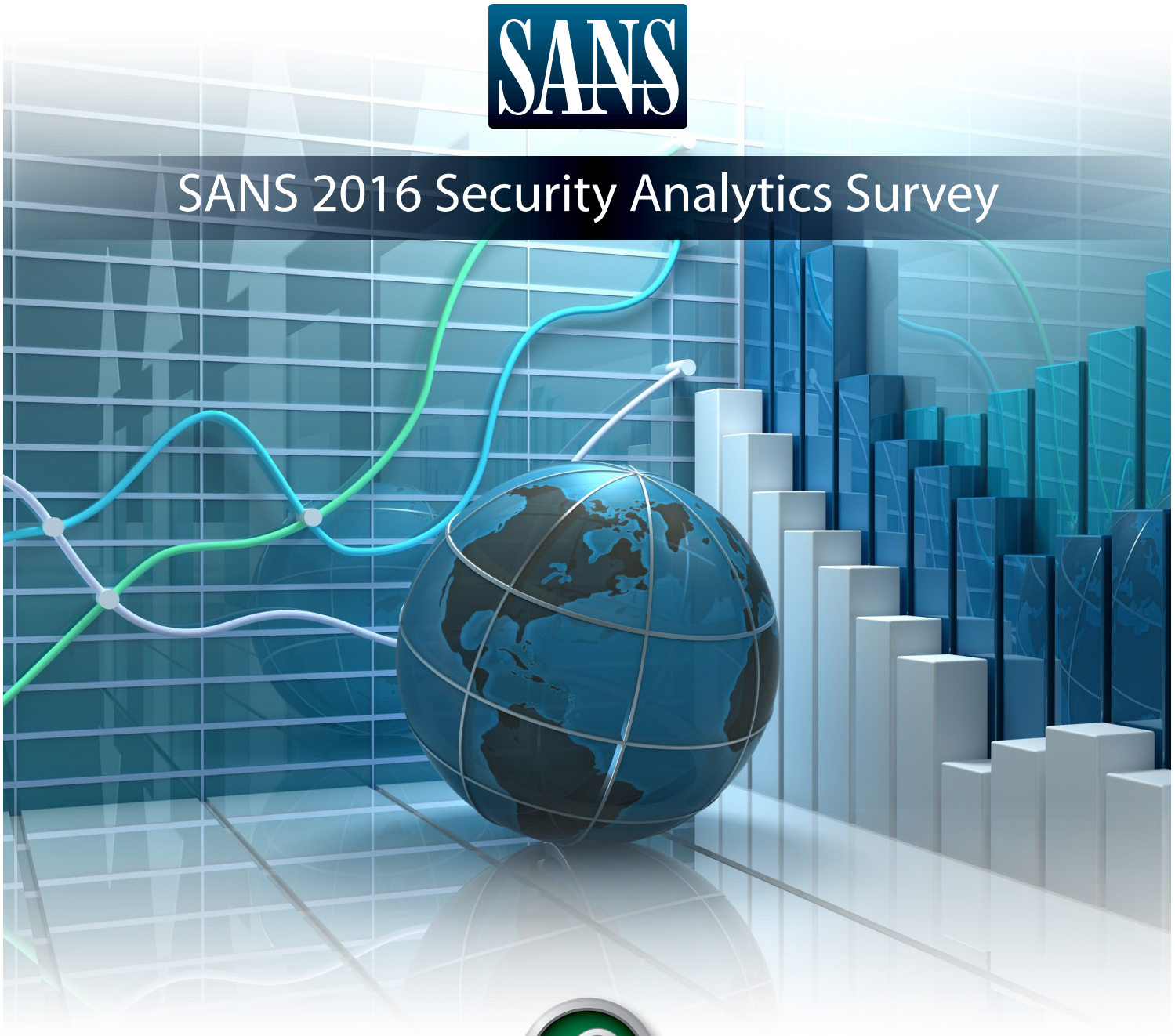
Interested in learning more about security?

SANS Institute InfoSec Reading Room

SANS 2016 Security Analytics Survey

Survey respondents have become more aware of the value of analytics and have moved beyond using them simply for detection and response to using them to measure and aid in improving their overall risk posture. Still, we ve got a long way to go before analytics truly progresses in many security organizations. Read on to learn more.



SANS 2016 Security Analytics Survey

A SANS Survey

Written by Dave Shackleford

December 2016

Sponsored by
AlienVault, Anomali, LogRhythm, LookingGlass Cyber Solutions, and Rapid7

Executive Summary

When SANS started conducting its security analytics surveys in 2013,[1] few organizations were actively leveraging security analytics platforms, intelligence tools and services. Fewer still had highly or fully automated processes in place for analyzing data and producing effective detection and response strategies. Since then, survey respondents have become more aware of the value of analytics and have moved beyond using them simply for detection and response to using them to measure and aid in improving their overall risk posture.

Of their top three use cases for security analytics data, 38% use analytics for assessing risk, 35% for identifying malicious behaviors within the environment, and 31% for meeting compliance mandates.

While usage of analytics has matured since SANS started conducting this survey, organizations appear to be losing ground on breaches and significant attacks, based on this year's survey results. Fewer respondents (17% in 2016 compared to 25% in 2015)[2] stated that they had not experienced a breach.

As in our past surveys, respondents report they are short on skilled professionals, as well as short on funding and resources to support security analytics. Worse, they're still having trouble baselining "normal" behavior in their environments, a metric necessary to accurately detect, inspect and block anomalous behaviors.

Automation has a lot to do with helping to overcome these issues, yet only 4% consider their analytics capabilities fully automated, and just 22% of respondents are currently using tools that incorporate machine learning. Machine learning offers more insights that could help less-skilled analysts with faster detection, automatic reuse of patterns detected and more.

We've got a long way to go before analytics truly progresses in many security organizations. Without a doubt, the event management, analysis and security operations skills shortage is the biggest inhibitor, and it's also the area most organizations rank as the top focus for future spending.

Analytics Usage

88% utilize analytics to some degree in their prevention programs, **89%** in their detection programs and **86%** in response programs

11% (on average) of respondents do *not* utilize analytics or don't know if they do

33% (the largest group) integrate analytics functions with SIEM systems

66% utilize in-house analytics systems of various types

Automation and Improvements

54% consider their analytics processes "fairly" automated

4% consider their analytics capabilities fully automated, and only 10% consider their environments "highly" automated

44% are able to quantify improvements in detection and response by using analytics

[1] "SANS Security Analytics Survey," www.sans.org/reading-room/whitepapers/analyst/security-analytics-survey-34980

[2] "2015 Analytics and Intelligence Survey," www.sans.org/reading-room/whitepapers/analyst/2015-analytics-intelligence-survey-36432, p. 15.

About the Respondents

Most of the 348 participants who took the 2016 SANS Security Analytics survey were security analysts or administrators, with 37% representing this group. Another 24% were IT or security managers—12% were IT managers, directors or CTOs; and 12% were security managers, directors or CSOs. Various titles, such as security architect, auditor and developer, were lightly represented, with one write-in job title of cyber threat intelligence analyst.

Industry Types

The top seven industries represented in this survey include banking and finance, technology, government, cyber security, education, manufacturing and healthcare. See Figure 1.

What is your organization's primary industry?

