2015 Analytics and Intelligence Survey

A SANS Survey

Written by Dave Shackleford

November 2015

Sponsored by
DomainTools

Introduction

In 2014, security professionals who took the SANS Analytics and Intelligence Survey[1] told SANS that they were struggling with visibility into their environments. During that survey period, few organizations were actively leveraging analytics and intelligence tools and services, and even fewer teams had highly or fully automated processes in place for analyzing data and producing effective detection and response strategies. Due to their ineffective programs, 24% of respondents also didn't know whether they had been hacked or not.

2014 and 2015 Results Show Some Improvement

2014	2015
35% consider big data as a buzzword	24% think big data is a buzzword
2% think big data is a dead concept	28% see big data and security data as using the same processes and tools
36% were unable to understand and baseline "normal" behavior in the environment	26% still can't understand and baseline normal behavior
30% cited lack of people and skilled dedicated resources	59% cited lack of people and dedicated resources as an impediment

In the 2014 survey, respondents reported difficulties in understanding and baselining "normal" behavior (making it difficult to identify and block abnormal behaviors), and noted a serious lack of skills to support the security operations roles teams were trying to fill.

This year's results seem to indicate slow and steady progress but also underscore a significant lack of maturity in how teams are implementing and using analytics tools.

First, organizations are doing a much better job of collecting more data, and they are getting the data from numerous sources. The use of threat intelligence is increasing, and more professionals are taking analytics platforms seriously. Visibility seems to be improving, but detection and response times are still similar to last year's numbers. Automation of analytics tools and processes seems to be getting better in general, as well.

However, respondents are still hampered by shortages of skilled professionals and are still having trouble baselining behavior in their environments. Now, we're also seeing challenges with central reporting and remediation controls. And even with much more threat intelligence data, we're still not prioritizing threats very well.

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

About the Respondents

A broad range of industries, organization sizes and IT security budgets are represented in the 476 participants who completed the 2015 SANS Security Analytics survey. The top five industries represented include technology and IT services, financial services and insurance, government, education, and health care. Most other major industries were also represented. The majority (26%) work in large organizations with more than 20,000 employees, but many midsize and smaller organizations are also represented, as shown in Figure 1.

How large is your organization's workforce, including both employee and contractor staff?

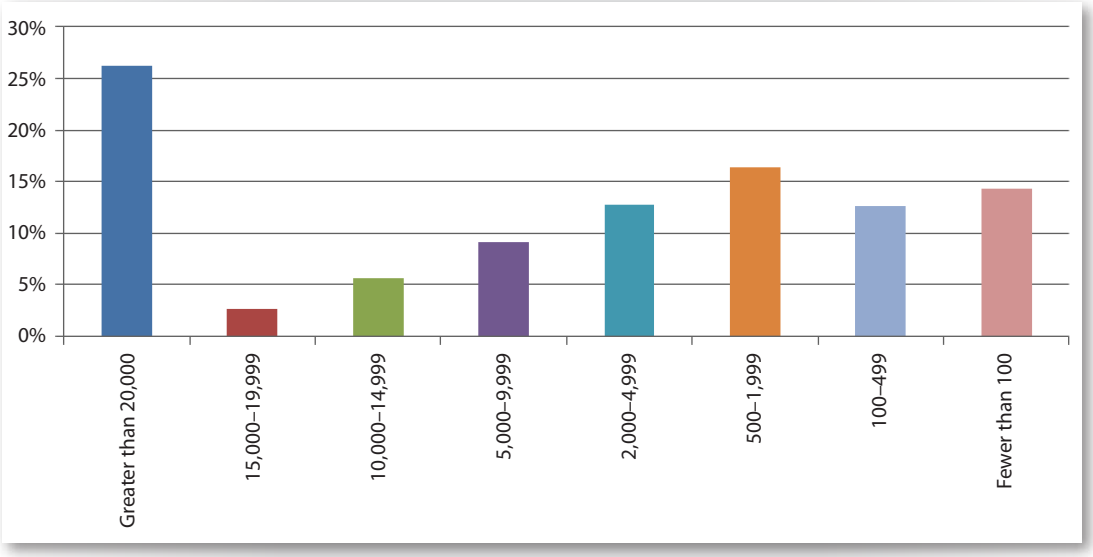


Figure 1. Respondent Organization Size

Many different roles and types of professionals provided data to the survey again this year. Security analysts and security managers (director, chief security officer or chief information security officer) topped the list, but network operations, systems administrators, help desk and support staff, as well as security operations teams, also responded, as seen in Figure 2.

What is your primary role in the organization, whether as an employee or consultant?

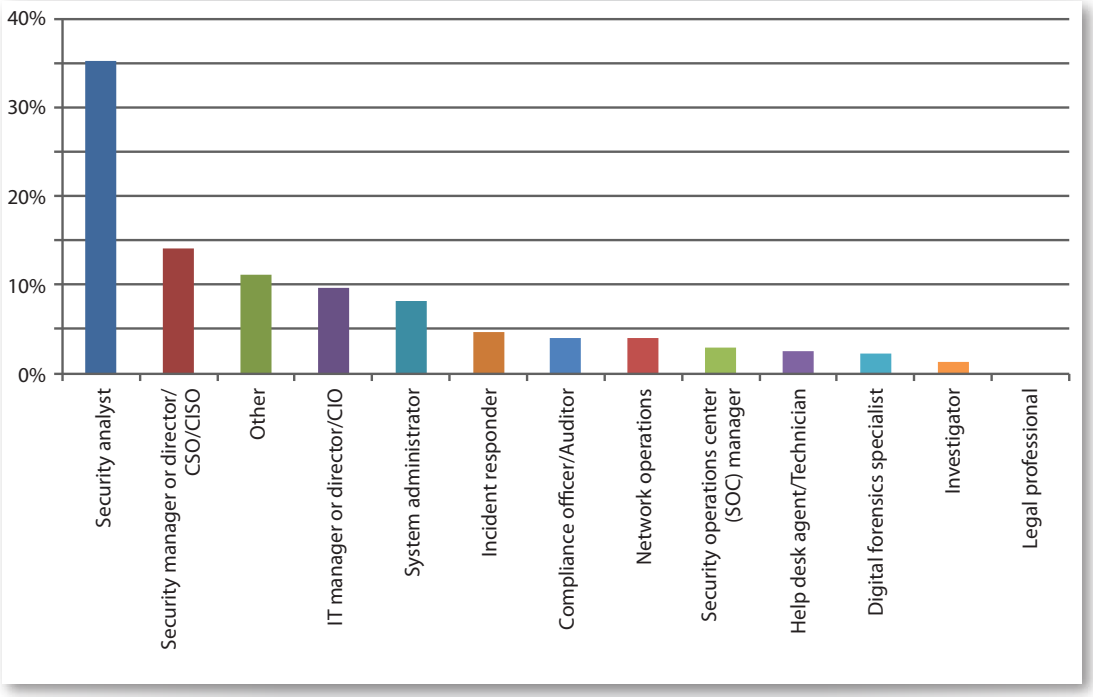


Figure 2. Respondent Roles

Based on survey demographics, 74% of organizations perform incident response activities in the United States, 35% do so in Europe, and smaller percentages do so in numerous other countries and regions, as illustrated in Figure 3.

