SC analysisbrief

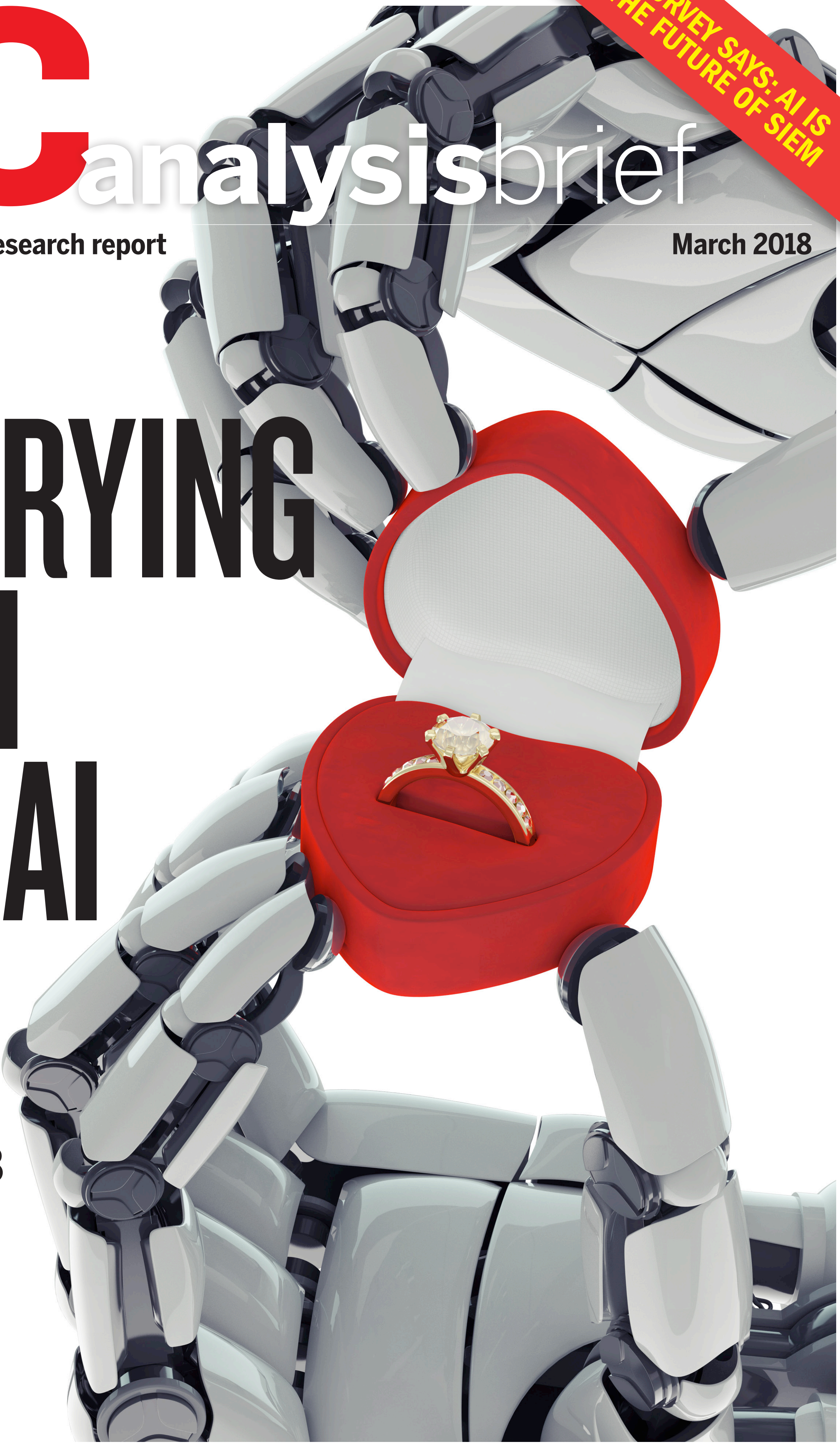
An SC Media/IBM research report

March 2018

SURVEY SAYS: AI IS THE FUTURE OF SIEM

MARRYING SIEM AND AI

More than 50% of enterprises expect to use SIEM with AI by the end of 2018



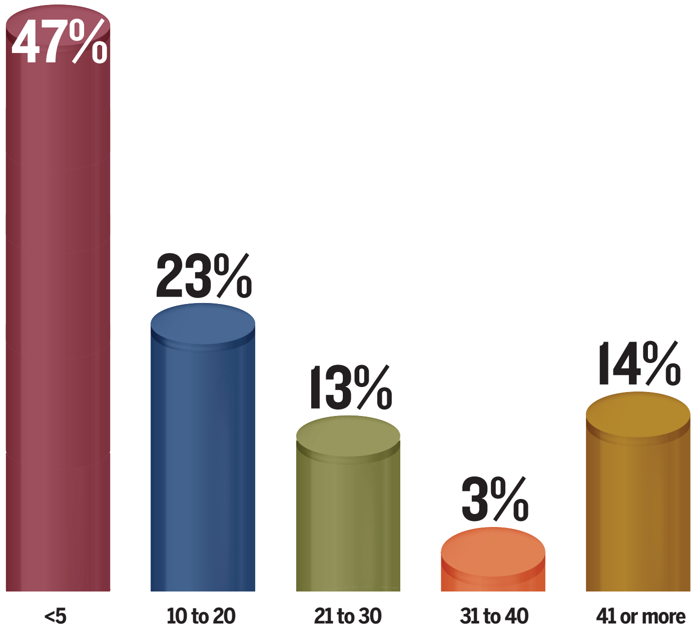
SURVEY SAYS:

AI IS THE FUTURE OF SIEM

While AI enhancements appear to be the logical next step in the evolution of SIEMs, we're not there yet. Esther Shein reports.