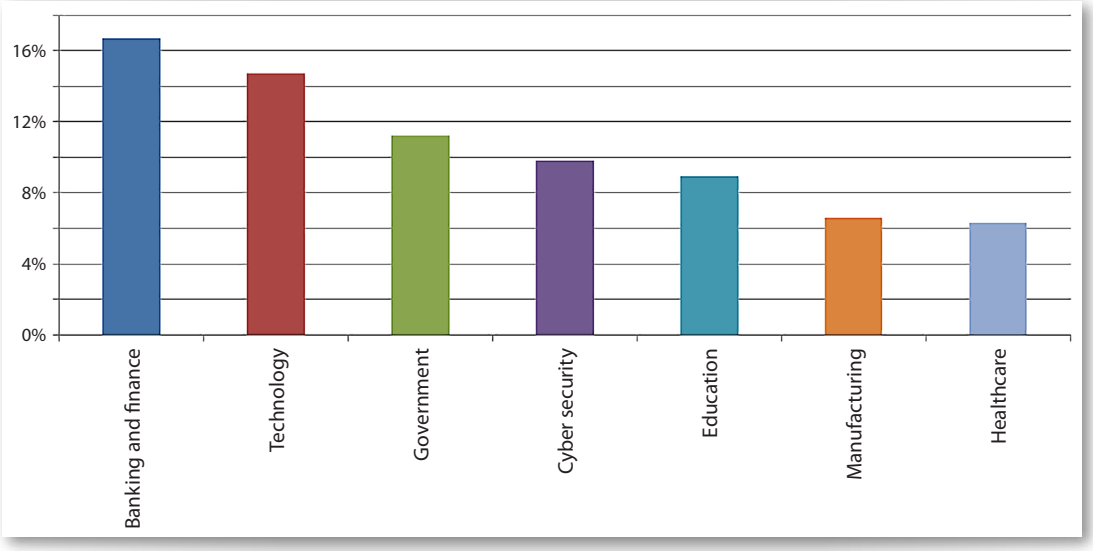


Figure 1. Top Industries Represented

Utilities, telecommunications, insurance, retail, media, transportation, nonprofit and hospitality together totaled another 20% of responses; while "other" represented 6%.

Sizes of Organizations

Organizational sizes represented in the survey sample are fairly balanced between very small, small, medium and large organizations. Just over 29% of respondents work in large organizations with more than 10,000 employees, 31% work for medium-size organizations that have 1,001–10,000 employees, while 23% come from relatively small, 101–1,000 employee, organizations. Another 17% came from small organizations with fewer than 100 employees. See Figure 2.

What is the size of the workforce at your organization, including employees, contractors and consultants?

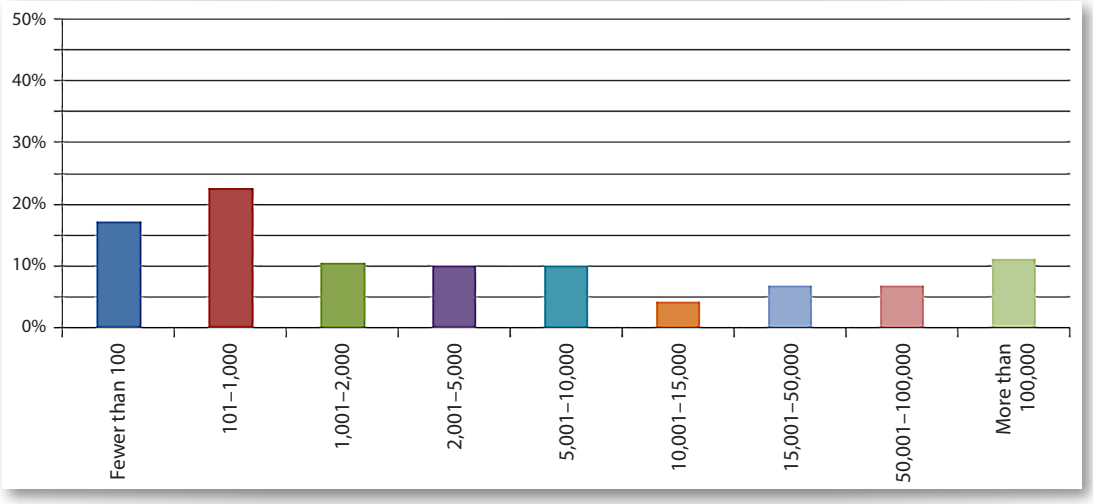


Figure 2. Respondent Organization Size

Global Reach

Most respondents (70%) are headquartered in the United States, with another 12% based in Europe, 9% in Asia, and smaller percentages scattered across other regions and countries.

When it comes to where they also have operations, responses are widely spread. Although 78% of organizations have operations in the U.S., there is significant diversity across other regions, as illustrated in Figure 3.

In what countries or regions does your organization have operations?
Select all that apply.

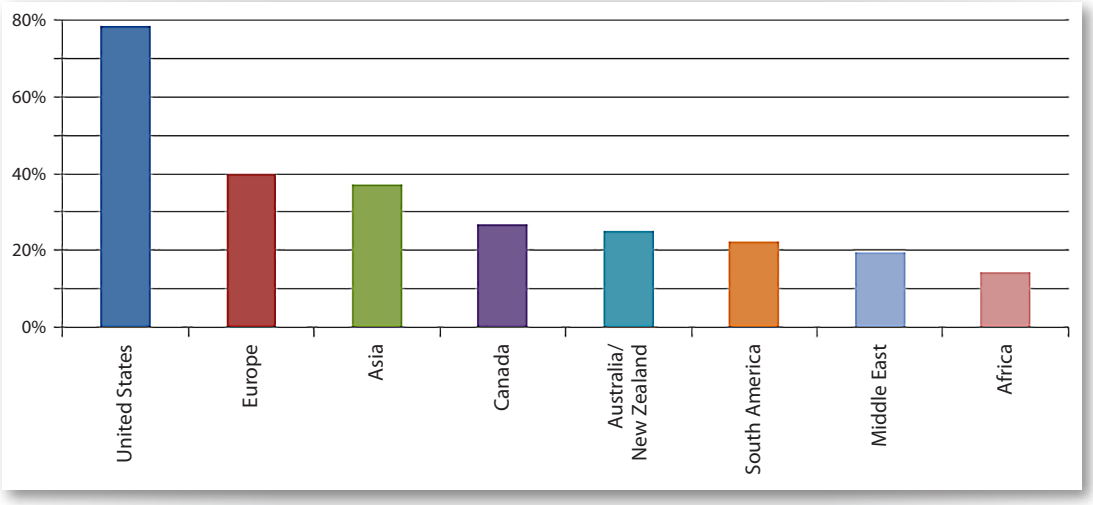


Figure 3. Respondent Geographic Operations (Locations)

Based on the trends we saw emerging in 2015, organizations are focusing on collecting more and more data to perform analytics processing. The more data security teams can collect, the more data can be normalized and baselined to detect malicious or anomalous behavior.

Security Data from Everywhere

Currently, the most common types of data being gathered and aggregated for use with analytics platforms include application logs and events, network security events and vulnerability management data. Host-based anti-malware tools and other endpoint security tools are also popular today. More than half of respondents are gathering data from common security technologies, such as SIEM, log management, and network packet capture and detection tools, too. See Table 1.

