SIEMple evolution

The future of SIEM is cloudy, literally and figuratively, as companies strive to keep up with potentially billions of events. Evan Schuman explains.

It has become an industry cliché to say that SIEM (security information and event management) is dead. Some SIEM vendors love those pronouncements because it drives wavering customers to make purchases before their SIEM systems of choice disappear. But here is food for thought: What if it is not that SIEM is too slow for the modern enterprise, but rather that today's modern enterprise has become too slow for the SIEM?

SIEM offerings are not so much a concrete entity as a constantly evolving set of security information and event management elements. The fundamental SIEM problem today is not the belief SIEM is going away, but that far too many enterprises are locked into a legacy mentality, one that, in effect, blocks them from changing security mechanisms fast enough to deal with a changing environment of cloud, mobile, shadow IT, as well as the changing threat where the bad guys are starting to use machine learning (ML) elements of artificial intelligence (AI), too.

Add to that changes in how companies create their homegrown software using DevSecOps (software development security operations), often referred to, correctly or not, simply as DevOps. So, with that in mind, would one still make the argument SIEM is dead or that it is more important than ever before?

One more consideration: The "death" of SIEM might simply come to pass when all the functionality of the technology is simply renamed something else for marketing purposes to differentiate the next-generation SIEM from legacy products. Sometimes "death" is evolution.

The concerns about SIEM, however, do not end with legacy-weighted-down slowness. A SIEM is not designed to work on its own and it never was. Many experts argue that it needs custom-crafted software from each enterprise to supplement the SIEM, along with a healthy dose of machine learning capabilities — two things that a lot of enterprises have not yet bothered to add.

Billions of events

Also, the number of attacks that a SIEM system has to deal with in the 2018 enterprise is massive and overwhelming. Umesh Yerram is the chief data protection officer at AmerisourceBergen, a $150 billion company ranked twelfth on the 2018 Fortune 500 list. He reports that his SIEM generates more than one billion events a week, a thoroughly unmanageable number. Using machine learning software that sits atop the company's SIEM, Yerram say that the "more than one billion" number is reduced to "less than a thousand" incidents that ML deems worthy of further investigation. That amount, he notes, is a manageable number for the AmerisourceBergen security team to probe.

Although many have questioned how accurate and precise ML screening is — it typically depends on what the system is programmed to seek — the counter-argument is that there is no viable alternative given the massive number of attacks that are being

OUR EXPERTS: SIEM

Allan Alford, CISO, Mitel
Dennis Chow, director of penetration testing, KPMG
Swapnil Deshmukh, security evangelist, Visa
Ray McKenzie, founder and managing director, Red Beach Advisors
Sammy Migues, co-founder, BSIMM
Michael Simmons, CISO, Southwest Airlines
Mitch Thomas, CSO, Encompass Health
Umesh Yerram, chief data protection officer, AmerisourceBergen

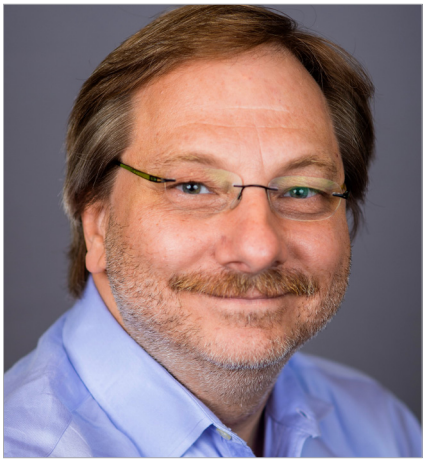
1,579

Total number of publicly disclosed data breaches in 2017

– Identity Theft Resource Center

launched. For better or worse, machine learning is the only option today for whittling down that number materially to something manageable.

This does raise the question of how much IT leaders trust ML and the answer is typically "not that much. But what choice do we have?" he says.


Sammy Migues, co-founder, BSIMM

"Having automation making security decisions for you, that is a very hard thing for a lot of large organizations to swallow," says Sammy Migues, co-founder of BSIMM in Mountain View, Calif. While the company is called BSIMM, the name actually is an acronym for "building security in maturity model."

Lock-in or replace

Allan Alford, CISO for Mitel, a $1.4 billion telecommunications firm headquartered in Ottawa, agrees. "Yes, [automation] requires more trust in the analytics, but you kind of have to trust it, as you need the fast response capabilities," he says.