In what countries or regions does your organization perform incident response activities? *Choose all that apply.*

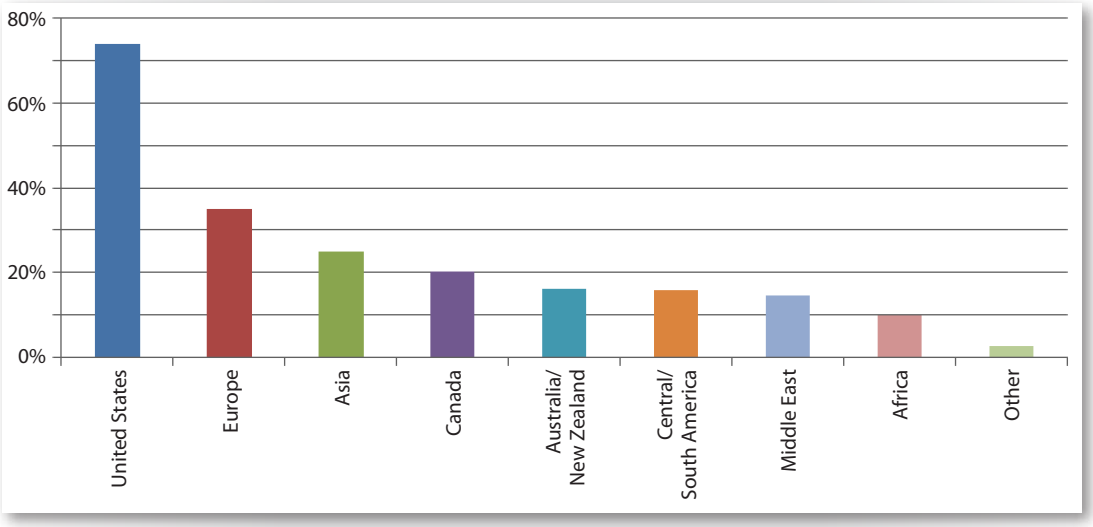


Figure 3. Respondent Incident Response Activities (Locations)

One of the predominant themes of security analytics is increasing the variety and volume of data we're collecting for security analysis today. In an announcement related to security analytics from April 2015, Gartner states, "As security analytics platforms grow in maturity and accuracy, a driving factor for their innovation is how much data can be brought into the analysis."[2] In a nutshell, this is critical because we have more data, and it's all becoming more relevant for security analysis, detection of events, and building better and longer-term baselines of behavior in our environments.

Analytics Data Collected

Our survey results indicate that much data is being collected from many devices for security analytics. Currently, the most common types of data being gathered and aggregated for use with analytics platforms include application logs and events, network-based security platform events (firewalls, IDS, IPS, etc.) and host-based anti-malware tools. Vulnerability management tools (scanners and patch/configuration management) and other endpoint security tools are also popular today. More than half of respondents are also gathering data from common security technologies such as security information and event management (SIEM), log management, and network packet capture and detection tools. See Figure 4.

What type of systems, services and applications are you collecting data from for security analytics?

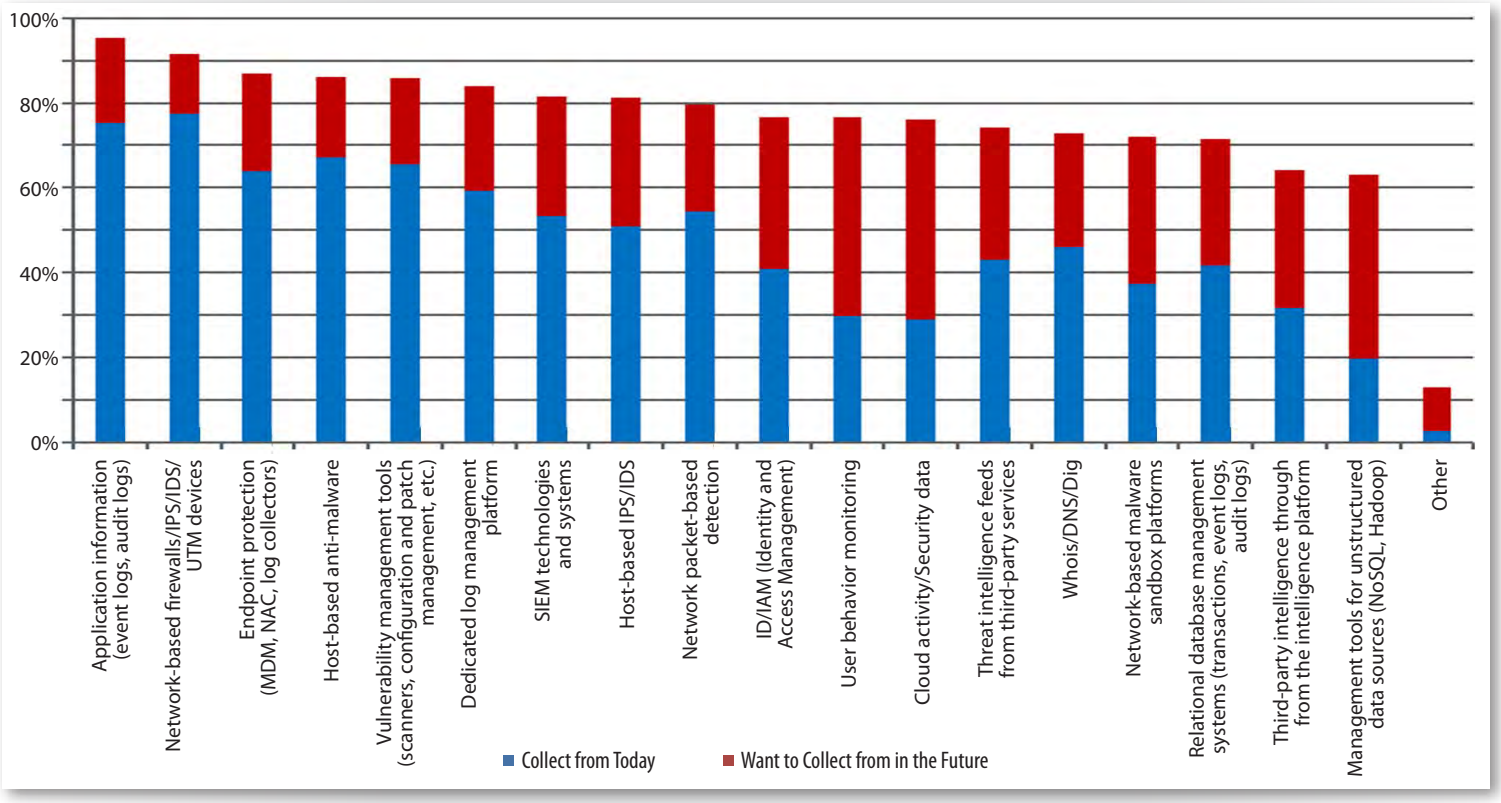
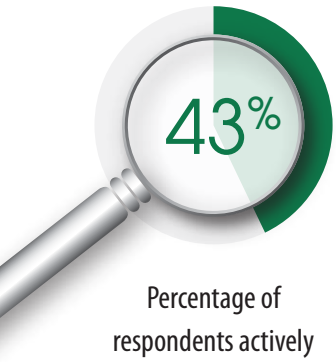
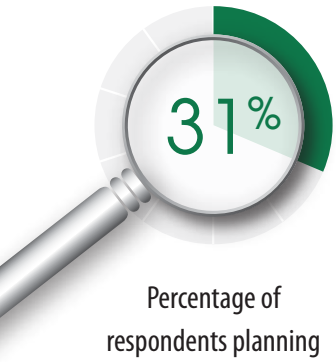