Table 1. Systems, Services and Applications Used for Data Collection Today

Systems, Services and Applications	Response
Application information (event logs, audit logs)	86.3%
Network-based firewalls/IPS/IDS/UTM devices	82.5%
Vulnerability management tools (scanners, configuration and patch management, etc.)	77.6%
Endpoint protection (MDM, NAC, log collectors)	72.0%
Host-based anti-malware	70.6%
Dedicated log management platform	65.0%
Whois/DNS/Dig and other Internet lookup tools	62.4%
Security intelligence feeds from third-party services	60.9%
Network packet-based detection	60.3%
SIEM technologies and systems	59.8%
Intelligence from your security vendors	58.6%
Host-based IPS/IDS	57.1%
Relational database management systems (transactions, event logs, audit logs)	53.4%
ID/IAM (identity and access management) systems	50.1%
User behavior monitoring	41.7%
Network-based malware sandbox platforms	41.4%
Cloud activity/Security data	36.2%
Management systems for unstructured data sources (NoSQL, Hadoop)	24.8%
Other	4.7%

In our 2015 survey, 29% conducted intelligence on their cloud environments.[3] In this year's survey, 36% are doing security analytics on their cloud activity, while 45% say they'll be doing so in the future. This increase illustrates the growth potential that analyzing cloud activity represents, which may be driven by organizations beginning to store more critical data in cloud applications.

Other growth areas include unstructured data management tools, with 40% planning this for the future, and user-behavior monitoring, planned for future investment by 37%. Given that network malware sandboxes are still a growing technology, the 41% of respondents' organizations actively incorporating data from them is still lower than some other tools, but another 33% plan to gather data from them in the future, as well.

Collection and Dissemination

TAKEAWAY:

The low amount of cloud activity and security information gathered today represents a major growth area for security analytics.

The largest percentage of respondents (33%) are integrating their security intelligence data with SIEM systems to correlate with a number of other data sources, such as whitelisting, reputation information and more. Another 21% gather data internally from network environments and systems and feed this information into homegrown systems. See Figure 4.

How do you gather and use security intelligence data?
Select the answer that most applies.

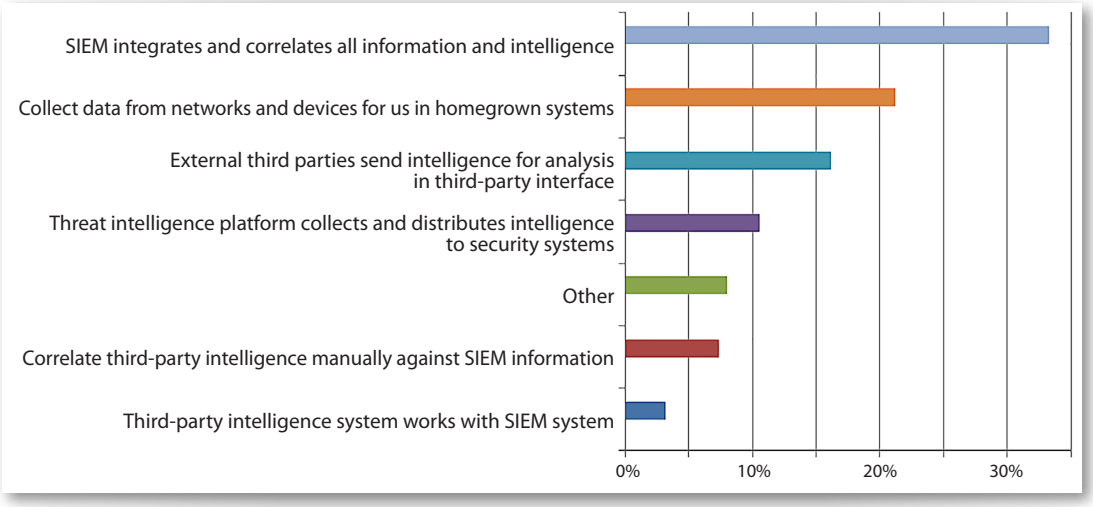


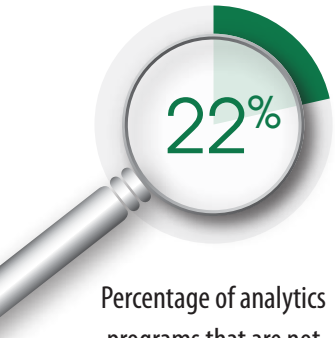
Figure 4. Threat Intelligence Collection and Integration

[3] "2015 Analytics and Intelligence Survey," www.sans.org/reading-room/whitepapers/analyst/2015-analytics-intelligence-survey-36432; Figure 4, p. 4

The development and maintenance of "homegrown systems" often requires significant time from skilled analysts utilizing manual processes. The heavy use of homegrown systems also ties to more security analytics systems being managed in-house. In the survey, 66% are running commercial systems internally, 38% use internally managed open source tools, and 29% use custom-developed in-house systems for analytics processing. Only 27% are leveraging cloud-based tools.

Lagging in Automation

In 2015,[4] only 3% felt that their analytics processes were fully automated, and another 6% stated that they had a "highly automated" intelligence and analytics environment. This year's results were almost identical for these values: 4% were fully automated, while 10% were "highly automated" (a slight increase). In 2015, 51% of respondents stated that their analytics processes were "fairly automated" through internal development, third-party tools or a combination of both. That number went up slightly in 2016 to 54%. Last year, 7% said that their level of automation in pattern recognition was unknown. This number is up to 11% this year, but we also found that 22% are not automated at all. See Table 2.



Percentage of analytics programs that are not automated at all

Table 2. Automation of Pattern Recognition 2015 and 2016

How automated is your pattern recognition process (i.e., ability to develop meaningful patterns of information from your data)?

	2015	2016
Fairly Automated	51.1%	53.7%
Highly Automated	6.4%	9.9%
Fully Automated	3.4%	3.6%
Not Automated	31.8%	22.1%
Unknown	7.4%	10.5%

On one hand, the number of "unknown" answers is higher in 2016, but the number of organizations completely lacking in automation has gone down significantly (from 32% in 2015 to 22%). This is still a new technology for many, and it will likely take some time for organizations to truly automate partially or fully.

[4] "2015 Analytics and Intelligence Survey," www.sans.org/reading-room/whitepapers/analyst/2015-analytics-intelligence-survey-36432, p. 6.

MACHINE LEARNING

Machine learning is the development and use of algorithms that can analyze data, discern patterns and make predictions based on the data and patterns detected, typically using system-to-system-based interactions on a large scale.

Machine learning, an essential part of automating the analytics process, is still not widely utilized by security teams. In our 2016 survey, only 22% are utilizing machine learning capabilities in their analytics programs, while 54% are not. The remaining 24% weren't sure. These results may be affected by differences in the way vendors promote their products as including machine learning and by the number of analysts responding to this survey. Analysts without direct access to the thresholds and algorithms driving their systems may not know whether machine learning is involved.

Detecting Breaches

While machine learning holds promise, a lack of automation capabilities and data science skills to analyze data from multiple tool sets may be partly responsible for a spike in successful breaches and attacks reported in this year's survey. In 2015, just over 23% of respondents didn't know whether they'd been breached; in 2016, 30% couldn't tell whether they'd been breached. Fewer respondents stated that they had *not* experienced a breach in 2016 (17% versus 25% in 2015), and the number of respondents experiencing one to five breaches increased to 32% from 30% in 2015. One positive note is that the number of organizations that experienced 11 to 50 breaches decreased from 11% to 6%. In both 2015 and 2016, less than 5% experienced more than 50 breaches. See Figure 5.

