-versus-false positive alert, a successful exploit versus a failed attempt or data exfiltration versus simple adware infection. Dooling says this can be an important differentiator, since not all SIEM products provide this functionality.

"The ability to view the alert history for an internal system allows analysts to easily profile and determine the role of the system on the network," he says.

If someone expects to install a SIEM and immediately begin reaping benefits in the form of valuable output, they will likely be disappointed, he says. That's because SIEM installations require a significant amount of tuning, network-specific configuration and, often, customized correlation rules, he says.

"Customers are interested in pulling logs into their SIEM from a surprising variety of log sources, including products and applications not supported by the SIEM vendor," says Dooling. These include non-security related (or indirectly related) applications. Whereas SIEM vendors tend to focus on supporting traditional, widely used security devices – such as firewalls, intrusion detection system (IDS), proxy servers and more – Dooling says he's worked with customers to integrate credit card processing application and enterprise resource planning (ERP) system logs.

"It seems that these customers use SIEM to provide home-grown IDS-like functionality for applications for which traditional firewalls and IDS do not exist," he says. "Although not taking advantage of some of the primary benefits of SIEM (normalization, correlation), this seems like a valuable use of the log collection and flexible alert-generation technologies."

up a consolidation box."

While Verry describes himself as a SIEM fan, he acknowledges that more than a few deployments have fallen short of people's expectations. He says that having a hierarchical-implementation approach offers the potential to solve a lot of problems in small and midsize environments. But, in large, enterprise-scale organizations, there will be thousands of entities producing security-relevant information.

"What we are finding in a lot of organizations is, in the initial excitement, people try to get all data into the system and only then

97%

of breaches in 2011 were avoidable through simple or intermediate controls.

– Verizon "2012 Data Breach Investigations Report"

figure out what to do with it," says Verry. "They turn SIEM into a consolidation project." And, he adds, one must consider the fact that an organization might have 20 different kinds of event sources – from different devices – and for each one, an agent with logic must be deployed. Then, those need to normalize and consolidate. "It can be a daunting undertaking and one may want to consider which elements are really important to the environment," he says.

> "...get reports and build a whole solution stack..."
>
> *– John Verry, principal enterprise security consultant at Pivot Point Security*

Verry recommend a point-specific approach. "Take a pain point, like a particular payment program," he says. From that starting point, determine all the logs that are relevant and then build a solution stack. "Get logs collected and normalized, and establish alerting and correlation rules or anomaly detection rules. Then, make sure you get reports and build a whole solution stack that reveals the wonderfulness of SIEM. Then use that as a template for the next point problem and then iterate through other problems," he says.

With that change in approach, one ends up in a situation where momentum builds, and users don't end up with limitless log consolidation, so people lose confidence in the effort. Instead, the user gets quick wins and moves to the next pain point. "The successful projects take that kind of approach, the less successful ones start with *all* the data," he says.

Most organizations don't do a good enough job on the requirements definition around SIEM, Verry says. "Most documentation is insufficient to differentiate major vendors. So, any vendor would work, not because they truly meet requirements, but because the organization didn't adequately define the requirements."

For instance, he says, organizations often fail to develop a list of all devices that need to be included or establish how many events per second they will need to handle. "Most organizations have no idea, and not knowing means one doesn't really know how to architect a solution," he says. What's more, even when organizations manage to cover those bases adequately, they often neglect to plan for incidents, such as a potential malware outbreak, which could raise normal traffic by 30 percent, he adds.

Consider staffing issues

What's involved in keeping a SIEM tool working effectively? Although it might only require one person to run a SIEM, to do it well requires multiple skill sets, says Verry. "SIEM is a database sitting on a data mart, so you need someone with database administrator (DBA) skills, but you also need network architecture skills to understand the environment," he says. "And to make sure the data is getting to the SIEM, one may need the skills of a programmer – someone who is comfortable working in scripting languages – and maybe even the skills of an auditor who can look at standards adherence. One probably needs a half-dozen part-time skill sets because one never sees all those capabilities in one individual."

Beyond getting the technology right, Verry says organizations need to plan how they will operationalize the information a SIEM is supposed to deliver. "The challenge is when you turn on the SIEM and it tells you that a server is compromised. Then what do you do?" he says. The answer is to make sure that SIEM information is operationalized into a response mechanism and is segregated and classified, he says.

One of the reasons SIEMs fail is because people don't understand the commitment involved, he says. "Businesses allocate capital for projects like SIEM, but not the money for

96%

of data breach victims in 2011 subject to PCI DSS had not achieved compliance.

– Verizon "2012 Data Breach Investigations Report"

the long-term attention," Verry says. SIEM tools need a lot of care and feeding so they are in sync with changes in operating systems, firewall settings, IP addresses and all the other factors that contribute to their effectiveness.

"I'm not advocating selecting a SIEM with less functionality, but one should prioritize what one wants to do because a lot of companies don't get their money's worth," says Graham Logsdon, deputy chief technology officer of global security solutions at Computer Sciences Corp. (CSC), a Falls Church, Va.-based firm that develops technology-enabled solutions. Indeed, many companies may find they just need basic log correlation or rudimentary forensic analysis to start, he says.

However, Logsdon says that what he often sees is his customers select a rich platform and packages that have diverse functionality – with all the connectors built in for any type of device or log source – and then not really put them to use.