That said, Migues argues, the future will be an IT world filled with far more automation and fewer humans. Security management might have emotional and intellectual qualms about it, but the pragmatics of the growth of attacks — coupled with a serious shortage of appropriately trained and experienced security professionals — will give them little choice, he says.

"The future of SIEM software is tracking every piece of software everywhere, monitoring every connection between every piece of software, helping Ops tell Dev that something is awry, and enabling Sec to make decisions about its small piece of the software pie and react at that cadence," Migues says.

"Some 90 percent of this will be with bots — no humans in the loop. Without good SIEM-like software, there is no real DevSecOps. Forward thinking DevOps shops are finding ways to fuse the configuration of their orchestration and other continuous delivery tools with intentional tagging and synthesis of SIEM alerts before humans receive them," he continues. "And, because this information is drawn from delivery and production logs, it reflects actual design rather than the best intentions scrawled on a whiteboard."

Migues also points out an organizational structure issue can create a SIEM problem. Any technology deeply embedded in the typical Fortune 1000 company — and it is hard to describe a SIEM implementation as anything other than deeply embedded — can take a long time to replace given the massive number of systems it touches and the potential disruption from a major change. That is a form of proprietary lock-in: It is far easier for IT to take update after update and even upgrade after upgrade than to go through the bidding and purchase paperwork — and delays — of purchasing a different SIEM system from a different company.

> "SIEM is in the troth of disillusionment"
>
> *- Sammy Migues, co-founder, BSIMM*

The idea of doing a major overhaul — a complete rip-and-replace — can strike fear into even the stoutest CISO. Sometimes, however, the stars align and such a major overhaul is appropriate.

Michael Simmons, CISO for $21 billion Southwest Airlines in Dallas, is a bit ambivalent about the SIEM future. "SIEMs still have a place today, but that may dwindle

75%

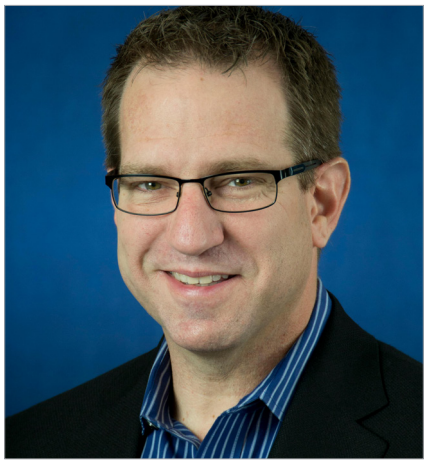
Percentage of data breaches caused by external attackers

– 2017 Verizon Data Breach Investigations Report

over time," Simmons says. "They're not easy to manage. Can they adapt and can their technology capabilities morph [into the future] easily? Will there be disruptive new players who come" and brand their SIEM-efforts something other than SIEM? This concerns Simmons.

The topic of SIEM is close to Simmons' thinking as his airline just replaced its SIEM with a SIEM that was entirely cloud-based SIEM leveraging infrastructure as a service.

Normally a full replacement of a SIEM would be unthinkable for a system that is integrated into so many parts of a network, but Simmons says it just so happened that an earlier security and IT effort to integrate the prior SIEM never quite worked right. "We never got it effectively implemented so I had a much cleaner rip-and-replace," Simmons says.



Allan Alford, CISO, Mitel

The reason why Simmons did such a radical upgrade is clear. "The magnitude of (security event) numbers is what was forcing the conversation, a rapidly changing and evolving threat landscape," Simmons says.

Pricing, as always, is another consideration — not necessarily the price itself, but rather the mechanism by which the price is determined.

Alford says that, of the many SIEM products he has worked with — he has held CISO or related security titles with several companies — he has seen only three, distinct SIEM pricing approaches. He identifies them as: the raw size of data gathered and the log size, the IP addresses to be monitored, and the number of sensors and aggregators/processors purchased/deployed.

> "The idea that a SIEM out of the box is sufficient is ludicrous"
>
> – Allan Alford, CISO, Mitel

"Regarding the pricing model question, I don't really think pricing models per se determine higher or lower cost. It's been my experience that [sensors and processors are] cheaper overall, but I think that's because the companies using that model are deliberately pricing under the guys who still do [log size]. So it's not the model per se," Alford says.

Regarding the log size and IP addresses options, he says "the migration of applications to Software-as-a-Service (SaaS) and the rigorous purging of legacy systems mean a theoretical reduction in cost of ownership. However, business growth and acquisitions outweigh this. Note that more users equals more traffic equals more logs, even if the total IP address count goes down.