TAKEAWAY:

Based on the survey data, organizations are using analytics more across the board, are seeing improvements in all phases of their security strategies, and have better visibility and response time within their environments, but the number of breaches is rising nonetheless.

How many breaches or significant attacks has your organization experienced in the past two years that required response and remediation?

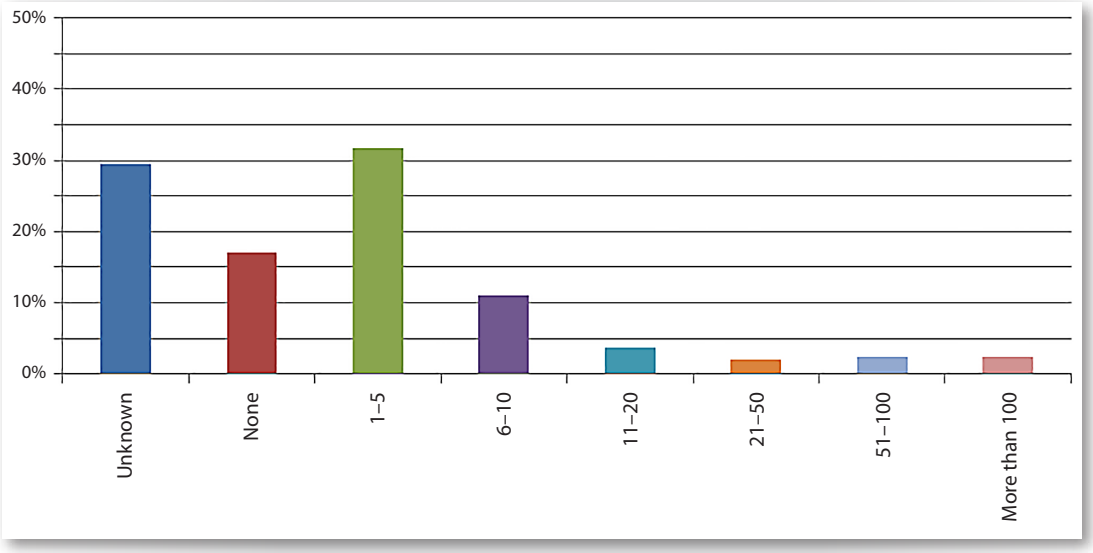


Figure 5. 2016 Breaches Reported

These results may indicate an increase in attack quantity or sophistication, or that organizations are still learning how best to utilize analytics tools and other controls for effective prevention, detection and response. As analytics systems go online, respondents may be more aware of threats they didn't know about before. We hope to see those numbers start coming down as organizations get better at using advanced analytics tools over time.

Responding Faster

On average, respondents to the 2016 survey are detecting affected systems more quickly. Figure 6 illustrates the shortest, longest and average times for detection of affected systems in 2016.

How long were systems impacted before detection?

Select an option for the shortest, the longest and the average time of impact before detection.

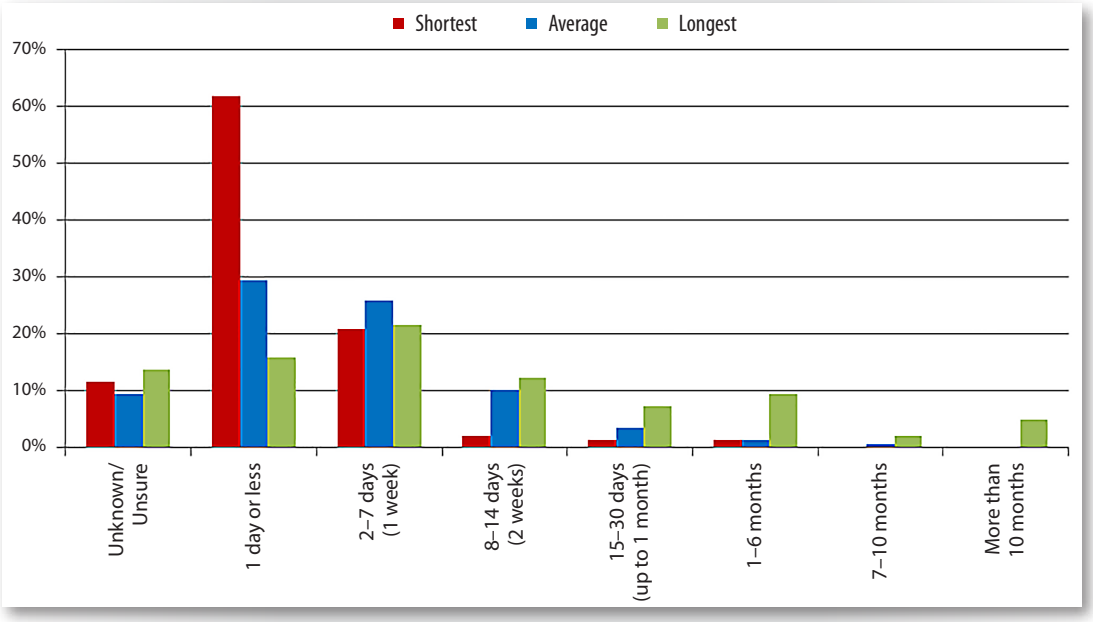


Figure 6. Length of Time Systems Had Been Affected Before Detection

TAKEAWAY:

Security analytics should improve detection and response times as organizations automate more of their processes and learn to accurately baseline normal behavior.

Those time frames are somewhat shorter, in general, than those reported in 2015:

- **Average time to detection decreased.** In 2015, for those that had experienced breaches, 37% indicated that the average time to detection for an impacted system was one week or less. This number decreased to 26% in 2016. In fact, for both years, 30% reported that they could detect an impacted system in one day or less.
- **Shortest time to detection increased.** In 2015, when asked about the shortest time to detection, 71% indicated breaches were usually detected within the same day. In 2016, the shortest time to detect (the same day) decreased to 62%.

  However, the second most frequent response shows a small improvement. In 2015, the second most common response to the shortest time to detection was within one week, chosen by 18%. In 2016, 21% chose within one week.

  Together, the shortest time to detection reported in 2016 is slightly slower than in 2015. Teams appear to be taking somewhat longer to detect and remediate overall, which could also be related to the quantity of breaches, sophistication of attackers, or both.
- **Longest time to detection decreased.** In 2015, some 7% of organizations indicated their longest time to detection was more than 10 months, and this number decreased to 5% in 2016.

Alerting Mechanisms

Endpoint security tools were the top means by which organizations were alerted to their breaches in this year's survey, which is a change from 2015, where the top alerting mechanisms were network and perimeter protection tools such as firewall and IDS. SIEM and other analytics were the second means of alerting in 2016, whereas this was third in 2015. Another noteworthy result was with regard to analytics platform alerting (aside from SIEM), which has increased in importance since 2014,[5] when analytics platform alerting was not even mentioned (again matching the earlier data showing heavier use and reliance on analytics in all phases).

Figure 7 shows the full list of alerting mechanisms that played a role in events and detection scenarios in 2016.

How were these events brought to the attention of the IT and/or security department?