Figure 4. Analytics Data Collected Today and Planned for Collection

[2] www.gartner.com/newsroom/id/3030818



Percentage of respondents actively integrating externally gathered threat intelligence data today



Percentage of respondents planning to do so in the future

The least commonly gathered data types today include events from unstructured data management tools, cloud activity or security data, and user behavior monitoring tools. The low amount of cloud activity and security information (29%) gathered today is disconcerting.

However, cloud activity or security data, selected by 47%, was the most popular answer when respondents were asked what data type they planned to collect in the near future. Respondents also chose user behavior monitoring and unstructured data management tools, with 47% and 43%, respectively, as being on the horizon for collection and inclusion in analytics processing soon.

Given that network malware sandboxes are still a growing technology, the number of organizations actively incorporating data from them (37%) is still lower than some other tools, but another 35% plan to gather data from them in the near future, because such sandboxes can help organizations identify unknown threats and potential zero-day exploits that perform malicious actions.

Multiple Intelligence Sources

Results show that teams are integrating network-based and host-level security intelligence and using central analytics platforms to analyze and correlate the data. In the survey, 43% of respondents are actively integrating data from external threat intelligence providers today, with another 31% planning to do so in the future.

Respondents are also reusing threat intelligence data. We asked if they caught advanced threats through the use of their own intelligence gathering for processing and reuse, or through the use of third-party intelligence or both. By advanced, we mean threats they don't already know about. Just over 44% say they currently collect advanced threat information internally and preserve it for future detection activities, while nearly as many also use third-party intelligence services to inform them of advanced or unknown threats, as shown in Table 1.

Table 1. Reuse of Threat Intelligence Data

Percent of Respondents	Action
44.3%	Collect advanced threat information internally, dissect it and include it for future detection
43.0%	Use external third parties to collect advanced threat information for detection and response
36.2%	Have a security analytics system that handles the intake of intelligence automatically behind the scenes and correlates this against whitelisting/blacklisting and reputational information
32.2%	Have a security analytics system that takes in intelligence and indicators of compromise automatically
30.2%	Correlate manually advanced threat information against information collected in their SIEM
22.5%	Don't correlate their event data with internally gathered intelligence data or external threat intelligence tools
17.8%	Have their SIEM vendor work with intelligence agents and update the intelligence data for them

One significant trend of note is the automatic digestion of intelligence data to analytics and SIEM platforms, which fell into third place with 36%, and even fewer, 32%, are using a security analytics platform to take in threat intelligence and indicators of compromise (IOCs) for forensic detection and response. These results may be due to 43% using external third parties, compared to 31% that used such services in 2014.

Going Backward?

In 2014, 9% of security teams stated that their analytics and intelligence processes for pattern recognition were fully automated, with another 16% asserting that these processes were "highly automated."[3]

Respondents to this year's survey are less confident than they were in 2014. This year, only 3% describe these processes as fully automated, and only 6% see themselves as operating a "highly automated" intelligence and analytics environment. See Table 2.

Table 2. Automation Levels for 2014 and 2015

How automated are your security analytics and intelligence processes (such as combining pattern recognition, whitelists, blacklists and reputational libraries)?	2014	2015
Not automated at all	N/A	31.8%
Fairly automated through internal development	19.4%	14.9%
Fairly automated through third-party intelligence tools or services	14.0%	17.6%
Fairly automated using a combination of third-party tools and internally developed systems	14.0%	18.6%
Fully automated through a combination of third-party and internally developed tools	9.0%	3.4%
Highly automated through third-party intelligence tools or services	11.3%	3.4%
Highly automated using only internally-developed systems	4.5%	3.0%
Unknown	27.9%	7.4%

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

Last year, 28% said that their level of automation in pattern recognition was unknown. This number is down to 7% this year, but we also found that 32% of respondents to this year's survey are still not automated at all. These numbers seem more realistic than last year's, as organizations have had more time to truly integrate analytics capabilities into their environments. This is still a new technology for many, and it will likely take some time to automate partially or fully.

Automation of pattern recognition, whitelists, blacklists and reputational libraries is one indicator of a maturing security analytics program. Organizations can increase the effectiveness of their analytics and intelligence programs by automating analytics and intelligence processes. See the "Machine Learning" section later in this paper, which describes the use of self-learning, behavioral and predictive analysis to continually improve detection and response.

Organizations can increase the effectiveness of their analytics and intelligence programs by automating analytics and intelligence processes.