When configured and managed properly, there is nothing like a security information and event management (SIEM) system to bring significant benefits to incident response efforts. And when paired with artificial intelligence (AI), SIEMs become even more effective, according to the findings of a recent survey of 295 IT security professionals co-sponsored by IBM and SC Media. Unfortunately, all too often, companies that have SIEM systems have nothing like a well-configured system, resulting in dissatisfaction with the software and its associated costs, according to our experts. The survey, conducted by C.A. Walker Research Solutions in February 2018, covered a wide swath of organizations in terms of size, revenue and industry.

How many security incidents does your SIEM alert you to on average per day?

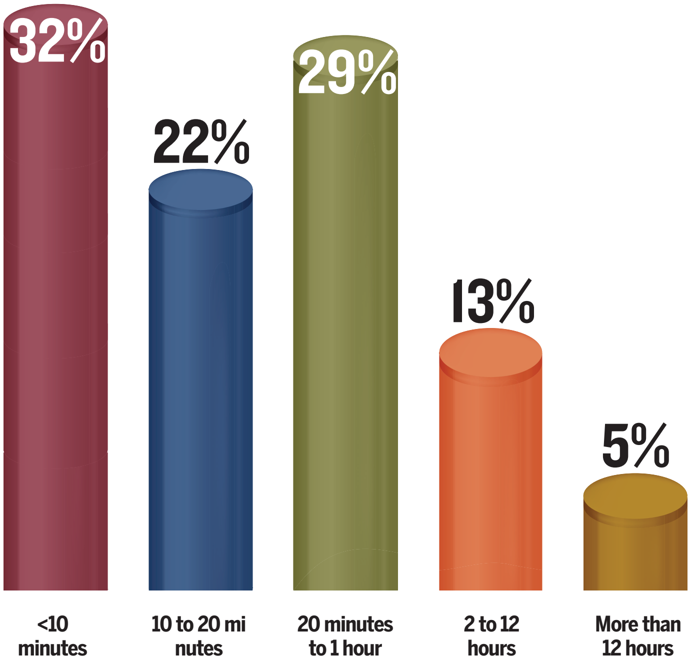


Even though SIEMs can be complex to implement, security professionals realize that modern SIEMs add value to their organization by helping to detect and respond to security incidents effectively.

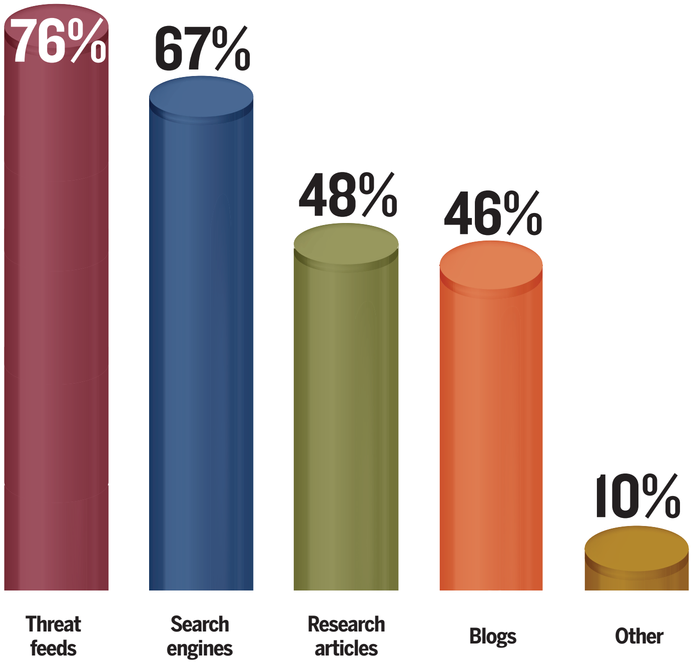
Roughly $1.2 billion in SIEM appliances and services were purchased by enterprises in 2017, according to Frost & Sullivan. The firm's early estimate for 2018 enterprise SIEM sales is for between 8 percent and 10 percent growth, says Christopher Kissel, a senior industry analyst on the cybersecurity team.

SIEM platforms merge security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts. They are used by the majority of large enterprises, whether managed in-house

How long do you take on average to investigate a security incident?