"In reality," he continues, "regardless of model, you are going up, not down, on usage of your SIEM year over year. And the SOC (security operations center) manager wants more feeds anyway, as the more data points he gets, the more accurate he is."

Feeding the beast

In general, Alford sees the SIEM battle as being a race against changing threat vectors, network environment changes and matching software capabilities with enterprise needs and wants. And he is not seeing IT typically winning that race. "We're fighting an uphill battle. The [increasing number of] feeds into the SOC [means that IT is] fighting a signal-to-noise ratio" battle, with signal meaning real security events and noise referring to false positives.

"We've hit a plateau and are making no further progress," Alford says. "If you don't have UEBA (user and entity behavior analytics) and ML, some shops just hit the wall."

Alford's top SIEM concern is that too many

$3.62M

Average cost of a data breach in 2017

– Ponemon Institute

companies treat SIEMs as though they were standalone, shrink-wrapped software with no need for customized code while being focused on the user's specific situations and needs. That is an untenable move.

"You still have to have the care and feeding of your SIEM. Somebody on your team must be dedicated to constantly tweaking your SIEM, training and teaching it and feeding it," Alford says. "The idea that a SIEM out of the box is sufficient is ludicrous. A SIEM is nothing more than an aggregator and an incomplete aggregator at that. SIEM without automation is incomplete. You have to fine tune what to ignore and what to look for."

Dennis Chow, director of penetration testing, KPMG

Migues opines that "As we get smarter, we develop different expectations of technology. Soon, the organization's expectations will have exceeded its grasp. SIEM is in the troth of disillusionment. What we needed and what we wanted could not be met."

Dennis Chow, the director of penetration testing at KPMG, agrees with Alford. "Everyone keeps claiming SIEM is 'dead.' It really isn't. It's just evolving. All the new buzzwords like orchestration, IMS (IP Multimedia Subsystem), UBA (user behavioral analytics) and threat intelligence were always supposed to be part of what a true SIEM was. What we saw was first generation vendors doing a [release to manufacturing] and realistically releasing what I deem a half-baked product. The same is true for most of these orchestration and 'threat intelligence' tools. SIEM is going to be more of this loose term in the future, like AI is today," Chow says.

"I'm former military and have had opportunities to observe how three-letter agencies deal with cyberintelligence-related needs," he continues. "SIEM was supposed to have solid use-case correlation and be complete enough to automate response actions. To be honest, I don't really call anything a SIEM unless it can also integrate ML functions, post-alert/script execution, and also be able to communicate in standard protocols to other security program components/pieces."

But Chow is not quite finished. "Don't forget to include common SSH and SSL termination to decrypt which is mostly encrypted traffic now. If you aren't decrypting traffic, you're missing out on so much. To much of the industry's dismay, first [generation] SIEM is also failing because of a gross lack of talent to properly deploy, tune, and extend their existing tools."

Customization Challenge

AmerisourceBergen's Yerram says that customization is desirable, but, depending on the SIEM being used, is not always do-able. "The product are sometimes limited in how much customization you can do," Yerram says.

Either way, customization takes resources, both for staffing levels and configuring the SIEM. For example, let us assume a SIEM saw a security incident and confirmed, to a limited extent, that it appears to be real, meaningful and dangerous. Once all that happens, it is critical for someone or something to alert all of the key players right away. Has someone alerted the VPN team, the Windows team, or a threat hunter? While appropriate staffing levels are essential simply to support basic SIEM maintenance, the company needs to ensure that it balances funding for maintenance and management with that of improving with providing the requisite staff for all the necessary security teams.

Alford recalls that the earliest days of SIEM marketing suggested that companies could purchase a SIEM and replace some tier-one

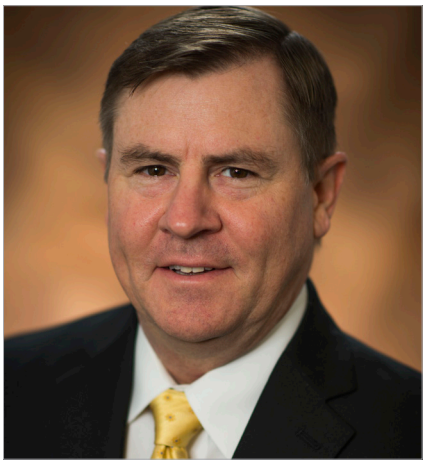
77%

Percentage of CISOs who said they were "highly concerned" about undetected security breaches

– The Global CISO Study by Oxford Economics

analysts, a claim that some EUBA vendors are making today. The claims were not true in the past nor are they accurate today, Alford says.