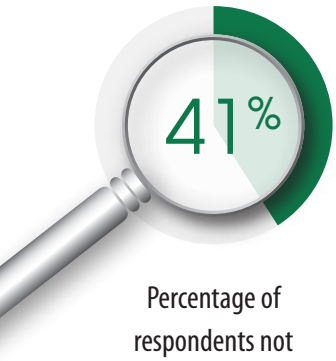
Still in Search of Visibility

The majority of respondents are satisfied with their analytics and intelligence systems, but very few respondents feel "very satisfied," and in some cases, such as with regard to visibility, they are more unsatisfied than satisfied.

For example, 53% of this year's survey respondents are dissatisfied with visibility into external adversary infrastructures based on intelligence and analytics processing. In addition, 42% are dissatisfied with their ability to alert based on exceptions to what is "normal" and approved, 45% aren't happy with their ability to use relevant event context (intelligence) to observe "abnormal behavior" and separate it from normal behavior, and 49% of respondents are not satisfied with visibility into actionable security events across disparate systems and users, including cloud services and mobile devices. The same percentage of respondents is just as dissatisfied with the ability to have a single consistent view across sources of reports and alerts. See Table 3.

Table 3. Satisfaction with Analytics Capabilities

Answer Options	Very Satisfied	Satisfied	Not Satisfied
Ability to alert based on exceptions to what is "normal" and approved	12.6%	42.0%	**41.6%**
Ability to have a single consistent view across sources of reports and alerts	10.9%	35.5%	**49.1%**
Ability to quickly correlate events to users	15.0%	41.6%	38.9%
Performance and response time	11.9%	51.2%	32.4%
Ability to identify compromised credentials and phishing attacks	14.0%	41.3%	39.9%
Integration of intelligence with security response systems for proper response	9.9%	39.9%	43.7%
Reduction of false positives and/or false negatives	8.5%	47.4%	36.9%
Training or expertise required to operate intelligence systems/conduct analysis	8.9%	42.7%	41.0%
Producing or having a library of appropriate queries/meaningful reports	11.9%	36.9%	43.0%
Costs for tools, maintenance and personnel	8.5%	42.3%	40.3%
Relevant event context (intelligence) to observe "abnormal behavior" and separate it from normal behavior	10.9%	35.2%	**45.1%**
Visibility into actionable security events across disparate systems and users, including cloud services and mobile devices	9.2%	32.8%	**49.1%**
Reduction of "mean-time-to-detect" and "mean-time-to-respond" to cyberthreats	10.9%	45.7%	34.1%
Visibility into external adversary infrastructure	7.2%	29.4%	**52.9%**



Percentage of respondents not satisfied with the availability of training and expertise needed to operate analytics and intelligence programs

In 2014, visibility also scored worst in terms of satisfaction: 49% were not satisfied with a single consistent view across systems and users, including cloud services and mobile devices, and 48% were not satisfied with visibility into actionable security events. Satisfaction with performance and response time had the lowest dissatisfaction rates, with just 33% dissatisfied in 2014 and 32% not satisfied in 2015. This means the products in use have not gotten any faster, but that could also be related to higher data quantities and processing requirements.

One area that did improve is the training or expertise required to operate intelligence systems and conduct analysis on events. In 2014, 48% of respondents were not happy with this, and that number has dropped to 41% in 2015, which may indicate that our security operations center (SOC) analysts are retooling their skill sets to better accommodate analytics.

Big Data Reality

Respondents are accepting that big data will continue to be a large part of security analytics. In 2014, nearly 35% of respondents thought "big data" was a buzzword and another 2% thought it was a "dead" concept. This year, 24% think big data is a buzzword, and security teams are evenly split on whether they think "security analytics" and "big data security analytics" are different in any meaningful way, as shown in Figure 5.

In 2014, 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?

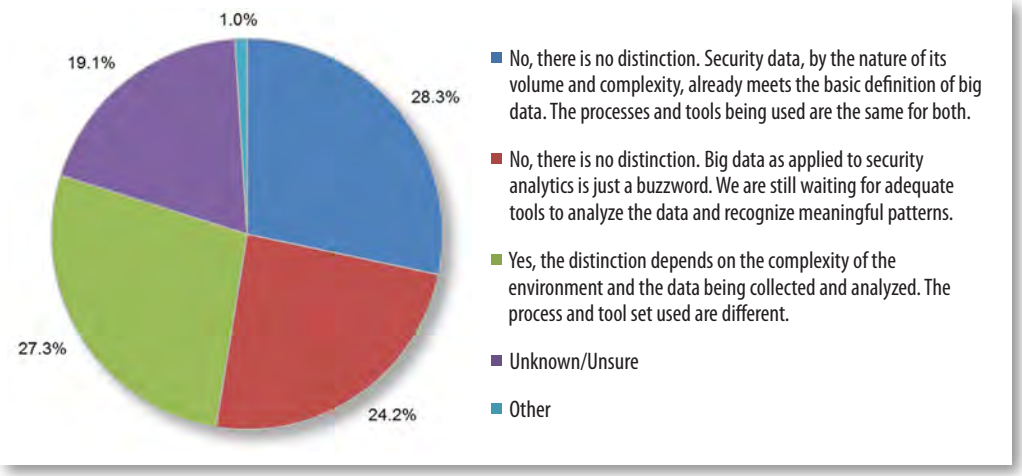


Figure 5. Distinctions Between Security and Big Data Analytics

Most security teams seem to feel that large quantities of data are crucial to proper analytics processing, but many are still unsure as to the distinction between big data and security analytics.

Most security teams seem to feel that large quantities of data are crucial to proper analytics processing, but many are still unsure as to the distinction (if there is one) between big data and security analytics. This may be just a matter of semantics, or it may be that "big data" is a concept usually associated with scientific, statistical and quantitative disciplines, not specifically with information security.

Analytics Usage Today

From a tools perspective, the biggest benefit of using analytics and intelligence tools, hands down, is assessing risk posed by threat indicators, selected by 21% of respondents as the most valuable and by 37% as in the top three benefits. Detection of external malware-based threats, visibility into network and endpoint behaviors, and baselining system behavior for exception-based monitoring were also top wins. Compliance monitoring and management rounds out the top five value areas for analytics. See Figure 6.

Which of the following are you finding most valuable when leveraging security analytics and intelligence tools?