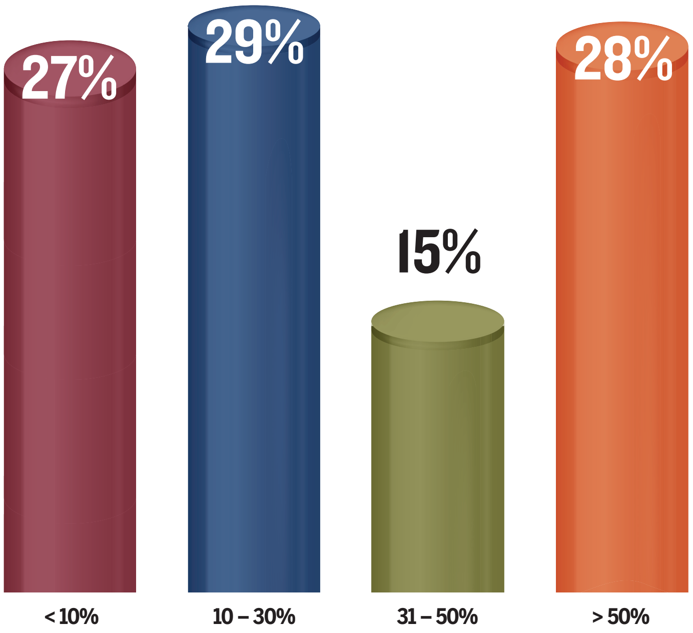
What are the various data sources you refer to while investigating a security incident?



or through outsourced services. However, while many organizations have procured SIEMs, most are not properly configured or managed, maintains Tara Swaminatha, a data privacy and cybersecurity partner at the law firm Squire Patton Boggs.

Because it often takes multiple skilled security staff members or a full team to first configure, then run and monitor SIEM systems, inadequate IT and security staff resources are often cited as the main reasons for not deriving benefit from SIEMs, adds Swaminatha, who is also a former federal prosecutor with the U.S. Department of Justice Computer Crime and Intellectual Property section.

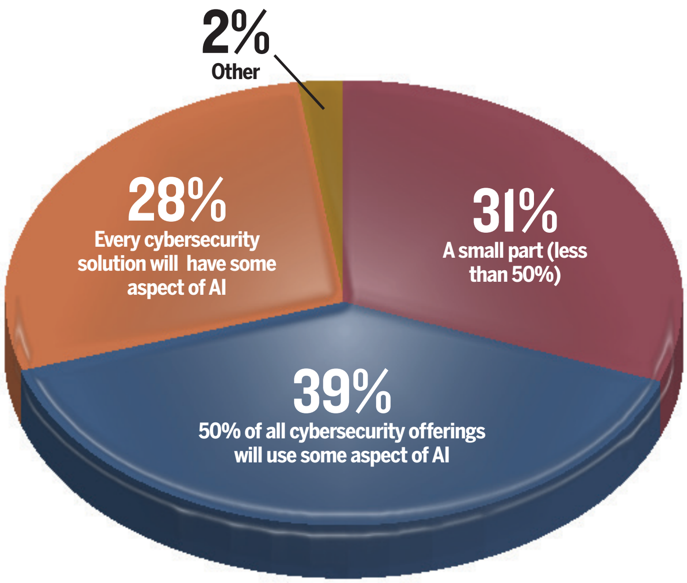
How many security incidents turn out to be false positives?



SIEMs and AI

One method companies use to determine how well or poorly their SIEM is configured is by the number of alerts generated daily. A SIEM designed to collect everything, no matter how insignificant, might generate huge numbers of alerts, mostly false positives, and would be considered poorly designed, the experts agree. A more finely tuned SIEM that weeds out many of these false positives will return far fewer alerts. According to the survey, some 30 percent of respondents from companies with more than $1 billion in revenue — 29 respondents of the 95 in that category — said their SIEMs return 31 or more incidents per day. From an employee headcount, that falls to 27 percent, or 29 of 103 respondents from companies with 5001 or more employees. The survey

How much will AI technologies (Machine Learning, Deep Learning, etc.) influence the cyber security market in the next 5 years?



did not cap the number of alerts a SIEM might generate.

Adding AI to a well-configured SIEM can add significant value by reducing the amount of false positives and noise, which makes security analysts more productive in the security environment. IBM's approach to AI works using a pyramid approach, where machine learning is at the bottom, then cognitive-oriented technologies are above that such as artificial vision, natural language processing, knowledge graphs and a reasoning engine at the top, says Robert Freeman, senior manager of Watson Security Research at IBM.

"If you look at some of those components, they provide individual machine learning and potentially deep learning insights, and that knowledge graph would be able to organize that information and reasoning engines would be able to surface abstractions," he explains. Reasoning engines are designed by humans to produce an awareness based on available inputs, Freeman says.

At the top of the pyramid would be "pure AI" that is independent in thought in raw, almost human-like capabilities of machine AI, he says.

The goal of adding AI to a SIEM is to reduce the time investment to create a baseline and tune with alerting without requiring highly experienced staff, says Paul Hill, senior consultant with SystemExperts Corp., a cybersecurity consultancy.

