Separating the important alerts from all the noise is of paramount importance.
SIEM

SIEM is a complex application that needs highly trained technicians to configure the system and then make sure the output is read correctly. Stephen Lawton reports.

Generally speaking, when a breach occurs, evidence is buried somewhere in the log files of the various systems. The challenge CISOs face is finding the right entry in the appropriate log so that the vulnerability can be remediated, which is why log management and analysis is considered one of the cornerstones of information security best practices.

Life would be much easier for security teams if log files could flash an alert that says, “The system has a problem here.” However, in reality for most enterprises the amount of data contained in logs can be massive, especially when the operating system, applications, network devices, storage devices, servers and workstations all are generating multiple log files concurrently. It is not uncommon for IT departments to be dealing with millions of log entries daily, so learning how to separate the few really important alerts from all the noise becomes of paramount importance.

Large enterprises often rely on security information and event management (SIEM) software to collect logs, analyze them and identify events that require additional investigation. In a perfect world, SIEM might seem like a panacea for managing massive log files and related data feeds. Unfortunately, IT rarely resides in a perfect world.

Large enterprises and smaller firms that are required to meet various governmental and industry regulations often end up spending large sums on SIEM implementations that, depending on the company, could well turn out to be a complete boondoggle, says Ondrej Krehel, managing director and founder of LIFARS, a New York-based digital forensic and cybersecurity intelligence firm.

Many companies spend big on software and hardware, he says, but fail to sufficiently train staff needed to manage the SIEM, which is a complex application that needs highly trained technicians to configure the system and then make sure the output is read correctly.

Often, Krehel notes, because this work might not require a full-time position, companies will assign it to lesser-trained technicians – perhaps tier 1 or tier 2 support personnel who normally are involved with password resets or SQL injections on staff – but fail to hire the high-priced and more talented tier 3 support engineer required to manage a SIEM. Instead, he says, a company might hire a part-time engineer to work on the SIEM a couple of hours a day or perhaps hire a managed security services provider (MSSP) to address the SIEM issues.

Either way, he contends, no one might be monitoring the SIEM when an alert comes through, delaying a response at best and missing it altogether at worst. In fact, the lack of spending on staff and training is the main reason why many SIEM implementations fail, he says. For every dollar a company spends on software, it will spend double that on first-year deployment costs, he estimates. After that, the ongoing costs to maintain a SIEM system will be roughly equal to the original software investment.

Jared Carstensen, CISO at CRH, a Dublin-based provider of building materials worldwide, has spent years working with SIEM in both CISO and consulting positions. “The
most notable area SIEM has transformed over the past years is a shift from the need to purchase a very costly SIEM solution, which may have been large, complex and not fit for purpose (particularly if you do not have the full time resources or functionality to take on monitoring and response 24/7), to managed services, which are now far more cost-effective and efficient in terms of resourcing and overhead,” he says.

“Companies now have the ability to focus their efforts and outsource the heavy lifting for more streamlined results,” Carstensen explains. “This represents a fundamental change and one which is welcome for those with lean security teams or tight budgets.”

However, while non-recurring costs drive up the first year’s budget for a corporate SIEM, budgets in the following years could see increases due to additional, unexpected costs for the hardware, LIFARS’s Krehel says. Additionally, companies should expect significant costs for integrating and configuring the software to make it operational.

Shortchanging configuration and implementation can result in software that is not tuned correctly and which will not return the expected results, Krehel says. Senior executives who signed off on the project will have preexisting expectations, which might not be realized if the system returns too many false positives or negatives.

Not every log management problem is best solved by SIEM, though, says Anton Chuvakin, a research vice president at Gartner, an information technology research and advisory firm headquartered in Stamford, Conn. Chuvakin, who has more than 15 years of experience focusing on SIEM, says that before a company decides to lay out $50,000 to perhaps more than $1 million, they should address four main questions:

What problems am I trying to solve? While this might seem basic, companies need to identify in advance exactly what they expect their SIEM to accomplish. Some likely will implement SIEM because they believe they need it for compliance purposes, although sometimes there are other ways to accomplish the same tasks, Chuvakin says. Trying to manage logs alone is an insufficient reason for companies to implement a SIEM. “It’s like saying I take aspirin because I have low aspirin content in my blood,” Chuvakin notes. Companies should make the business case for SIEM before authorizing a purchase.