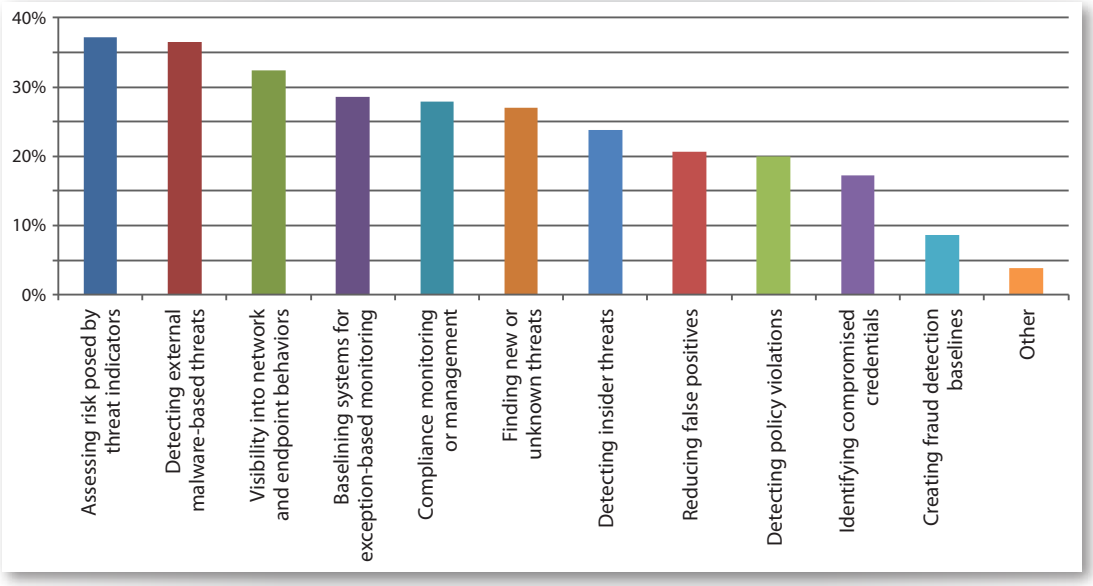
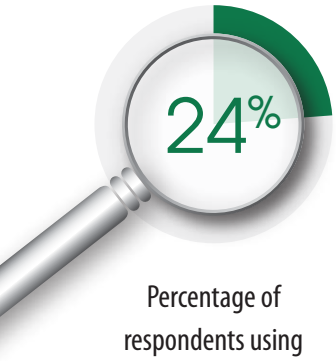


Figure 6. Top Benefits of Using Analytics and Intelligence Tools

This marks some major changes from 2014, when the overwhelming benefit was "finding new or unknown threats," which comes in sixth in 2015, with 27% finding it a top benefit. This change, and the top benefits noted in 2015, indicate that some of the data we're gathering and the threat intelligence we're developing is starting to pay off. We now have more and better threat indicators than ever, and analytics are playing a more central role in determining the real risks we face from those threats versus simply identifying new ones.

Machine Learning

Much has been discussed in the information security community about "machine learning" for improving our detection and response capabilities. In a nutshell, machine learning uses algorithms that can analyze data, discern patterns and make predictions based on the data and patterns detected. Today we are asking our security analytics platforms to collect large and disparate internal datasets, comb through that data looking for patterns and creating correlations, and provide guidance on the anomalies and potential threats we face. Given the different tools available, it is acceptable that these tasks be competed in multiple time frames, including real-time analysis and dumping data for later analysis.



Percentage of respondents using analytics for one or two years

At the same time, many security teams have started incorporating threat intelligence into their datasets to gain perspective on what others are seeing in the wild. We asked respondents whether they were using these methods and technologies, as well as whether they were integrating threat intelligence feeds into their analytics platforms to provide larger datasets and gain deeper insights into behavior in their infrastructure. Integration is occurring, mostly over the past two years, but not on a large scale. See Figure 7.

Estimate how long your organization has used machine-based analytics, how long it has used external threat intelligence services or products, and how long you have integrated these intelligence feeds into a centralized analytics platform.

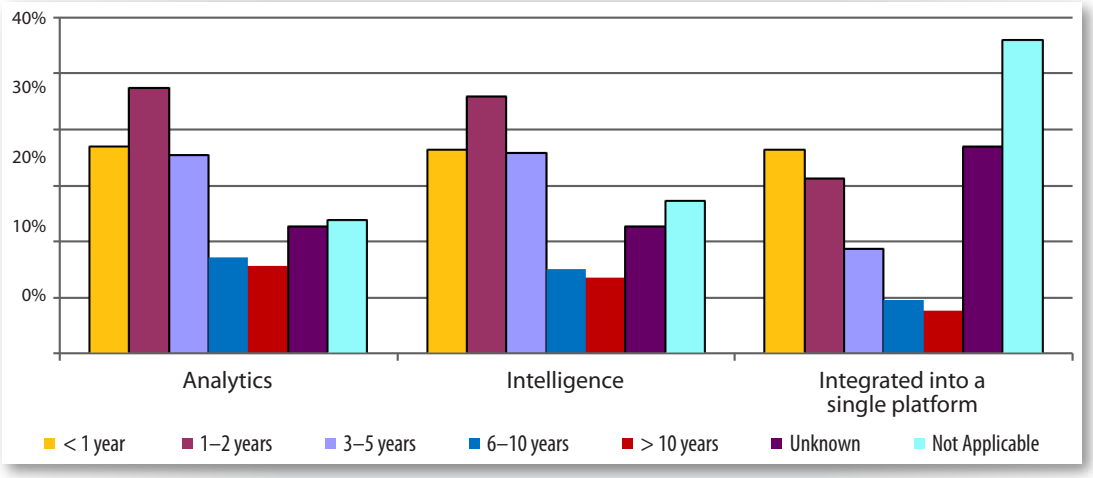


Figure 7. Machine Learning, Threat Intelligence and Analytics Integration Still New

The majority of those using analytics have been using the technology for only one or two years (24%), with another 18% using machine-based analytics for a year or less. Only 8% have been using analytics for longer than 10 years. These numbers are very similar to those for users of external threat intelligence products and services, with the largest percentage (23%) using the products for one or two years, and the second-largest (18%) using threat intelligence for less than one year.

It's also obvious that integrating analytics and intelligence into a single platform isn't yet mature. This is a very new technology set, with 34% of organizations leveraging this for two years or less. For the majority, integration of analytics and threat intelligence hasn't happened yet (28%) or they're unsure of what they may have in place (18%). These numbers aren't surprising given the relative newness of the space.

Using Analytics Data

TAKEAWAY:

In the past several years, more organizations have started seeing benefits to adopting both analytics and intelligence technologies, but many are still relying on traditional tools for data aggregation, detection and response activities.