Overall, 72 percent of respondents at companies with revenues between $100 million and $1 billion, representing 57 of the 79 respondents in that category subset, find their AI-enhanced SIEM systems to be effective, along with 69 percent of respondents at companies with between 1,001 and 5,000 employees (59 of 85 respondents in that category). Even companies with revenue less than $100 million said they find their AI-enhanced systems to be effective (56 percent or 68 of 121 respondents) along with those that have fewer than 1,000 employees (60 percent 64 of 107 respondents). In the largest enterprises with $1 billion or more in revenue, 68 percent (65 of 95 respondents) and 65 percent of high employee-count companies 67 of 103 respondents in companies with more than 5000 employees) found AI-enhanced SIEMs to be effective.

But when we drilled down and asked how effective their AI-enhanced SIEM systems are, only 28 percent of all our respondents find them to be very effective. Forty-seven percent of mid-size companies (37 respondents of 79) who have revenues between $100 million to $1 billion and 36 percent of large enterprises with more than $1 billion (34 of 95 respondents) said they are somewhat effective.

> "Separating signal from noise is no joke with SIEMs"
>
> Tara Swaminatha, Squire Patton Boggs

Freeman attributes this to the fact that AI is still new, "and there is more education that we can do to demonstrate the value of AI on top of SIEM solutions for customers."

While there might well be a lack of awareness or familiarity with AI, Freeman believes it is just a matter of time before AI becomes ubiquitous, and if there is not an AI offering on top of a given SIEM system, "it may be the case where it becomes a requirement for the business or it might preclude that solution from consideration. This is where the world is headed."

Investigating incidents

Generally speaking, companies believe they are well positioned to investigate incidents that are identified by their SIEM. For small companies with revenue of less than $100 million, it takes fewer than 10 minutes to investigate an incident, according to 53 of the 121 respondents in that category. When looking at small companies by head count rather than revenue, 43 percent of respondents at firms with 1,000 and fewer employees also said it takes less than 10 minutes.

The plurality of companies with 1,001 to 5,000 employees, 31 percent or 26 of the 85 companies in that category, said it takes from 20 minutes to one hour to investigate an incident, while the plurality of midsize companies by revenue, 34 percent, or 27 of 79 companies, also were in the 20-minute to one-hour time slot. Large enterprises ranked by personnel and revenue each clocked in at 34 percent as well. The findings will vary because there are different things people are looking at, depending on their environment, says Chris Hankins, offering manager, Cognitive Security, at IBM.

The key takeaway, according to the company, is that if each analyst is spending 20 minutes to one hour per alert times a large number of alerts per day, a company can run out of staff capable of following up on alerts quickly. And since these alerts occur daily, it is not necessarily possible to put off following up on those alerts to the next day, since each day has 30 or more alerts in a large company. AI can play a role in reducing the number of alerts, IBM says.

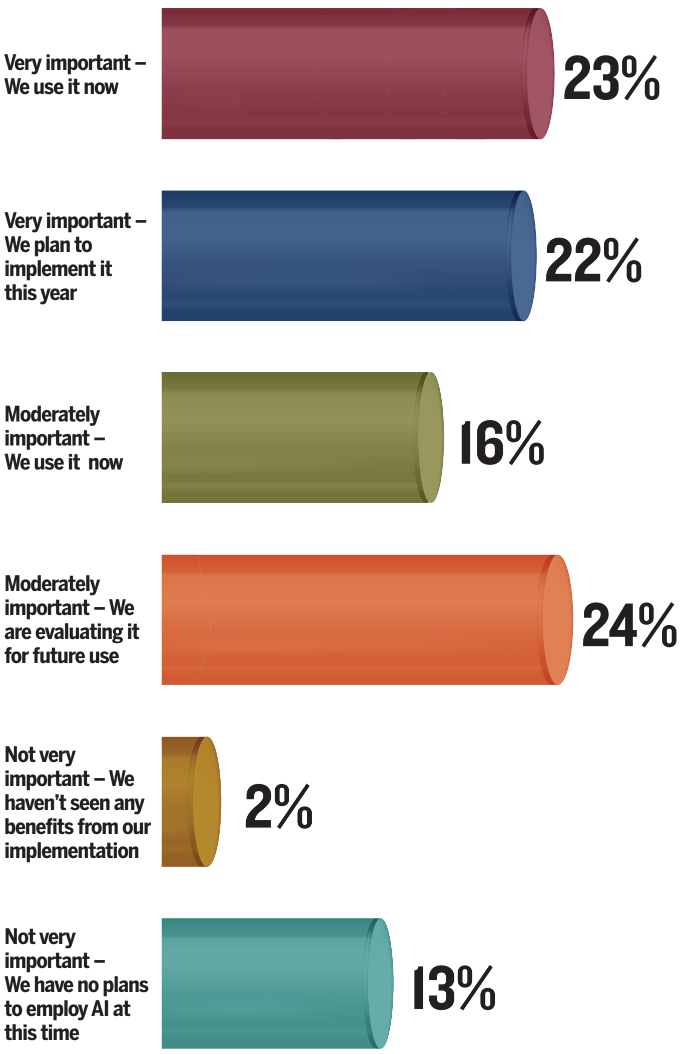
Some people look at alerts from a very general perspective, while others will look at malware protection or threat protection around denial of service, he says. “Then there are people who want to throw everything at a SIEM and you have to bridge the gap … and try to identify what it is you’re looking at.”