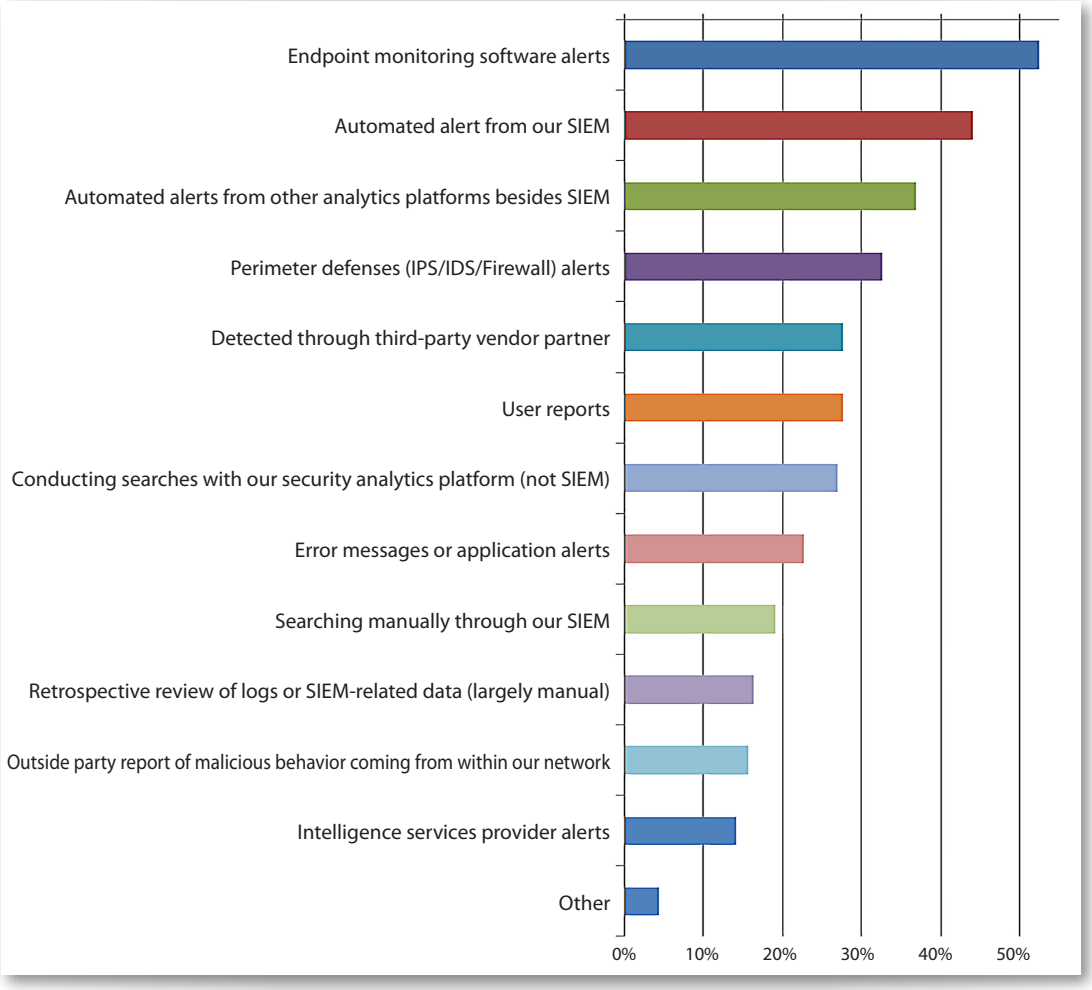


Figure 7. Alerting Mechanisms During Incidents

[5] "Analytics and Intelligence Survey 2014, www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507

Skills Shortage to Blame?

The skills shortage may also be partly responsible for this year's reported rise in breaches. This year, as in our past surveys, a shortage of specific security skills was cited as the top impediment to discovering and following up on attacks. See Figure 8.

What are your three greatest impediments to detection and remediation?

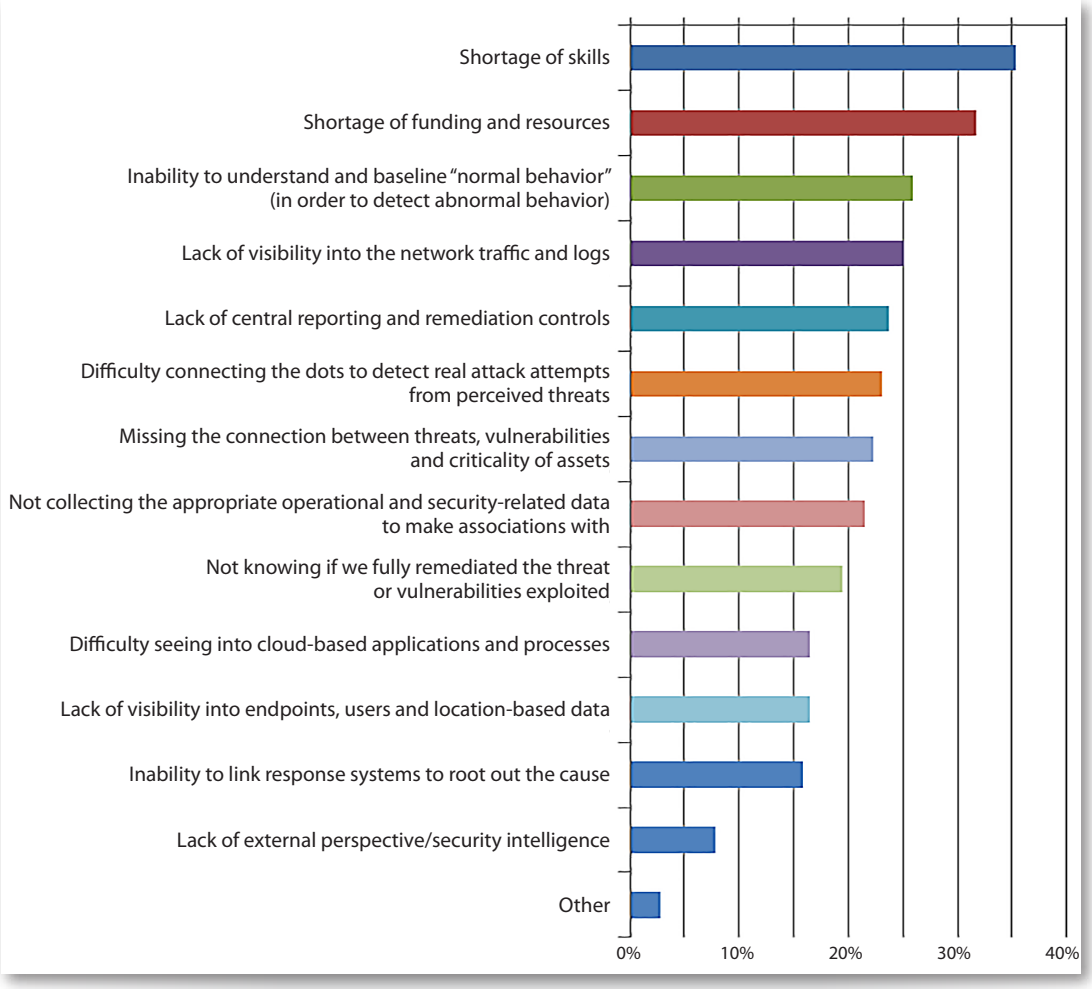


Figure 8. Top Detection and Response Challenges

Besides finding people with the right skill set, 32% of respondents cited lack of funding and resources as a major impediment. Baselining "normal" behavior (and creating pattern matches for anomalies) was also cited as a top challenge by many, and this was observed in 2015 as well (likely coinciding with organizations slowly maturing their analytics programs).