Can SIEM do it? Just because a company has a lot of logs to analyze, that does not mean SIEM is necessarily the best tool. “Can you load the right data to solve the problems?” Chuvakin asks. Having log files alone is not sufficient if the logs do not contain the appropriate data needed to solve the problem at hand.

Is the SIEM the best way to do the task? Sometimes the data a company really needs is buried in Windows file access logs. If that is the primary reason the company is looking

$1.6B
in revenue spent on SIEM implementations in 2014.

– Gartner,
at SIEM, then SIEM might not be the best tool for the job, he notes. Instead, a data loss prevention tool might provide higher quality tactical results at a lower price point and support requirement than the SIEM.

Can I do what I need done with a SIEM? It might be that the company has identified a problem that needs addressing and a SIEM might be a valid tool to get the job done. In fact, he says, a SIEM might be the best choice of options to solve the problem, but SIEM might still be the wrong choice. Does the company have the necessary personnel to manage the application? Are all of the prerequisite security controls in place on which the SIEM relies? Does the company have the financial resources to maintain a SIEM installation? Just because SIEM can solve a problem, Chuvakin says, doesn’t necessarily mean that the potential user has the technical or financial resources and where-withal to implement SIEM.

If the company is able to answer “Yes” to the first three questions, all might not be lost. Chuvakin agrees that an MSSP might be a viable alternative, but outsourcing this service still requires that all the prerequisites are in place and the company is able to collect and filter the incoming data so that the SIEM is getting what it needs to produce the appropriate output.

Creating a budget for SIEM is no easy task, Chuvakin says. As with other mission-critical applications, the companies need to determine if a commercial off-the-shelf (COTS) SIEM is needed or if the company needs to do a lot of customization before implementation.

While open-source might seem like a cost-effective option, open source software generally requires even greater customization than COTS software. Traditional applications generally have a variety of built-in tools, dashboards and reports, he says, while open source generally requires the user to compile their own tools and develop custom reports and dashboards. While the initial cost of the software might differ, open source can end up costing significantly more to configure and require a lot more staff time. “Open source does not mean free,” Chuvakin explains.

According to the “Analysis of the Global Security Information and Event Management (SIEM) and Log Management (LM) Market,” published in April by the consulting firm Frost & Sullivan, the average annual contract (ACP) price in 2014 for SIEM/LM products was $37,000. By 2019, the firm expects the ACP to rise to slightly more than $39,000. “The comparative lack of growth in SIEM/LM average ACP is the result of an increase in smaller companies using SIEM/LM products, and persistently strong competition in the enterprise segment,” wrote Christopher Kissel, network security analyst and author of the report.

---

**SIEM installation: 12 components**
SIEM is an integrated platform with each of these components included. Each component also can be purchased as a standalone appliance.

1. Log management
2. Archives (storage)
3. Analytics (NBAD, customized)
4. Compliance reporting
5. Statistical baselining
6. Network mapping
7. Data ingestion
8. Application management
9. Single console monitoring
10. Forensics
11. Integrations with ticketing
12. Threat management

*Source: Christopher Kissel, network security analyst, Frost & Sullivan*

---

60% of enterprises will discover a breach of sensitive data in 2015.

– Forrester, “Planning For Failure, 2015”
Sometimes the best choice is not a SIEM implementation at all, says Mike Spencer, a SIEM expert and consultant at the Denver-based information security services provider Accuvant. Spencer agrees that companies first have to have the basics in place. “You don’t buy a Ferrari if you just got your learner’s permit,” he says. Before a company considers something as advanced and expensive as a SIEM, it needs to make sure that its existing tools are insufficient to get the job done.

Network behavior models are sexy sounding, but you need a baseline.”
– Mike Spencer, consultant, Accuvant

Determining whether or not to make a SIEM investment generally comes down to the security and IT teams determining what they need and comparing it to what they have. Sometimes companies look to its first SIEM implementation because it is the “bright and shiny thing,” but they soon discover that it is not the silver bullet to defending against attacks. “A lot of people get overwhelmed by SIEM,” Spencer says. “They pay a lot of money to get it installed and they want it to flash up on the screen and point to all their vulnerabilities. That’s not how it works,” he says.

Rather, he says, some companies might benefit from making better use of existing point products. For example, if a company does not have an existing policy of how it does patch management, it might benefit from creating such a program before making the leap to SIEM. “If you’re not covering the basics,” he says, “you might not need SIEM.”