Like everything in IT and security, the cloud is changing many of the rules and the realities. As more data gets poured into the cloud, the type of cloud structure becomes critical, especially for SIEM security issues, Alford says.



Mitch Thomas, CSO, Encompass Health

"The more you offload to the cloud, the more you offload everything to the cloud, including security awareness," Alford says. SaaS is especially problematic. With SaaS, "you're handing over a good bit of trust. What you're going to be able to monitor are the ins and outs. You'll have no visibility inside," Alford says, adding that it is essential to structure cloud deals that allow for users to have full visibility — and even better control — over all elements of the cloud infrastructure.

> "SIEM platforms should automate the work of tier one analysts to allow teams to focus on the tier two and tier three work of threat hunting, incident response, closing the OODA loop faster, which also helps with the skills shortage problem"
>
> *– Mitch Thomas, CSO, Encompass Health*

Mitch Thomas, CSO for Birmingham, Ala-based Encompass Health, a $3.9 billion healthcare company, agrees that SIEM should automate the analysts' works. "SIEM platforms should automate the work of tier one analysts to allow teams to focus on the tier two and tier three work of threat hunting, incident response, closing the OODA loop faster, which also helps with the skills shortage problem," he opines. (The OODA loop — observe, orient, decide, and act — was developed by the US military for combat operations processes.)

KPMG's Chow also expresses concerns about the cloud and security. "Cloud testing is a pain.... There's so much complexity and you have to test all of these components," Chow says, adding that CISOs must deal with "all of this stuff that is proprietary to that cloud."

Chow agrees with Alford that an agreement, including architectural access and control, is critical. "You need to have an architectural use case of the cloud to know what you're doing. The cloud has limitations on how you manage it. You don't have the rights like you do with on-prem."

Trillions of lines of code

Still, cloud is not going to be easy to avoid. Swapnil Deshmukh, the security evangelist leading DevSecOps at Visa in Foster City, Calif., says that because of the nature of the Visa network and the fact that it transfers money around the planet, it gets attacked continually. He estimates that the Visa SIEM sees 115 million events per second "and those are staggering numbers. We have an explosion of data."

(Due to the payments nature of its business, Deshmukh notes, Visa defines events much more broadly than many other companies. For Visa, an event is any transaction anywhere in the world. That is because it must analyze every transaction to see if there are any red flags. Others view an event as a security event and each event already reflects some pattern deviation worthy of further exploration.)

That explosion of events is especially true for a company like Visa that is so heavily regulated, Deshmukh says. "You need to

74%

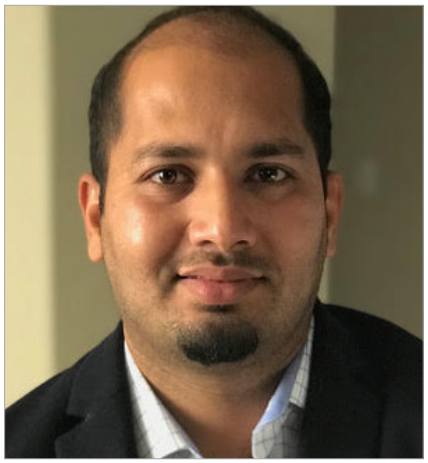
Percentage of survey respondents who said they felt vulnerable to an insider attack

– Haystax Technology

store this data somewhere, which adds to the hardware costs" so that necessitates employing the cloud, he says. "With these trillions of lines of code, how do you identify if there is any personally identifiable data?" he asks. That forces an awful lot of data sanitization.

"These events are growing exponentially, due to programmable infrastructure and hyperconnected workplace and user can now access sensitive information from mobile phone, from software-defined WANs or even on various cloud offerings," Deshmukh says. "This explosion of event logging is causing scalability issue for many SIEM storage. In near future, SIEM must solve the scalability problem.

"Currently, organizations with deeper pockets are solving this problem by adding expensive infrastructure to SIEM storage or leveraging cloud storage options such as Amazon S3 buckets or Google cloud storage," he continues. "As these events are sensitive in nature, organizations storing information on cloud might have to jump additional hops of managing keys that tokenize these events. From budgeting standpoint, adding storage to support SIEM may add huge overhead and in many cases it can be a deal breaker for organizations with limited budget."