The majority of respondents are right in the middle of the adoption curve for all phases of analytics data uses (collection, detection, response and reporting). For collection, however, respondents are slightly above average in adoption, with 22% of responses indicating significant or extensive use of analytics during this phase. This makes sense, as analytics tools and analysis platforms are focused on large datasets. See Figure 8.

To what degree do you use analytics in each phase of your security program?
Indicate your usage from 1 (Not at all) to 5 (Extensively).

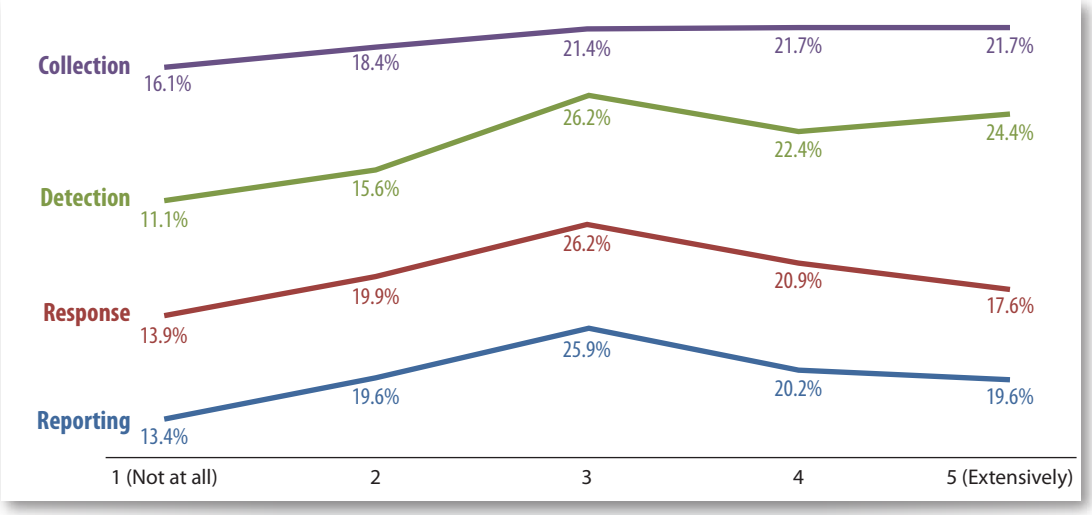


Figure 8. Analytics' Role in Security Program Phases

13.4%

13.9%

11.1%

Another telling data point is that all but 11% were using analytics tools for detection. In fact, detection seems to be the phase of a security program most likely to have heavy analytics use currently, with the highest numbers across the board compared to other phases. Security operations teams are obviously finding some success in putting the data to use, finding more indicators of compromise and identifying more distinct patterns of anomalous behavior than ever.

According to survey results, 50% of organizations were able to quantify improvements in their programs as a result of using analytics tools. Some respondents (11%) stated that they had seen 100% improvement in their visibility into actual events or breaches, but most noted that improvements came in between 25% and 75% across all categories. The following are some relevant statistics for each area listed in Table 4.

Table 4. Improvements Attributed to Use of Analytics Tools

	Percentage of Improvement		
	25%	50%	75%
Accuracy of detection/response (reduced false positives)	27.4%	24.2%	25.3%
Attack surface(s) reduction (as result of response/repair)	26.9%	28.5%	21.0%
Detection of unknown threats	23.1%	26.9%	19.9%
Duration of events	24.2%	21.0%	18.8%
Reduced time to detect and/or remediate	21.0%	31.2%	23.7%
Skills/staffing reduction for detection and response	16.1%	18.8%	18.3%
Visibility into actual events or breaches	23.1%	25.8%	23.1%

Another category that saw significant improvement is reduction of time to detect threats and incidents and respond to them. Based on experience, this is an area in which 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. Seeing definitive improvements with analytics in this area is a trend that will likely continue in the near future.

Dearth of Skills

One of the major challenges cited in the 2014 report was finding qualified personnel with the right skill sets to configure and operate analytics platforms. Currently, most organizations have between 2–4 full-time employees/equivalents (FTEs) for both detection and response responsibilities. Close to 14% have 5–10 FTEs, and roughly 12% have 11–25. Approximately 26% of respondents have one or fewer FTEs for detection and response, with a small number (from very large organizations) having more than 25. Most organizations are struggling mightily with finding the right skill sets to properly operate and maintain a security analytics platform for detection and response. In fact, this was overwhelmingly cited as the top impediment to discovering and following up on attacks today, as illustrated in Figure 9 on the next page.

What are your greatest impediments to discovering and following up on attacks?