"What we typically see is every major organization employing SIEM in some form or fashion," says Logsdon. "The question is how much do they truly use it." Frequently, when his company is asked to help support SIEM, it finds the customer organization is using less than half of the product's capabilities and perhaps not even collecting events. The reason for that state of affairs is resources, or the lack thereof, he says. "Effective use of SIEM is a 24/7 activity, but as so often happens, the staff time available isn't always enough," he says. "When one considers implementing a SIEM, if it will only get limited use, look particularly at ease of deployment and how many prebuilt connectors and reports are available."

In fact, what Logsdon has found is that many SIEMs are used to run only two or three reports. On the other hand, organizations with complex infrastructure and challenging security requirements may actually need the "biggest, baddest SIEM you can find." Those systems must handle high levels of events per second, potentially across thousands of devices.

Logsdon says that aside from purchasing the SIEM itself, implementation makes only moderate infrastructure demands. "It depends on what you want to do, but you could certainly run a SIEM with just a basic 'Wintel' box," he says. However, in a larger enterprise, one might need to invest in some dedicated storage. ■

For more information about ebooks from SC Magazine, *please contact Illena Armstrong, VP, editorial director, at illena.armstrong@haymarketmedia.com.*

55%

of all hacking intrusions are done through exploitation of default or guessable credentials.

– Verizon "2012 Data Breach Investigations Report"

Sponsors

HP Enterprise Security

HP Enterprise Security is a leading provider of security and compliance solutions for modern enterprises that want to mitigate risk in their hybrid environments and defend against advanced threats. Based on market-leading products from ArcSight, Fortify and TippingPoint, the HP Security Intelligence and Risk Management (SIRM) Platform uniquely delivers the advanced correlation, application protection and network defense technology to protect today's applications and IT infrastructures from sophisticated cyber threats.
For more information, visit hpenterprisesecurity.com.

nitrosecurity

now part of McAfee

McAfee, a wholly owned subsidiary of Intel, is the world's largest dedicated security technology company. Backed by global threat intelligence, its solutions empower home users and organizations by enabling them to safely connect to and use the internet, prove compliance, protect data, prevent disruptions, identify vulnerabilities and monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep its customers safe.
For more information, visit mcafee.com.

Q1 Labs

Total Security Intelligence | An IBM Company

Q1 Labs, an IBM company, is a global provider of high-value, cost-effective next-generation security intelligence products. The company's flagship product, the QRadar Security Intelligence Platform, integrates previously disparate functions – including SIEM, risk and log management, network behavior analytics and security event management – into a total security intelligence solution, making it the most intelligent, integrated and automated security intelligence solution available.
For more information, visit q1labs.com.

Masthead

EDITORIAL
VP, EDITORIAL DIRECTOR Illena Armstrong
illena.armstrong@haymarketmedia.com
EXECUTIVE EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
DESIGN AND PRODUCTION
ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com
PRODUCTION MANAGER Krassi Varbanov
krassi.varbanov@haymarketmedia.com

U.S. SALES
VP, SALES DIRECTOR David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
EASTERN REGION SALES MANAGER Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WESTERN REGION SALES MANAGER Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*
ACCOUNT EXECUTIVE Dennis Koster
(646) 638-6019 *dennis.koster@haymarketmedia.com*
SALES/EDITORIAL ASSISTANT Roo Howar
(646) 638-6104 *roo.howar@haymarketmedia.com*

IF YOU WERE BREACHED, WOULD YOU KNOW?

HP Security Information and Event Management (SIEM) is the market leading solution that provides organizations with an increased visibility of cyber threats and risks.

For more information go to www.hpenterprisesecurity.com.

ENTERPRISE SECURITY

CONNECTED SECURITY IS SMARTER SECURITY

Security is no longer about where. It's about everywhere. So that's exactly where McAfee focuses its efforts.

The Security Connected framework from McAfee provides a seamless integration of solutions, services, and partnerships that intelligently reduces overall risk.

And with our recent acquisition of NitroSecurity, organizations now have even greater visibility into potential insider threats across their entire organization.

With unmatched brainpower and unmatched obsession, we build global connected solutions that deliver smarter security. On every device, every network, everywhere.

SAFE NEVER SLEEPS.

McAfee®
An Intel Company

OPEN YOUR EYES TO POTENTIAL THREATS

There's a lot going on across your network that **you're simply not seeing.**

Targeted attacks. Insider fraud. Unauthorized configuration changes.

It's time to upgrade to ***Total Security Intelligence*** with a next-generation SIEM from Q1 Labs:

- **Gain greater visibility** with automated correlation and anomaly detection of all user, server and network activity (including Application Layer visibility via deep packet inspection).
- **Rapidly deploy** -- without adding headcount -- through security analytics, auto-discovery and pre-built rules and compliance reports.
- **Scale to the largest and most diverse environments** with a single unified architecture for SIEM, log management, configuration and vulnerability management, and network behavior analytics for virtual and physical infrastructures.

Predict Risk | Detect Threats | Exceed Compliance Mandates | Improve Operating Efficiency

Q1 Labs®
Total Security Intelligence | An IBM Company

Q1Labs.com

Visit Q1Labs.com/SIEM2/SCMag.aspx
to Download a technical white paper
and learn if it's time to replace your SIEM