Hill agrees that the results are highly dependent on the environment. “Analysis can take hours or a few seconds. For example, consider a company that uses NAT (network address translation) addressing and some devices are located where an external public IP address will be recorded in the log, while other devices record the internal private NAT address,” he says. “Other log data may reference the server name rather than an IP address. If the company doesn’t publish DNS reverse records, and the SIEM doesn’t have access to the translation table, then analysts will have to do lots of manual research.” But if the SIEM is integrated into the network management system and associated tools, the SIEM can help speed up the analysis greatly, Hill adds.

The timing is also very dependent on the maturity of the system, notes Swaminatha. “Enterprises have to collect and review log data over time in order to develop an understanding of typical activity,” she says. “Only after doing so can a SIEM team determine how to configure alerts to pick up on anomalous behavior and specify events and rules to mark meaningful incidents.”

Hankins says it’s important to understand how to apply analytics and then additional enrichments such as threat intelligence, to a SIEM, so an analyst can gain a broader context to alerts. “You want to be able to identify something that you can apply action to,” he says.

How important is AI to the future of your cybersecurity defenses?



On-prem and cloud SIEMs

Integrating on-premises and cloud-based SIEMs continues to be a challenge for companies large and small. Just 32 percent of respondents at companies with revenue of $1 billion and more, some 30 of 95 respondents, said they can integrate both on-prem and cloud-based data to identify anomalies, while this was the case for just 19 percent of large enterprises of more than 5,000 employees with 20 of 103 respondents reporting.

For mid-size firms, just 13 percent, or 10 of 79 companies with revenue of $100 million to $1 billion, could make that claim, while the corresponding total for mid-size firms by employee count was a healthier but still relatively small 24 percent or 20 of 85 companies.

Overall, one in four companies of all sizes are not using cloud-based SIEMs at all, with mid-size firms in both categories scoring higher in the 34th percentile of companies without cloud-based SIEMs.

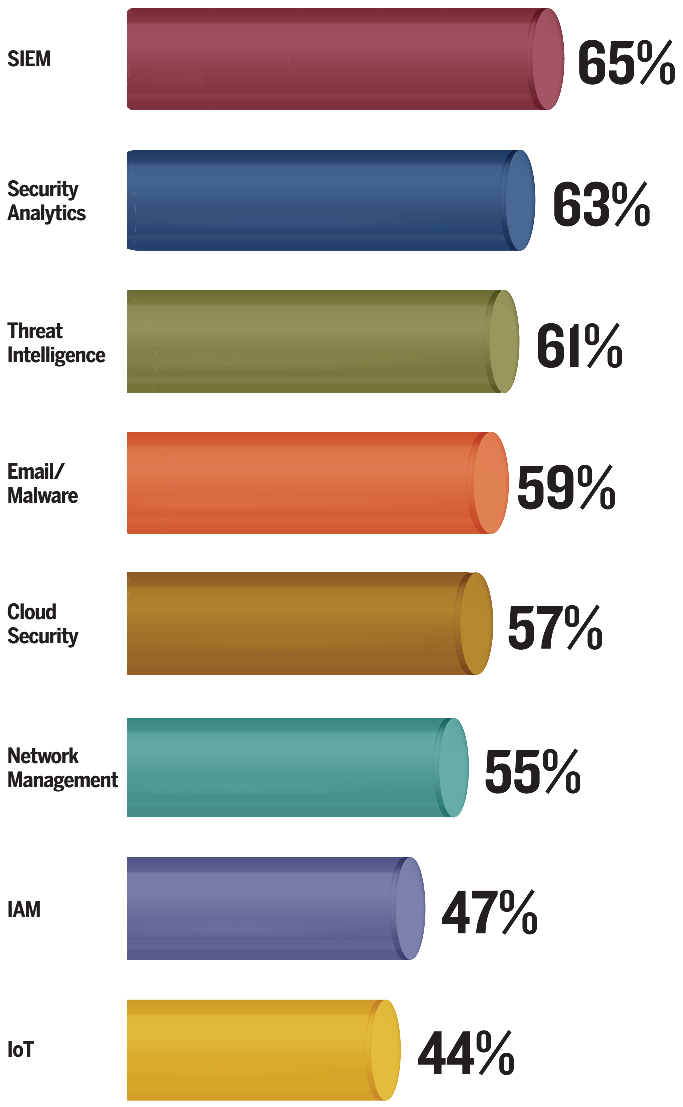
When a SIEM is on-premise, a security professional can learn what the network is seeing and the outcomes of existing investigations, as well as future incidents, says IBM's Freeman. "Similarly, there are ways on an on-premise basis to incorporate external data feeds as well to gain additional abilities to correlate data on your network that operators need to run scripts."

However, Freeman adds that when you have a cloud-based or hybrid SIEM service "you're getting the advantage of a lot more processing power in the cloud and the advantage of mass knowledge bases, and you can integrate a lot more data." This can be done by leveraging insights from anonymized data among different customers, for example, if there is a malicious file or malicious website that is being seen a lot, he says.

"That sort of trending information isn't going to expose a customer to other customers, but it would help inform a solution that there's something happening that [is being seen] across different customers," Freeman says. It could also help inform the AI product by conveying a different context in the scope of translating the incident to whatever visual and language components it uses to relay the information to the analyst, Freeman says.