You cannot buy and install a SIEM the way you do with anti-virus software, he notes. A successful SIEM installation requires a culture of security, including support from senior management. “Integrating a SIEM is not a trivial undertaking,” he says.

Further, some companies end up ripping out and replacing their SIEM if their results do not match the promises made by the software vendor’s sales team, he says. However, the problem may not be with the SIEM software at all, but rather how it was installed, configured and maintained. One of the keys to success is having an IT staff that understands the business processes of the company so that the SIEM can be tuned to provide the right information for the way that company conducts its business. If the baseline network analysis is faulty and SIEM is configured incorrectly, it could take some time to figure out why the SIEM is not producing the kind of data the IT manager expects.

“Network behavior models are sexy sounding, but you need a baseline,” Spencer says. “Let the machine learn the network and hope nothing too bad happens this week [while the machine is learning].”

The Frost report underscores Spencer’s view about how the system needs to be integrated with the overall network defenses. When SIEM is integrated with a firewall, advanced threat detection, vulnerability management, network access control, mobile device management and other platforms, “it improves the efficacy of both SIEM and the integrated platforms,” Kissel writes. “The bidirectional flow between platforms is inevitable. Pernicious attacks like zero-day threats evade detection from perimeter-based systems. However, at some point the signature ends up on the SIEM.”

LIFAR’s Krehel says that SIEM is good for high-volume environments, but is inappropriate for someone trying to solve a single issue. If a company is trying to focus on solving specific security issues, other options are generally better and less expensive. SIEM needs a central intelligence center within the enterprise and, while it is excellent at managing numerous data feeds and crunching large data sets, it is overkill for a company trying to solve an intrusion detection problem for a mission-critical database.

43% of companies experienced a breach in the past year.
– Ponemon Institute
Sometimes, Chuvakin says, all a company needs is a good syslog management service. While some companies might want to opt for a SIEM because a consultant or vendor told them they needed it for compliance or some other sales pitch, many of these client firms simply do not have the appropriate internal capabilities for a successful implementation, and the key resource most companies fail to consider are their human resources.

Sometimes a first SIEM is purchased to fill a checkmark on a compliance form, but Krehel says that reason alone is not enough. “You need to derive value from the solution, or it will end in failure,” he says.

Spencer cautions companies if they plan to purchase a SIEM product that is preconfigured. Some appliances could have literally thousands of rules built into the system. If the customer simply turns on all of the pre-configured rules, they could end up generating so many alerts that the system essentially is just creating noise of no value. Too few alerts being set or alerts set at the wrong threshold can create a false sense of security. Tuning the SIEM to collect the appropriate data to identify network anomalies and not just background noise – or tuning the network security applications that are being used in lieu of a SIEM – is essential for determining the company’s real risk.

SIEMs generally require top-of-the-line servers, he says, which need to be replaced every three to five years. The cost of support is significant, often approximately 25 percent of the price of the software alone per year. On top of that, he says, a company needs the right mix of engineering expertise to operate the SIEM.

Staffing is often a fraction of the price of the overall cost of a SIEM implementation, but can get short shrift if the company is trying to offset the cost of the software by scrimping on the staff. Imagine an IT staff that has only one or two people fully dedicated to the SIEM, says Spencer. Now imagine that the SIEM starts issuing 300 email alerts per day to your one or two staffers. Perhaps they can handle it, but likely not, he says. Now consider that they receive thousands of alerts. Are you staffed to handle that? he asks.

Anecdotally, Spencer says he has seen companies that might spend $1 million or more on a SIEM implementation with hardware and software, then balk at paying the $80,000 or $90,000 salary for technicians to make sure the system is configured correctly and providing valuable data. Understanding what the capabilities of the SIEM staff are and making sure that the company has the right expertise on hand to gain the benefit from the SIEM is very important, he says. While the number of full-time engineers might vary based on a company’s size and complexity of its network, it will depend on each implementation. No two companies’ needs are identical, so the staffing will be based on multiple variables. “One size does not fit all,” he says.

Often the systems administrators who “own” the log files are not necessarily part of the information security team, he continues. In order to obtain the requisite log files, the security team needs to know where every computing asset is located, what is on it, and who owns responsibility for that system. However, before logs can be generated, it’s essential to make sure that every device that might generate a log has auditing turned on.

Without a detailed model of the entire network and its assets, crucial input can be missed. Spencer recommends that network auditing be used to identify assets and the

49% of respondents said their company has adopted a SIEM solution.