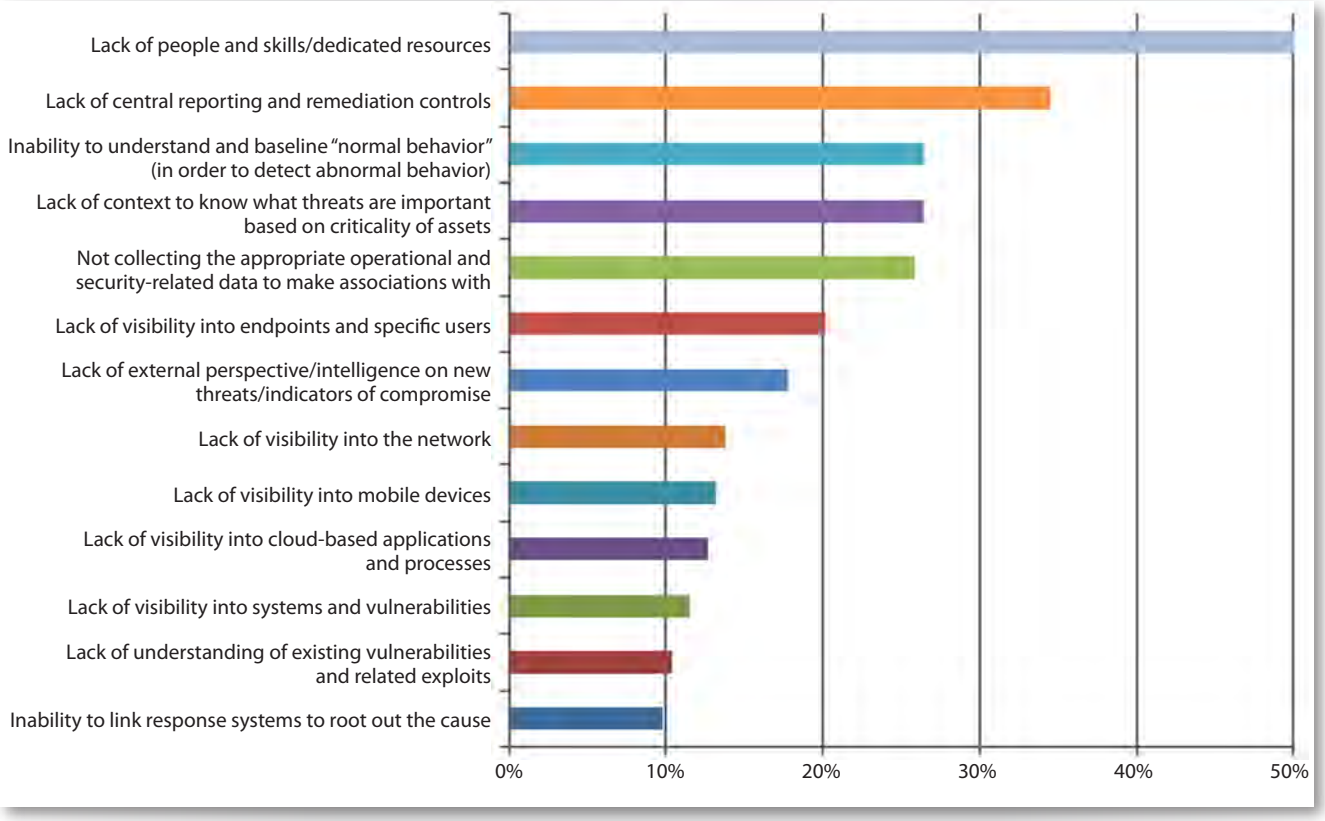


Figure 9. Detection and Response Challenges

Last year more organizations were just getting started with analytics, so data collection and visibility were bigger headaches. This year, using that data effectively has been more of an issue.

Finding these skill sets in today's marketplace is difficult due to incredibly high demand for top talent that understands SIEM and correlation, forensics, event management and now, with analytics in the mix, pattern analysis across large diverse datasets. This challenge was ranked third (30% of responses) in the 2014 survey, indicating that this problem is actually getting worse.

Centralizing and Prioritizing

Besides finding people with the right skill set, lack of central reporting and remediation controls, and lack of information for prioritization of threats were the top major hurdles organizations experienced with analytics platforms. Baselining "normal" behavior (and creating pattern matches for anomalies), the second-worst problem in 2014, was also cited as a top challenge by many. Given its shift in position, baselining may be getting better as teams learn more and tools improve.

Results also indicate that security personnel are having trouble developing normal and anomalous baselines, prioritizing threats, and reporting the appropriate metrics and risks using analytics.

This likely represents a natural learning curve. Last year more organizations were just getting started with analytics, so data collection and visibility were bigger headaches. This year, using that data effectively has been more of an issue. This could also be related to organizations having trouble finding the right people to get these initiatives moving!

Detection and Response

Organizations are still experiencing breaches. But are we seeing fewer than in the past? In 2014, 24% of respondents didn't know whether they'd been hacked, which has decreased slightly to just over 23% in 2015. More respondents stated that they had not experienced a breach in 2015 (25% versus 21% in 2014), and the biggest category (2–5 breaches) stayed exactly the same (23%). However, the number of organizations that experienced between 11 and 50 breaches increased by a small percentage (9% to 11%).

In general, these numbers indicate that people's fundamental detection and response capabilities may have improved somewhat, but prevention capabilities may have stayed relatively static. In other words, we know more about our environments and may be better equipped to detect the presence of attacks and breaches than in the past (as well as respond to them), but the breaches are still occurring, nonetheless. See Table 5 for some comparative statistics between 2014 and 2015.

Table 5. Time to Detect, 2014–2015

How long were systems impacted before detection?
(Select an option for the shortest, the longest and the average time of impact before detection.)

		Within the same day	One week or less	One month or less	Three months or less	Five months or less	10 months or less	More than 10 months	Unknown
Shortest Time	2015	70.8%	18.1%	4.7%	1.2%	1.2%	0.0%	0.0%	3.5%
	2014	58.5%	13.2%	2.9%	1.0%	0.0%	0.0%	0.5%	22.9%
Longest Time	2015	14.0%	30.4%	22.8%	9.9%	2.9%	4.7%	7.0%	5.8%
	2014	12.2%	23.4%	8.3%	8.3%	7.8%	2.4%	4.9%	26.8%
Average Time	2015	29.8%	36.8%	14.0%	3.5%	3.5%	0.6%	0.0%	5.3%
	2014	25.4%	24.4%	13.2%	2.4%	0.5%	0.5%	0.5%	24.9%

In 2014, for those that had experienced breaches, 50% indicated that the average time to detection for an impacted system was one week or less. This number increased in 2015 to 67%. It appears that average detection times have decreased.

When asked about the shortest time to detection, 59% of 2014 respondents indicated breaches were usually detected within the same day, 13% needed one week and 4% needed one to three months. In keeping with the year-over-year decrease in average detection time, the shortest time to detect (the same day) increased to 71% in 2015, followed by 18% needing one week and 6% taking one to three months to detect an incident.

On the other end of the spectrum, in 2014 some 5% of organizations indicated their longest time to detection was more than 10 months, and this number increased to 7% in 2015. The good news is, however, that fewer respondents indicated that they didn't know how long it took them to detect a breach.

The primary alerting mechanisms that triggered events were still network and perimeter protection tools, such as firewalls and IDS, as well as endpoint security tools, matching the data from 2014. However, in 2015, SIEM and other analytics tools came in right behind these controls. Figure 10 shows the full list of alerting mechanisms that played a role in events and detection scenarios.

How were these events brought to the attention of the IT and/or security department?
Select all that apply.