How effective are your AI-enhanced security tools?

(Combined percentages for Very Effective and Somewhat Effective)



Respondents were also asked how efficiently their on-premise and cloud-based SIEMs are at producing actionable reports. Company size mattered here. Thirty-six percent at companies with 1,000 and fewer employees said they have no plans to enrich their SIEM output, while 29 percent at companies with more than 5,000 employees are planning to enrich SIEM output in the next six months.

Like attorney Swaminatha, security consultant Hill says the traditional problem with a SIEM is the amount of time and expertise required to establish a valid baseline of normal traffic within an organization's network. "Simply deploying a SIEM and turning on every preconfigured report … is not productive," he says. "In most organizations that will result in a flood of information, much being false positives."

However, a properly tuned SIEM can discard the false positive and let staff focus on a small number of actionable items, Hill adds.

For example, “In the last six months I was interacting with one company that generates approximately eight billion raw log events per month,” he says. “The SIEM filters those down to 19 million events per month. With tuning, the SIEM generated approximately 7,000 alarms per month.” The first-tier security operations center (SOC) staff reviews the alarms and end up creating on average, 16 tickets per month for further investigation, Hill says.

The number of false positives a SIEM generates is something with which security professionals often have to contend. The survey found that overall, 47 percent of respondents are alerted to fewer than five security incidents on average per day from their SIEM systems. But Swaminatha sees the number being significantly higher, saying that “for a mid-to-large sized enterprise, a SIEM can generate upwards of 10,000 alerts per minute, which include a massive amount of false positives and require a monumental amount of personnel resources to analyze in order to identify true malicious activity. Separating signal from noise is no joke with SIEMs.”

It is important to look at data from a granular perspective and drill down to the rules a security team has established as components of what they’re trying to do, says Hankins.

If you are trying to identify suspicious user activity, for example, you know users should not be logged into the corporate virtual private network (VPN) from China when they are sitting in their office, he notes. That means looking at a number of variables, including geography, whether a user is logged into their local PC, the source IP and user authentication, to establish a baseline for the data elements that will meet the use case, Hankins says.

The output from SIEM systems can be extremely useful at providing security professionals with actionable data, says Eric Ogren, senior security analyst at 451 Research. “There’s no way to plug in the gaps between the silos of security products,” he says. “If an enterprise has 20, 30, 40 security products, there’s only one place where logs and event data get pulled together so you can do analytics and manage your workflow,” meaning responding to the events an IT analyst sees. “That’s through a SIEM. You can’t do it any other way.”

This is why there is a lot of talk about integrating analytics and AI, says Ogren, whether on-premise or in the cloud. “AI can help you see how many of these alerts are coming from the same incident,” he says. “So it’s boiling down thousands of alerts to less than 100 or 50. Where the AI executes from doesn’t really matter.”

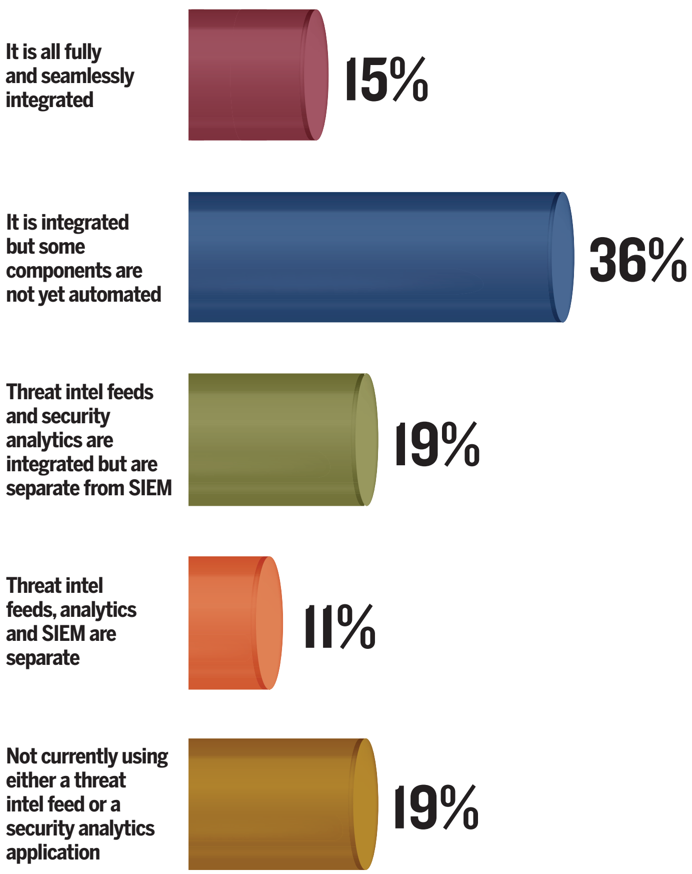
Like Ogren, Swaminatha says AI/machine learning can make significant differences in the management and utility of SIEM systems.

“Such systems can block threats without human intervention, detect anomalies over time and screen out network noise in order to allow the human security professional to focus on real threats and events,” she says. “Importantly, this technology also provides invaluable threat intelligence and network security analytics in order to proactively prevent future threats.”