Swapnil Deshmukh, security evangelist, Visa

The cost of SIEM support is not limited only to small or mid-size businesses with shallow pockets. Thompson says that his team is also seeing "an exponential growth of data collection and I can't keep pace with that from a cost standpoint."

Responding to every SIEM alert can be daunting if filters to weed out false positives are not in place. "Every alarm, every indicator is some kind of event. How can you manage all of that?" Thomas says rhetorically.

Although some enterprises have worked with AI's machine learning, such as AmerisourceBergen, Deshmukh says Visa hasn't and he blames the extensive use of proprietary code used by many SIEM vendors, including the one that Visa uses. "The vendors have it in a proprietary format. Because of that, we can't create our own models, due to the vendor's lock-in. The proprietary format makes ML nonviable right now. That's the reason why the adoption of machine learning in SIEM is not there yet," Deshmukh says.

Unstructured data

Another SIEM concern that several experts touched on were challenges inherent in scanning unstructured data such as images and video.

Deshmukh says Visa does not look currently at unstructured data because, in his view, Visa's SIEM "can't make any sense of it" giving it "very limited visibility" into a place where cyberthieves can try and hide malware. But he expects that to change in the next few years. "In the future, we expect new techniques to convert unstructured data into structured. At this point in time, we don't have those techniques."

Migues agrees and he adds that even email can be baffling for analytics. "Understanding context from unstructured data is really, really hard," Migues says. A big part of the problem is that, with unstructured data, so many enterprises, as well as vendors, use different terminology and structure to achieve similar results. "Different companies use different words, different ways," he says.

For example, an email might include the words "Employee Salaries. Do Not Release" but it "doesn't necessarily mean that it really has employee salaries," Migues says.

$102B

Estimated spending on security-related hardware, software, and services in 2020

– Worldwide Semiannual Security Spending Guide (IDC)

Ray McKenzie, the founder and managing director for Red Beach Advisors, agrees that unstructured data is a problem, but argues that some vendors have addressed it quietly — too quietly.

"SIEMs are behind the curve, for the most part, in terms of dealing with unstructured data. You always have to add packages or add content. The SIEMs don't recognize it upfront" and out-of-the-box, McKenzie says. "Vendors and CISOs are not talking about the unstructured data problem. Threats are a much easier discussion."

Ray McKenzie, founder and managing director, Red Beach Advisors

But McKenzie maintains that he knows of some unspecified SIEM vendors who have mastered the unstructured data problem, but they are not marketing that fact. "Unstructured data is still a problem. The people who have solutions to the problem haven't promoted it. There are platforms that can (handle unstructured data) today."

AmerisourceBergan's Yerram disagrees with McKenzie, at least as it impacts the major SIEM players. "No, the leading products out there — as identified [by the major analyst firms] — cannot handle unstructured data," Yerram says.

Yerram has other practical concerns about SIEM usage. "Correlating the information and triaging takes a long time right now. I want one single pane of glass," Yerram says, referring to one screen to handle all needed activity, rather than "having to go to multiple different consoles" so that his team can have "integration with multiple different intelligence sources. I don't believe that a lot of the traditional SIEM devices do that. It doesn't happen in a single screen."

Yerram offered an example of the SIEM detecting suspicious activity on an IP address. "To look up who owns that address, I have to go to multiple different sources [on different screens] to collect that information," Yerram says.

Machine learning analysis can be used to recommend actions by the security staff or the ML can be instructed to take specific actions automatically when it encounters certain conditions. Yerram says his team does a little ML automation, but they are being cautious.

ML automation "is a good idea once you teach the system the right things" to justify an automatic reaction, Yerram says. "Our automation is limited right now. We are still taking our time to make sure that we are getting it right. There can be significant impact on the brand [due to the automatic ML action] causing an outage of some fashion. It comes down to what you teach and what the comfort level is."

So what is the future of SIEM? That can be difficult to determine, short of assuming increased integration with AI and machine learning. As noted, the next generation of SIEM might distinguish itself by not even using the term "SIEM." Whatever the future of SIEM will be, it is a given that it will still be big, complex, embedded into every corner of the network, and more than likely, still expensive. What it likely will not be is plug-and-play. ■

For more information about eBooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an eBook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

60%

Percentage of SMBs that go out of business after a data breach

– Switchfast Technologies