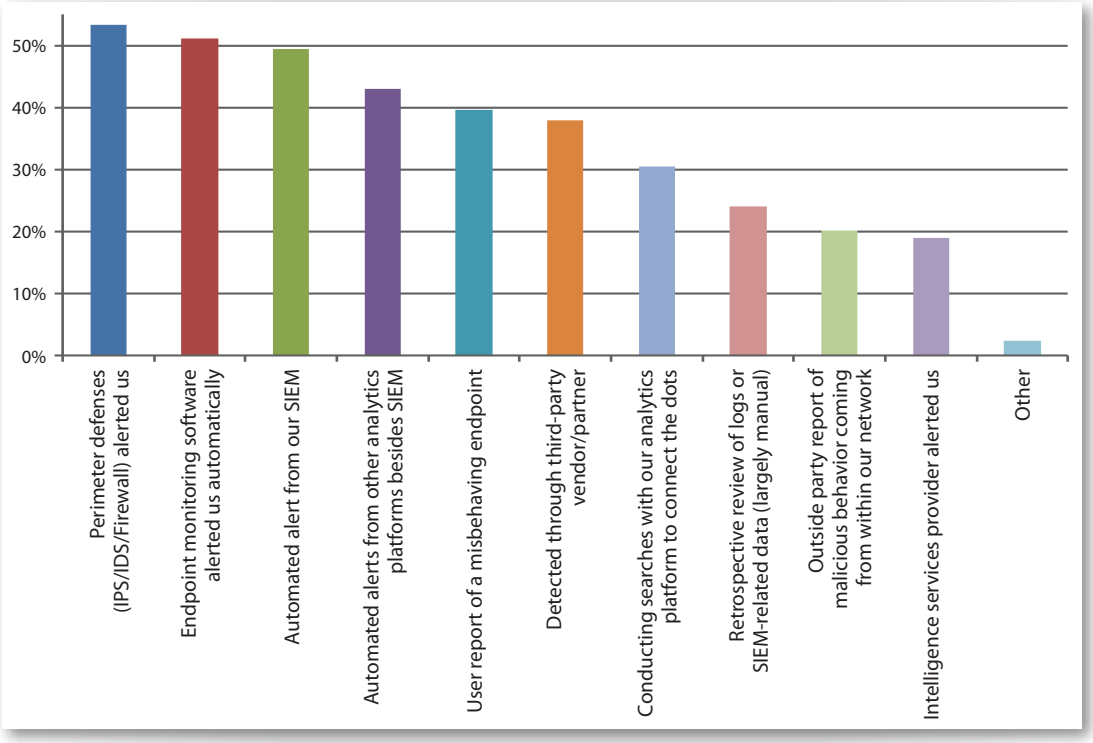


Figure 10. Alerting Mechanisms During Incidents

On the surface, it seems that security teams are detecting some breaches and attacks more quickly, but the longest time to detection is increasing (likely due to advanced adversaries who are stealthy in nature).

Are we improving? Over time, the answer is likely yes, but many teams are just starting to leverage their analytics platforms with more data and data sources, and seeing detection times truly decrease across the board may take time as teams' tools and processes mature. As organizations become better at baselining normal behavior and understanding deviations from normal, they will have even more ability to point to improvements in detection and response times.

Looking Ahead and Wrapping Up

When it comes to their future programs, the biggest change, by far, was in investing in threat intelligence products and services, which garnered only 25% of responses in 2014, yet came in at 43% in 2015. Another big change related to using big data and analytics products, which saw 21% of responses in 2014 and 34% in 2015. Obviously, organizations are focusing more on gathering external threat intelligence and integrating it into their SIEM and analytics environments. See Figure 11.

Where do you plan to make future investments related to security analytics?
Select all that apply.

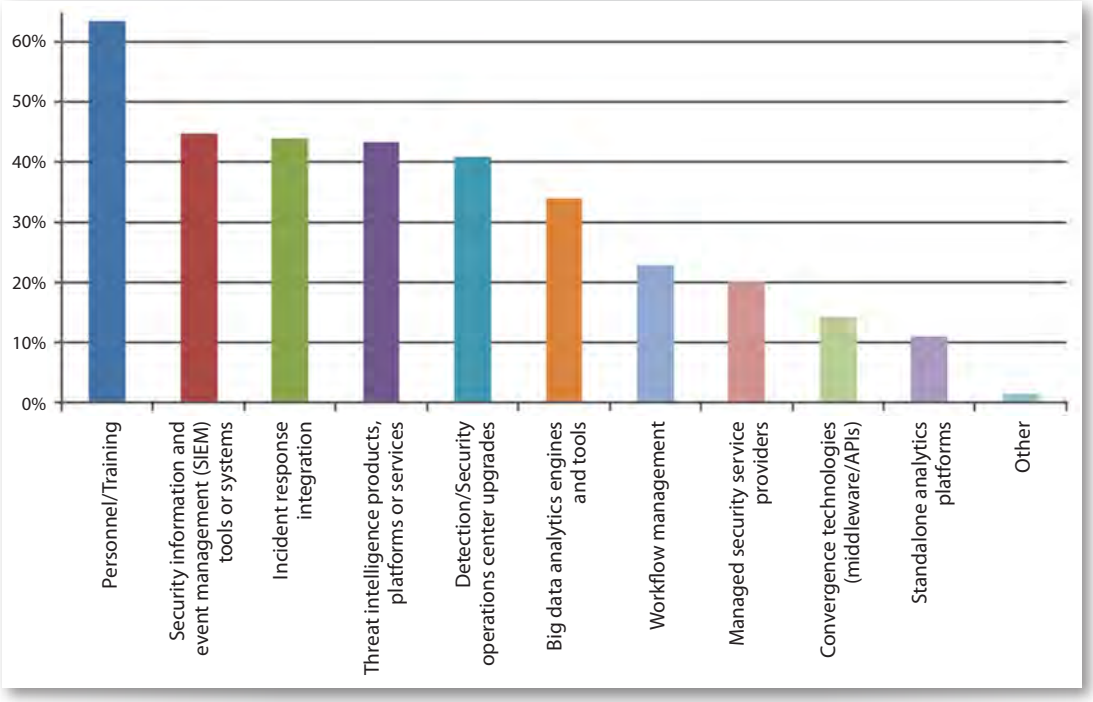


Figure 11. Future Investments Related to Security Analytics

Much like 2014, training and staffing topped the list of future investments organizations will make to fill the gaps in their security analytics and intelligence programs, with 64% selecting this option. In 2014, incident response tools came in second place, with SIEM tools in third. In 2015, those numbers were reversed, but the differences were minor.

In a nutshell, most of the trends from this year echo those from 2014. Overall, there is a lack of maturity in the implementation and use of analytics platforms, although the shortest and average times to detect incidents improved somewhat. More teams are using analytics tools, and we're definitely collecting more and better data. We still have a long way to go in truly getting the most out of analytics platforms for detection and response activities, but organizations are seeing gradual improvements in detection time.

Threat intelligence services are becoming more popular, and we're working to get these feeds integrated into our analytics platforms, but 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 may be due to a serious lack of skills in the SOC. Teams are having a difficult time finding the right skills today, and many organizations are planning to invest in training and hiring in the future, which echoes the 2014 survey.

We're slowly improving, and we've done a much better in collecting data. However, more effort is needed to detect, respond to and report on 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.

Sponsor

SANS would like to thank this survey's sponsor:

DOMAINTOOLS®