Integrating security apps

Not many respondents have integrated their SIEMs with their threat intelligence and analytics applications.

How is your SIEM integrated with your threat intelligence and analytics applications?

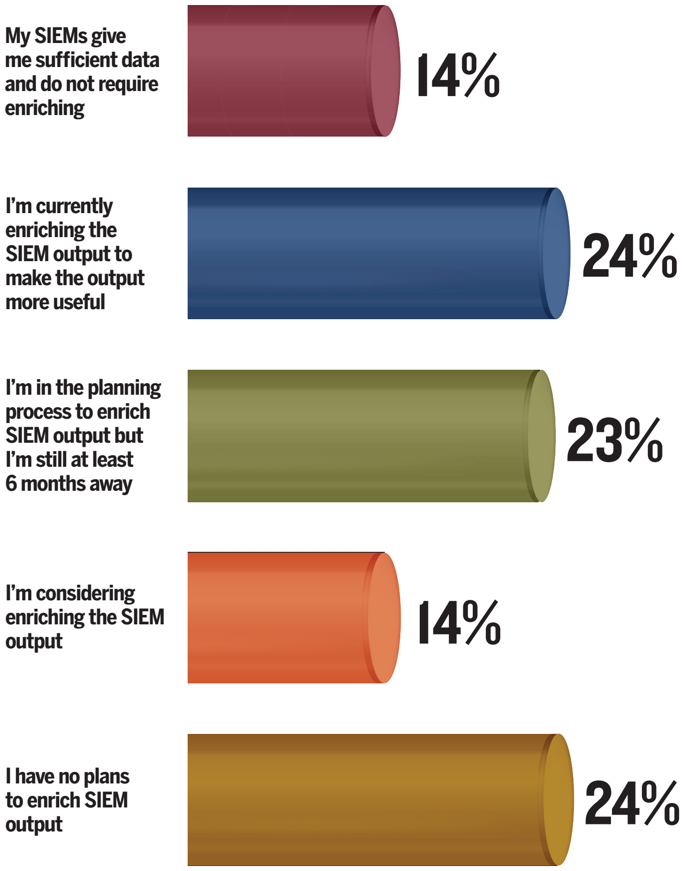


Only 15 percent (15 of 103 respondents at companies of more than 5,000 employees) said it is all fully and seamlessly integrated. That's the same percentage for all reporting respondents.

Some 40 percent of respondents at enterprises with more than $1 billion in revenue have done the integration work, but some components are not yet automated. That's also the case at 39 percent of enterprises with more than 5,000 employees.

The findings are surprising, says Cameron Will, a threat intelligence engineer at IBM Security. "I would hope that more people would be integrating intelligence sources into their SIEMs. I feel like it's getting easier and easier to integrate any threat intelligence sources you want into your SIEM, especially if they conform to some standard schema like STIX (Structured Threat Information eXpression)," he says. Because STIX is an open standard, it makes it more seamless to have a unified language for talking about threat intelligence, Will explains.

How efficiently are your on-prem and cloud-based SIEMs producing actionable reports?

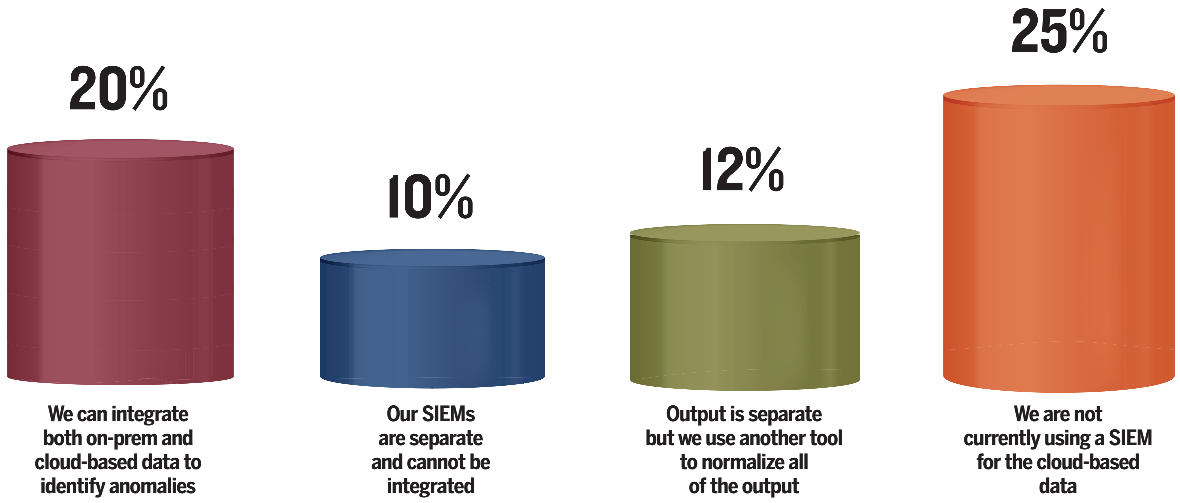


Most of the SIEM product leaders offer cloud-based options with a pricing model that is based on how much data is logged per month, says Hill. These vendors are also offering some AI or machine learning-based supplemental services.