TAKEAWAY:

Attracting the needed skill sets is difficult due to the incredibly high demand for security engineers and analysts who understand SIEM and correlation, forensics, event management, and now, with analytics in the mix, pattern analysis across large, diverse data sets.

As in past years, we strove to determine how analytics was playing a role in all phases of a security program today (prevention, detection and response). In 2015, most organizations were fairly even across the board. The majority reported using analytics in all phases to at least a moderate extent. In 2016, we tried to get a better handle on usage. The highest number of responses in all phases points to use of analytics 75% of the time or more across the board! This is a very significant shift from last year. The breakdown of each phase and how analytics is used in each is shown in Figure 9.

How often do you use security analytics in prevention, detection and response?

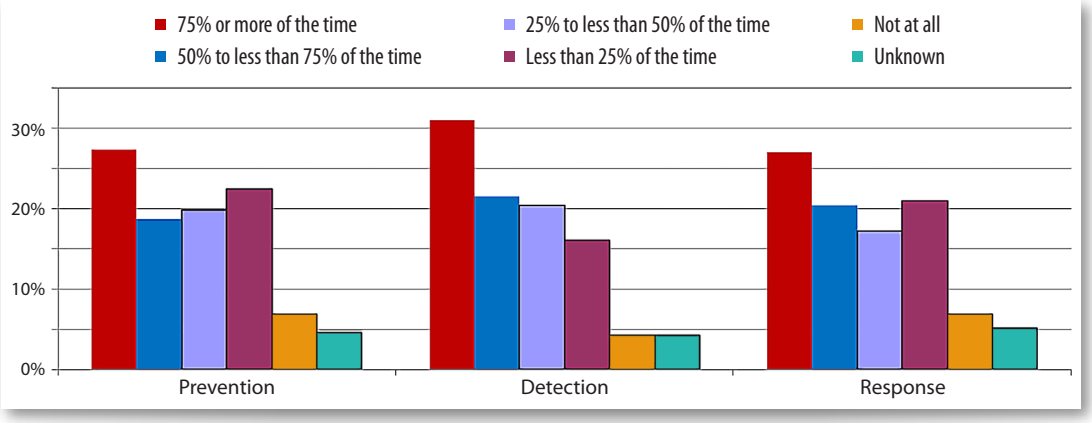


Figure 9. Analytics' Role in Security Program Phases

Across phases, the highest use overall was for detection, but response and prevention were not far behind.

Getting Value

Assessing risk was still the top primary use case in 2016, followed by a fairly even mix of identifying suspicious user behavior, compliance monitoring and detecting external malware threats. Insider threat identification and gaining visibility into network and endpoint behaviors round out the top five overall use cases for 2016. Last year's top use cases included assessing risk posed by threat indicators, detection of external malware-based threats, and system behavior baselining for exception-based monitoring.

The third most important use case two years ago, in 2014, was "visibility into network and endpoint behaviors," which ranked fifth in 2016. Figure 10 shows the top benefits of analytics platforms, according to respondents.

What are your most valuable use cases when leveraging security analytics and intelligence?

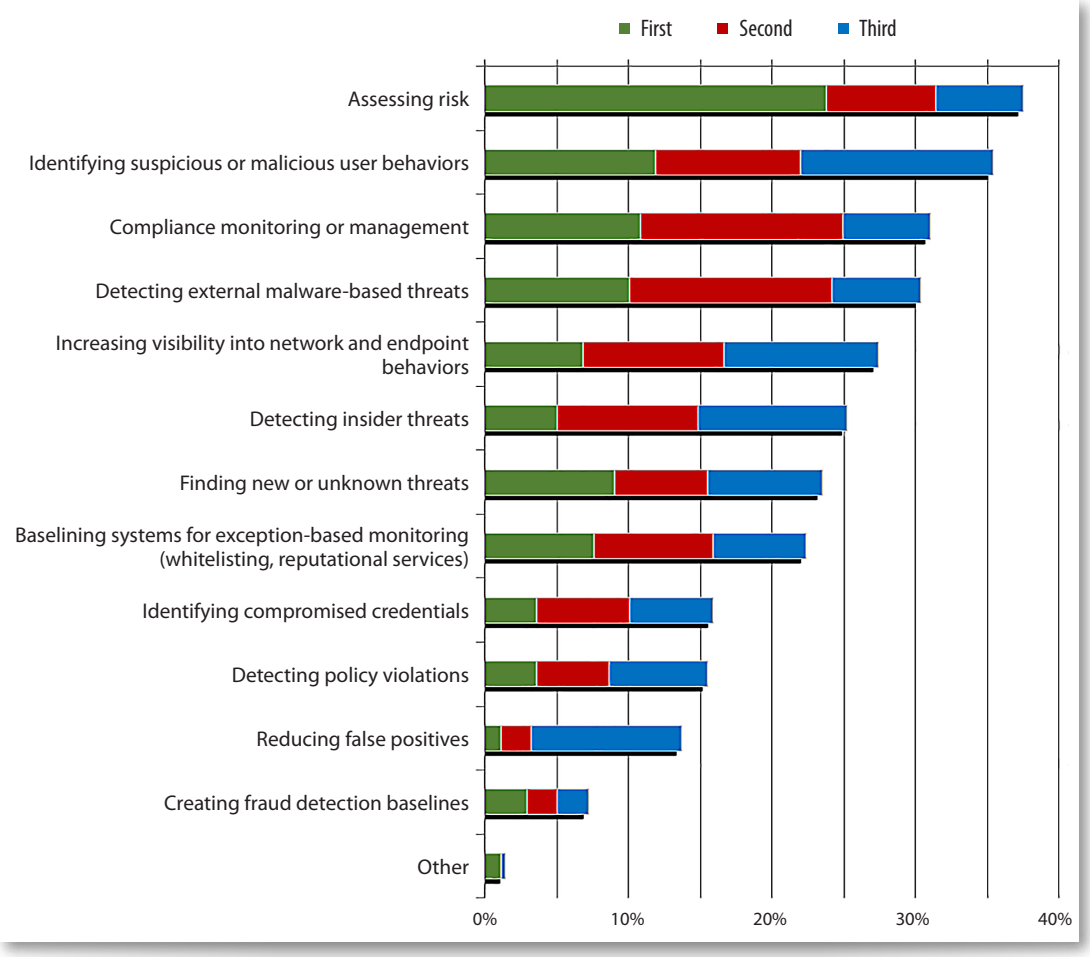


Figure 10. Most Valuable Benefits of Analytics Tools Today

Overall, responses indicate that we now have more and better data coming from systems and networks, and analytics are playing a more central role in determining the real risks we face from threats in our environment at all levels.

Quantifying Improvements

According to survey results, 44% of organizations were able to quantify improvements in their programs as a result of using analytics tools, which is down from 50% in 2015.

Of those that could quantify improvements, 17% of respondents stated that they had seen 76% to 100% improvement in their visibility into actual events or breaches (an increase from the 11% who reported 100% improvement in 2015).[6] Most reported improvements due to use of security analytics and intelligence across all categories are in the "between 26% and 50%" category, represented by the blue bar in Figure 11.

How much improvement has your organization experienced in the following areas as a result of its use of security analytics and intelligence?