– CompTIA, April 2015
activities on those assets. Once you can identify what’s critical, he says, “get the logs.”

While it might seem obvious that log files are necessary for feeding the SIEM, some organizations have internal rules that block IT from getting log files it requires. For example, he notes, some HR departments could have rules that block IT from monitoring certain types of actions by employees. While monitoring an employee’s system for web activity might seem reasonable to IT, it could violate a company’s privacy practices, he says. For example, an employee’s computer might display videos on a sports website, putting a heavy load on network bandwidth. Even though such activity could have a negative impact on network operations, he says, HR might consider that activity to be the employee’s right, and with the log files, therefore, private information.

Understanding what a SIEM is capable of performing and what it is not might seem academic, but because SIEM can do so much this basic issue can be misunderstood, especially by small to midsized businesses (SMBs) that do not have extensive security staffs. SIEMs excel at collecting and processing data, but they do not remediate problems. That happens after an engineer first analyzes the output from the SIEM.

A poorly designed and implemented SIEM can be a nightmare, Spencer says. If insufficient resources are allocated to the SIEM application, it could take months to troubleshoot the results delivered by the system and determine why they fail to match expectations. To benefit from such a large expense of time, money and personnel, a company needs a mature security culture. Otherwise, he says, SIEM is no more than “shelfware with a bad attitude.”

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

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, sales, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.
Alert Logic is a leader in security and compliance solutions for the cloud, providing security-as-a-service for on-premises, cloud and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 2,800 organizations worldwide.

For more information, visit www.alertlogic.com

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. The mission of Intel Security is to give everyone the confidence to live and work safely and securely in the digital world.

For more information, visit www.mcafee.com

EventTracker is a leading provider of comprehensive IT security solutions. Its industry award-winning SIEM and log management solutions enable businesses and organizations to meet compliance requirements with confidence, increase the security of their IT environments and reduce overall risk.

For more information, visit www.eventtracker.com

HP is a leading provider of enterprise security solutions designed to mitigate risk and defend against today’s most advanced threats. With market-leading products, services and innovative research, HP Enterprise Security Products enables organizations to take a proactive approach to security, integrating information correlation, application analysis and network-level defense.

For more information, visit www.hpenterprisesecurity.com

LogRhythm empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company’s award-winning platform unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence.

For more information, visit www.logrhythm.com
Your business is constantly changing, and so are the threats against it. Our 24x7 security-as-a-service solution integrates security technology, human analytics, and monitoring to keep your infrastructure safe from threats, wherever it's deployed. We aren't just keeping you secure. We're redefining how you stay secure.

Alert Logic. Security Will Never Be the Same.

www.alertlogic.com
EventTracker...significantly improves security while simultaneously demonstrating compliance, saving time and maintaining the standards for best practices.

EventTracker + SIEM Simplified = SUCCESS

Your IT Security & Compliance needs: SOLVED!

Award winning SIEM, expert services.

Change your view of security with instant clarity into threats.

HP ArcSight. Understand the threat potential of every event across your organization. HP ArcSight analyzes the broadest set of data sources, such as log data from devices on premise or in the cloud. Then it prioritizes events based on risk level, and displays them on a customizable dashboard to turn data into actionable intelligence. So you can get to bad guys before they get to you. Learn more at hp.com/go/ArcSight

Think like a bad guy.
Make a smarter security decision.

Use a smarter SIEM.

McAfee® SIEM Solutions.
Security intelligence for optimized incident response.
mcafee.com/siem

McAfee is now part of Intel Security.
That's where we come in. LogRhythm’s next-generation security intelligence platform identifies high-impact threats and neutralizes them before they can result in a material breach. It uniquely unifies SIEM and log management with network and endpoint forensics and advanced security analytics to provide comprehensive threat life cycle management and the ideal foundation for today’s cyber security operations.

HE WILL GET IN.

YOUR FATE WILL BE DETERMINED BY YOUR SPEED OF DETECTION AND RESPONSE.

That’s where we come in. LogRhythm’s next-generation security intelligence platform identifies high-impact threats and neutralizes them before they can result in a material breach. It uniquely unifies SIEM and log management with network and endpoint forensics and advanced security analytics to provide comprehensive threat life cycle management and the ideal foundation for today’s cyber security operations.

IMPROVE YOUR SECURITY INTELLIGENCE POSTURE AT LOGRHYTHM.COM/SIMM