There are also systems that integrate AI into security operation centers that smaller companies might find useful. They are, in effect, tack-ons to SIEM logs, analyzing this data through their AI system, says Swaminatha. "Smaller companies that might not have the human resources capable of continuous monitoring may find that such AI functionality enables their IT and cybersecurity staff to focus on the detections that really matter," she says.

Security operations and analytics platform architecture (SOAPA) is the next generation of SIEM and helps to

How do you integrate your on-prem and cloud SIEMs?



address many of the common problems with traditional SIEM systems, namely, time and staff constraints, she adds. SOAPA systems brings together different data sets onto one platform and integrate some level of dynamic machine learning to be able to analyze, manage and report any anomalies.

Future of AI and cybersecurity

Looking ahead, everything is headed toward cognitive innovation, maintains Freeman. AI can be utilized to synergize data both from structured data sources and natural language, and that's what organizations want, he claims.

"Right now, the solutions I'm aware of are acting as adjuncts to help businesses make decisions faster, and that's the draw of these SIEM solutions that have an AI component," he says. "In addition, you're likely to receive some analytical benefits," such as being able to make correlations among customers and their risk profile.

While respondents are not overwhelmingly running to AI as if it is the next generation of iPhone – a plurality of companies with more than 5,000 employees, 30 of 103 respondents or 29 percent, said it is very important and they plan to implement it this year – Freeman believes AI technologies like machine learning and deep learning will have a dramatic impact on the cybersecurity market in the next five years. It is worth noting that this total is in addition to the 26 percent, or 27 respondents, who already are using AI, pushing the number to more than 50 percent by the end of 2018.

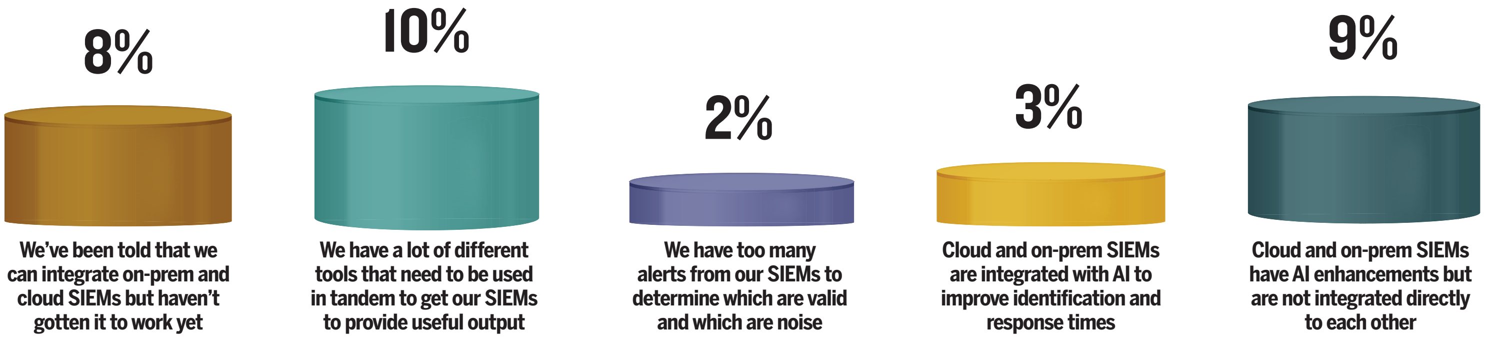
That's a reasonable timeframe for a lot of innovation to reach mass awareness, he says. Whether it is looking at SIEM analysis or orchestration or anti-malware, "pretty much across the board, if vendors aren't looking at integrating AI with their solutions … they're going to find in a five- to 10-year timeframe they're in real trouble."

Ogren concurs. "I am absolutely convinced that in three years security operations will be driven by AI first and some deterministic pattern matching next," he says. Right now, a lot of CISOs are looking to utilize AI to optimize all their SIEM data, but he believes in three years, "AI will be smart enough to make decisions faster than people. It won't replace security; it starts with AI and then goes down into the specific security tools. Analytics and AI [are] central to that whole strategy."

Methodology

This survey was based on 295 responses from a broad cross-section of company sizes and revenues and eight industry verticals, including federal and state and local government, technology services, finance, education, manufacturing, medical and healthcare, legal/real estate and retail and wholesale distribution. The survey was conducted in February 2018 by C.A. Walker Research Solutions, Glendale, Calif. The results of this survey might not equal exactly 100 percent due to the following reasons: rounding errors during the analysis phase of research; respondents who skip a question; and respondents who provide more than one answer to a question. This survey has a confidence level of +/- 6 percent.

How do you integrate your on-prem and cloud SIEMs?


We've been told that we can integrate on-prem and cloud SIEMs but haven't gotten it to work yet
We have a lot of different tools that need to be used in tandem to get our SIEMs to provide useful output
We have too many alerts from our SIEMs to determine which are valid and which are noise
Cloud and on-prem SIEMs are integrated with AI to improve identification and response times
Cloud and on-prem SIEMs have AI enhancements but are not integrated directly to each other