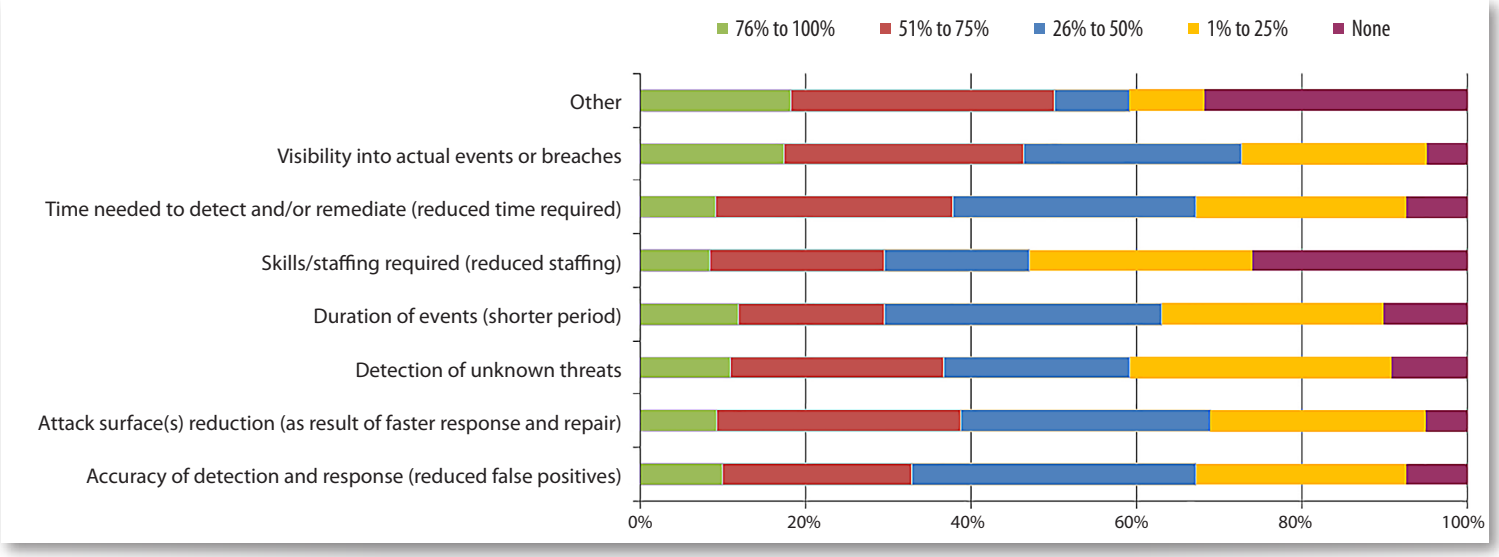


Figure 11. Improvements in Analytics Capabilities

Another category that saw significant improvement is reduction of time to detect threats and incidents and remediate them. This is an area where many security operations teams already have metrics in place, and tracking the amount of time involved in initial detection, opening tickets, investigating and closing out incidents is something they're actively doing.

In 2015, we predicted that this area would improve, and that seems to be the case. Another area that improved significantly was in detection of unknown threats. In 2016, 36% saw 51% to 100% improvement. Clearly, analytics systems are getting faster, more intelligent and more intuitive about what is going on within the environment.

[6] In 2015, respondents could choose 25%, 50%, 75% or 100% improvement. For 2016, the options were ranges of improvement. We have assumed that any respondents from 2015 who wished to indicate greater than a discrete percentage marked the next highest option.

Capabilities Improving

Regardless of their lack of automation, survey respondents are finding analytics tools and capabilities more valuable in improving their detection and response capabilities.

In this year's survey, as in past surveys, few respondents are currently "very satisfied" with the capabilities of their analytics platforms. Yet, satisfaction with various capabilities is inching higher. In 2016, 15% were very satisfied in the system's ability to identify compromised credentials and phishing attacks, up 1% from 2015. Ability to baseline what is normal behavior and then alert on exceptions also improved by 1% from 13% in 2015 to 14% in 2016.

In this year's survey (2016), 16% of organizations were "very satisfied" with their time to detect, followed by identifying compromised credentials, and the same percentage was "very satisfied" with integration with detection and response systems. Another 54% were satisfied with performance and response time, tied with appropriate queries and reports, followed by time to respond. Inversely, 46% were least satisfied with visibility into the adversary infrastructure, followed by ability to accurately predict and prevent unknown threats.

The level of satisfaction with various analytics capabilities is shown in Table 3, which is ordered from the highest level of combined satisfaction to the lowest, with yellow shading indicating the highest percentage and blue shading representing the second highest percentage.

Table 3. Satisfaction with Analytics Capabilities

Answer Options	Very Satisfied	Satisfied	Not Satisfied
Performance and response time	15.1%	54.1%	26.5%
Appropriate queries/meaningful reports	12.9%	54.1%	28.0%
Alert based on exceptions to what is "normal" and approved	13.6%	53.4%	27.6%
Time to respond	12.9%	53.8%	30.1%
Identify compromised credentials and phishing attacks	15.4%	49.5%	30.1%
Quickly correlate events to users	12.5%	51.3%	31.9%
Time to detect	16.1%	47.3%	34.1%
False positives and/or false negatives	11.5%	49.8%	34.8%
Integration with detection and response systems	15.4%	45.5%	34.8%
Cost of tools, maintenance and personnel	10.8%	47.0%	37.6%
Accurately predict and prevent unknown threats	11.8%	43.7%	40.9%
Visibility into actionable security events across disparate systems and users, including cloud services and mobile devices	12.2%	42.3%	38.7%
Single consistent view across reports and alerts	14.7%	38.7%	39.1%
Visibility into external adversary infrastructure	9.3%	36.2%	45.5%
Other	3.2%	7.2%	6.1%

The level of satisfaction went down in some areas since last year. For example, in our 2015 survey, 15% said they were very satisfied with the capability to quickly correlate events to users, and only 13% were very satisfied with this capability in 2016.

Many respondents were still unsatisfied with visibility into external adversary infrastructures based on intelligence and analytics processing, but the situation has improved slightly, as illustrated by a decrease in dissatisfaction from 53% in 2015 to 46% in 2016. An additional 41% were also dissatisfied with their analytics tools' capabilities of accurately predicting and preventing unknown threats, followed by dissatisfaction with the ability to have a single consistent view across reports and alerts and visibility into actionable security events across disparate systems and users, including cloud services and mobile devices (both roughly 10 percentage points down from 2015).

TAKEAWAY:

The percentage of those not satisfied with performance and response time has actually improved (27% were not satisfied with this capability in 2016, compared to 32% in 2015). This means the products in use have gotten faster, even with higher data quantities and processing requirements.

Big Data vs. Security Analytics

In 2015, security teams were evenly split on whether they thought "security analytics" and "big data security analytics" were different in any meaningful way. That's changed in 2016, where more teams DO feel there is a distinction between true "big data analytics" and "security analytics," as shown in Figure 12.

In 2015, the majority of organizations acknowledged that "big data analytics" is here to stay, and many said it provided better visibility into events. Do you see a distinction between security analytics and "big data" security analytics? If so, why?

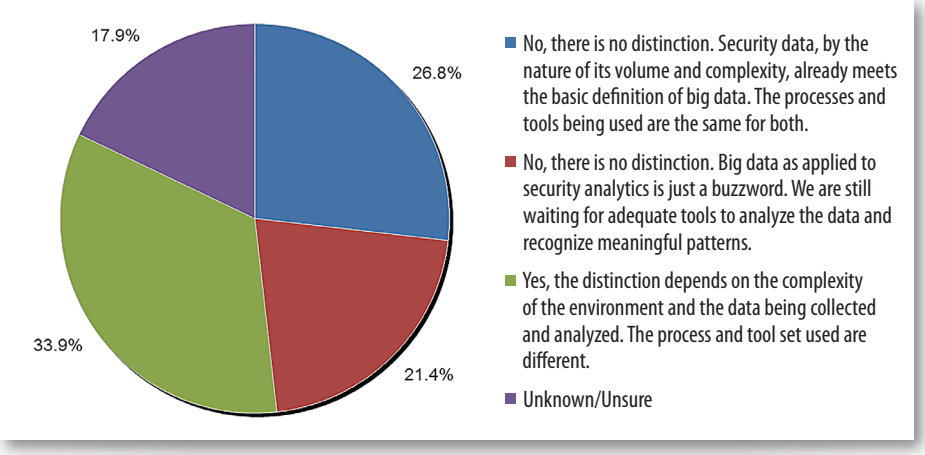


Figure 12. Distinctions Between Security and "Big Data" Analytics

Most security teams seem to feel that large quantities of data are crucial to proper analytics processing, but for the first time, more are making a distinction between "security analytics" and "big data security analytics." This trend is heartening, because security analytics bakes in the technologies needed to analyze large datasets into solutions designed for security professionals to use.

Looking Ahead

Organizations will continue to work on staffing and skills for as long as there are shortages. Much like 2015, training and staffing topped the list of future investments organizations will make to fill the gaps in their security analytics and intelligence programs, with 49% selecting this option in our current survey. See Figure 13.

What are your top three areas for future investment related to security analytics and security intelligence to enable a stronger security posture for your organization?

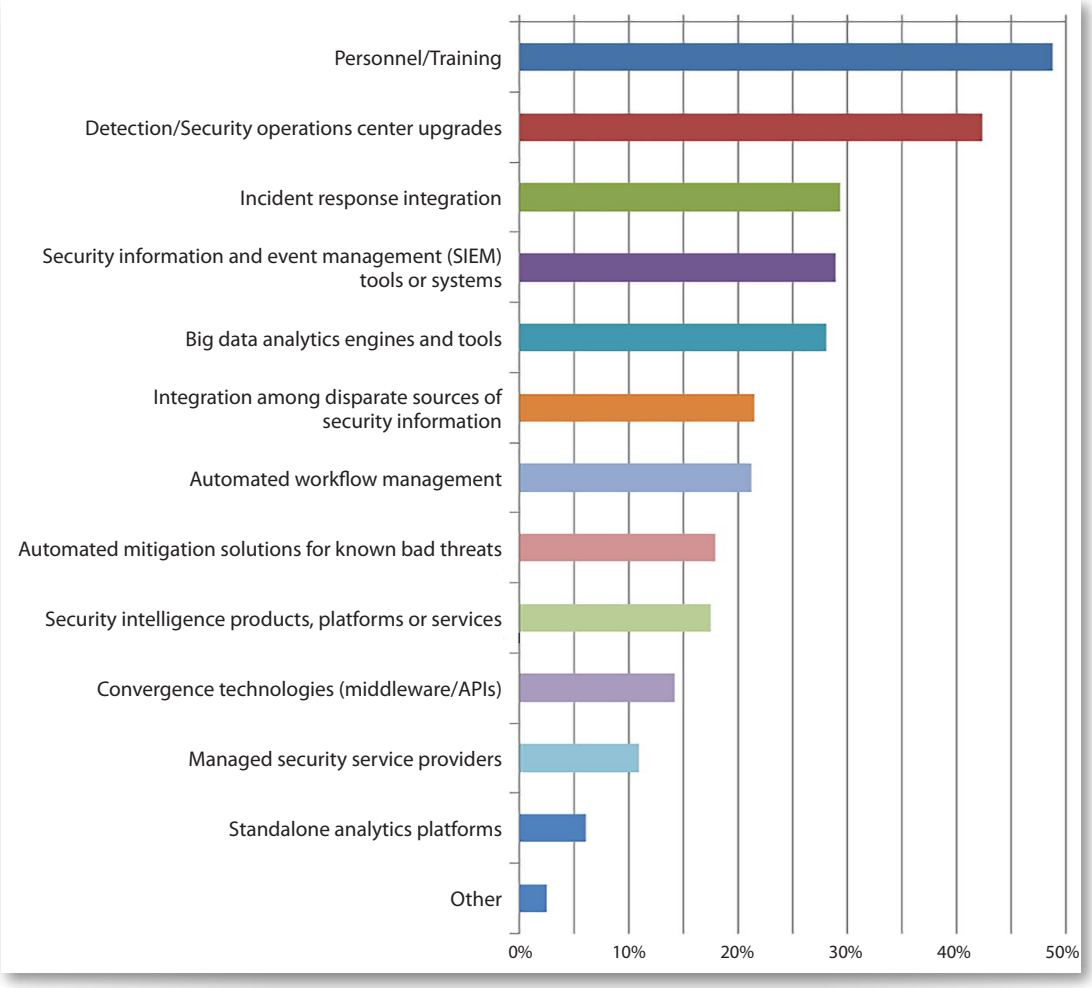


Figure 13. Future Investments Related to Security Analytics

In 2016, we saw organizations choosing to invest in detection and security operations center upgrades (42%) and incident response integration (29%). In 2015, however, SIEM tools came in second place, with incident response tools in third. Security intelligence products and services decreased from 43% in 2015 to 18% overall in 2016, which may indicate organizations are currently placing more emphasis on internal data collection than on third-party products and services.

Conclusion

Despite the varying degrees of maturity represented in this survey, organizations are feeling more confident than ever in their use of security analytics. In this year's survey, 21% indicated that they were highly confident that their security analytics and intelligence systems were effectively protecting their organizations, and another 52% were somewhat confident. When asked to compare their confidence levels, 39% were more confident in their capabilities this year than last year, with another 36% indicating no change in their confidence.

Security folks are hesitant to be overconfident, so these numbers are encouraging. Despite the nasty breach landscape we're facing, security teams feel as if they are getting better at finding threats with analytics and hope they are preventing attacks and breaches from occurring as well.

More teams are using analytics tools, and we're definitely collecting more and better data. Our biggest issue today, much as it was in 2015, is that we're not using the data very well to improve detection and response. Even though we're finding unknown threats more readily, we're still not doing a good job of prioritizing threats, centralizing remediation and reporting, or baselining normal patterns of behavior versus those that are anomalous in nature.

Much of this is due to a chronic lack of skills in the security operations center (SOC), as well as a surprising lack of management support and funding for more advanced tools and tactics for detection and response. Teams are having a difficult time finding the right skills today, and as in the 2015 survey, many organizations are planning to invest in training and hiring in the future.

Utilization of security analytics is slowly improving, and we've done a much better job of collecting data, but more effort is needed to detect, respond and report results using analytics before we can say we're really maturing in this space.

About the Author

Dave Shackleford, a SANS analyst, instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsors

SANS would like to thank this survey's sponsors:

ALIEN VAULT

ANOMALI™

LogRhythm®
The Security Intelligence Company

LOOKINGGLASS

RAPID7

Last Updated: August 1st, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS SEC460: Enterprise Threat	San Diego, CAUS	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Antonio 2017	OnlineTXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced