Despite perceived gains in security analytics and intelligence capabilities, many organizations are still using the term *analytics* to describe what is fundamentally event management and monitoring, according to the SANS 2014 Analytics and Intelligence Survey recently taken by 350 IT professionals. By conducting this survey, SANS had hoped to see more improvements in the use and benefits of security analytics and intelligence. However, security teams are struggling with visibility, and the use of “intelligence” is slipping.

Only 29% of respondents are using these intelligence tools and services today, down from 38% in our 2013 survey, and 39% of respondents today say they lack visibility into application, underlying systems and vulnerabilities, with 20% indicating that it is their number one impediment.

The survey also shows that those who are properly deploying analytics and intelligence are experiencing benefits of improved visibility—but only to the degree that they are integrating across platforms for security response.

Only 16% had highly automated and 9% had fully automated intelligence and analytics capabilities today within their overall IT infrastructures. Yet, the survey also shows respondents are putting more of the correlation responsibility on their service providers. As such, SANS also expects that the service providers and vendors should make integration and automation a priority for their customers in 2015.
Data Analytics

Data-driven information security is not new, but pinpointing its inception date is probably impossible. One might consider the rise of intrusion detection systems (IDSs) to indicate the start of this trend, thus starting in the late 1980s and benchmarked by a 1986 paper by Dorothy E. Denning and Peter G. Neumann that presented a model of an IDS that forms the basis for many systems today. Since then, analyzing logs, network flows and system events for forensics and intrusion detection has been an increasingly complex problem in the information security community, with regulatory demands increasing and the number of devices that need to be monitored exploding.

Subsequent surveys have shown that security information and event management (SIEM) tools are now replacing log management tools to handle this explosion of security data. The hope is that by correlating all types of security data coming at them, organizations can finally find that “needle in a haystack” and gain visibility into what is happening.

Unfortunately, as past SANS surveys have shown, most organizations continue to struggle with the means to analyze all this data, put context around it and provide the visibility organizations need to see and stop threats coming at them. Some SIEM vendors have moved forward with their own intelligence layer to wrap into the SIEM, while others turn to third-party intelligence services to help connect the dots.

Even as more intelligence providers come on the scene to help organizations connect the dots among their alarms, logs, network behaviors and other indicators of events, security teams will need trained staff who can distinguish normal from abnormal behavior and think just enough outside the box so that they can flag deviant behavior. They should be able to do so through their SIEM or other security information management platforms. Sorting through all the data manually will not be possible, particularly when time is of the essence.

---

A broad range of industries, organization sizes and IT security budgets are represented in the 350 participants who completed this year’s survey. As shown in Figure 1, the top single category is the financial industry, registering 17% of respondents; however, the aggregate government (federal, state/local and military) category comprises the largest total sector represented, with a total of 21%.

The “Other” category, which accounts for 15% of the sample, includes such areas as insurance, consumer technologies, IT services, cloud vendors and other such industry segments, illustrating a widespread interest in analytics.
Respondents represented organizations of all sizes, with large international organizations of more than 50,000 employees accounting for 19% of the sample, as shown in Figure 2.

The respondents also represented a variety of job titles and management levels, indicating that security team members who are familiar with analytics and event management are likely the operators of tools and day-to-day technical practitioners. See Figure 3.
However, more and more different security disciplines are interested in and involved with analytics projects and concepts than ever before, as evidenced by the “Other” responses, which included such titles as security architect, pen tester and security contracts program manager—even one title that said “big data analyst.”

Based on responses, most security teams assigned to detection and response have from two to four full-time employees, with duties split fairly evenly among employees. There is also some overlap, with the same team members responsible for both detection and response. This overlap occurs in both small organizations and larger organizations. Figure 4 breaks down the number of full-time equivalents (FTEs) each organization has in each role.

These results also align with the recently published SANS Incident Response Survey, in which the most common dedicated response team size was three to five team members.
The number of respondents who don’t know if they’ve been hacked (24%) has actually gotten worse since last year’s survey, in which only 20% didn’t know if they had been hacked.

This response might indicate that organizations have less visibility into events and attacks in their environments. It could also indicate a new level of honesty: “We’ve taken stock of the environment, and we know we don’t know a lot,” which at least gives us a healthy starting point from which to improve. See Figure 5.

Of those organizations that are able to detect attacks, more than 23% experienced 2 to 5 breaches or significant attacks in the past two years, while 6% experienced more than 50 attacks in the same time period. This is nearly double last year’s numbers (3%). This also brings us back to the assumption that, despite the data available to them, organizations are still unable to get the visibility they need to detect and respond to attacks.

Figure 5. Number of Advanced Attacks in Past Two Years
**Time to Detection**

Of the 55% of the responding organizations that have suffered a breach or significant attack in the last two years, 54% indicated that the average time to detection for an impacted system was one week or less. When asked about the shortest time, 59% indicated breaches were usually detected within the same day. An additional 13% report the shortest time to detection was within one week, and 4% chose within 3 months. On the other end of the spectrum, some 5% of organizations indicated their longest time to detection was more than 10 months. There are also many who indicated that they didn’t know their best, worst and average detection times.

What do these responses indicate? Much like we saw in 2013, it seems that many organizations feel they are detecting threats fairly rapidly. Many signature-based tools, like antivirus, are still contributing to short detection times, but there have also been improvements in intelligence based on event collection and analysis. (We’ll get to this point later in the paper.)

**Barriers to Detection and Response**

When asked about their key impediments, visibility is directly implicated as a key issue for respondents, 39% of whom cited lack of visibility into application, underlying systems and vulnerabilities as their overall top impediment to attack detection and response (20% indicated that it was their number 1 impediment). They also pointed to lack of visibility across networks, with 25% overall selecting this option, and 22% selecting lack of visibility into endpoints and specific users. Another 19% chose lack of visibility into mobile devices, and 14% chose lack of visibility into cloud-based applications and processes.
A breakdown of responses is shown in Table 1.

<table>
<thead>
<tr>
<th>Impediment</th>
<th>Overall</th>
<th>First</th>
<th>Second</th>
<th>Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of visibility into applications, underlying systems and vulnerabilities</td>
<td>39.1%</td>
<td>19.8%</td>
<td>9.5%</td>
<td>9.9%</td>
</tr>
<tr>
<td>Inability to understand and baseline “normal behavior” (in order to detect abnormal behavior)</td>
<td>36.2%</td>
<td>12.3%</td>
<td>13.6%</td>
<td>10.3%</td>
</tr>
<tr>
<td>Lack of people and skills/dedicated resources</td>
<td>30.0%</td>
<td>11.1%</td>
<td>9.5%</td>
<td>9.5%</td>
</tr>
<tr>
<td>Not collecting the appropriate operational and security-related data to make associations with</td>
<td>26.3%</td>
<td>6.2%</td>
<td>9.1%</td>
<td>11.1%</td>
</tr>
<tr>
<td>Lack of visibility into the network</td>
<td>24.7%</td>
<td>11.9%</td>
<td>7.8%</td>
<td>4.9%</td>
</tr>
<tr>
<td>Lack of visibility into the endpoints and specific users</td>
<td>22.2%</td>
<td>9.1%</td>
<td>9.1%</td>
<td>4.1%</td>
</tr>
<tr>
<td>Lack of visibility into mobile devices</td>
<td>19.3%</td>
<td>4.5%</td>
<td>8.2%</td>
<td>6.6%</td>
</tr>
<tr>
<td>Lack of context to know what threats are important based on criticality of assets</td>
<td>18.5%</td>
<td>4.9%</td>
<td>9.1%</td>
<td>4.5%</td>
</tr>
<tr>
<td>Lack of external perspective/intelligence on new threats/indicators of compromise</td>
<td>15.6%</td>
<td>3.7%</td>
<td>3.3%</td>
<td>8.6%</td>
</tr>
<tr>
<td>Lack of visibility into the cloud-based applications and processes</td>
<td>14.4%</td>
<td>3.3%</td>
<td>4.9%</td>
<td>6.2%</td>
</tr>
<tr>
<td>Lack of central reporting and remediation controls</td>
<td>13.6%</td>
<td>2.1%</td>
<td>2.5%</td>
<td>9.1%</td>
</tr>
</tbody>
</table>

What is even more enlightening is the high emphasis respondents place on other impediments that are most likely the root causes of why there is a lack of visibility:

- Knowing what to look for (36% cite inability to understand and baseline normal behavior)
- Having the trained resources to perform the analysis (30% cite lack of people, skills and resources)
- Knowing what key information to collect and correlate (26% admit to not collecting the appropriate data)

Given respondents’ answers to the size of teams handling response and remediation, resources will continue to be a problem until the day that organizations can automate and integrate their analysis, intelligence and response functions.
Alerting Mechanisms

Tried, tested and mature technologies still rule the alerting organizations respondents use to detect real events in their enterprises, according to responses. The majority (57%) indicated that traditional perimeter defenses like IDS, IPS and firewall platforms were the tools that alerted them to their breaches first. Another 42% chose endpoint agents like antivirus as providing their initial alerts about events. Figure 6 shows the full range of responses.

Automated alerts from SIEMs alerted respondents 37% of the time, indicating that next-generation SIEM can analyze and make intelligence alerts. Still, 32% of respondents indicate that retrospective review of logs or SIEM-related data were responsible for initial discovery.

Because respondents could choose more than one answer, organizations are clearly mixing a variety of these choices into their incident detection and investigation. This response also shows movement toward SIEM-based analytics and intelligence, which can be programmed to make intelligent alerts and integrate with outside intelligence services as needed.
The Role of Security Data Analytics in Building Security Intelligence

Despite market impressions that “big data” was a buzzword, respondents to this year’s survey believe the concept is valid (whereas in 2013 they didn’t believe it was going to stick). In this year’s survey, 36% feel that the concept of big data is key for detection and investigation, and another 25% see the growing importance of big data and analytics in event management and security intelligence (see Figure 7).

One thing is certain: Analytics solutions will need to integrate with numerous internal detection platforms in an effort to increase visibility and improve security intelligence.

As you can see from Figure 8, tried and tested legacy technologies (firewalls, IPS, UTM) are currently employed most frequently, as is host-based malware detection (which accounts for the results in Table 1).
The Role of Security Data Analytics in Building Security Intelligence (CONTINUED)

What types of detective technologies do you need your analytics and intelligence capabilities to interface with?
Please indicate which ones are currently integrated into your environment and those that are planned but not integrated yet.

TAKEAWAY:
Organizations are using or planning to use a variety of different tools. Threat intelligence data needs to integrate with a wide variety of security tools and platforms.

Tools focused on users, applications and systems like NAC (32%), network-based antimalware (31%), user behavior monitoring (29%) and others seem to be increasingly planned for future integration. Security data from these devices should also improve correlation and analytics.

Figure 8. Current and Planned Control Integration with Analytics
Threat Intelligence

Threat intelligence is the set of data collected, assessed and applied regarding security threats, malicious actors, exploits, malware, vulnerabilities and compromise indicators. Its use allows organizations to more effectively plan and act for detection and response; more accurately pinpoint implicated users, systems and actors in an event; and connect the dots between event data collection and the steps or trajectory of the attack.

In 2014, 29% of respondents state that they don’t correlate log and event data with internally gathered data or external threat intelligence tools. In 2013, 38% of respondents stated that they were not correlating log and event data with any external threat intelligence tools. This difference indicates a slight growth in the use of threat intelligence tools and services.

Correlation may also be moving to a services model, with the largest group (31%) stating that their correlation is handled largely by the service providers and other vendors they rely on to feed intelligence data into the environment and update for them.

Figure 9 shows the breakdown of how threat intelligence data is being acquired and leveraged for detection and response programs.

The use of both external and internal threat intelligence is increasing, although correlation with existing security technology and processes is somewhat stagnant.

This actually shows some maturation of the intelligence industry since last year’s survey, with vendors and service providers stepping in to fill the gap where issues like standardization of event information and having the internal knowledge of events cannot be overcome by individual IT organizations.
Automation

Automation is another avenue that can lead to better visibility. Based on responses, automation of intelligence and analytics functionality is on the rise, with 25% (up from 9% in 2013) feeling that these functions are fully (9%) or highly (16%) automated, as shown in Figure 10.

![Level of Automation for Security Analytics and Intelligence Processes](image)

**Figure 10. Level of Automation**

Surprisingly, 28% replied that they didn’t know the level of automation, which again could be due to an overall lack of visibility into the environment and how it’s operating, or it could be due to a lack of clarity on what constitutes analytics versus more disparate tools and functions.

**TAKEAWAY:**
Greater emphasis on automation is needed. By increasing their automation of intelligence and analytics capabilities, organizations can reduce the effect of lack of trained staff, improve visibility, and enhance detection and response.
Intelligence Services: Pulling It All Together

Fifty percent of respondents are currently investing in third-party intelligence tools or services for security analytics and threat intelligence, while 36% are not. The rest (14%) aren't sure, which is likely due to different roles and involvement in these projects.

With such an increase in investment in intelligence, why do security professionals still feel as if they have such little visibility? Without speculating too much, it may be due to a lack of cohesiveness between tools and data at the current stage of many implementations. This is likely exacerbated by the ongoing issue of silos between IT ops and security, as indicated in SANS' recent survey on Incident Response.4

The ideas behind central data aggregation and analysis are sound, including input from and correlation with both internally and externally sourced threat intelligence channels—but many organizations indicate they are in the earliest stages of investigation and deployment of such tools.

In fact, when asked about the types of tools and services they were using for security intelligence and analytics, their fill-in answers listing specific vendors were all over the map: They listed SIEM, log management, malware sandboxing, web application proxies and scanners, vulnerability scanners, and even firewalls and intrusion detection systems vendors as their intelligence vendors. Each of these tools can collect data that can facilitate developing an intelligence network, with their findings becoming valuable information that can be used to stop similar future attacks.

While only 25% stated that their teams had highly (16%) or fully automated (9%) intelligence and analytics capabilities today—which is not surprising, given the relative immaturity in understanding of analytics architecture, data integration and definitions, as well as integration with the complexity in threat landscape, data sources and data volume—we expect this group to grow at a steady pace. Automation is key to more rapid integration into detection, and response tools—and processes—and will probably lead to a much higher likelihood of success with analytics overall.

4 www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342
Despite their lack of visibility, overall, users are experiencing benefits with the capabilities they have rolled out. Of those using these capabilities, 58% are satisfied with performance and response time, 55% are experiencing improved ability to quickly correlate events and 51% are able to quickly identify compromised credentials and phishing attacks. For those actively using analytics tools, reduction of false positives and/or false negatives is a plus, as well, with a 50% satisfaction rating, as shown in Table 2.

However, we see dissatisfaction with current capabilities that echoes the impediments to detection and response. The major categories in which users aren’t satisfied relate to visibility (49% dissatisfied with their “Single consistent view across disparate systems and users, including cloud services and mobile devices,” 48% dissatisfied with “Visibility into actionable security events across disparate systems and users, including cloud services and mobile devices,” and 43% dissatisfied with their ability to separate normal from abnormal behavior). This is likely due to the interoperability issues discussed earlier and may reflect market immaturity. Most respondents are also dissatisfied with the training/expertise needed to effectively operate these tools (chosen by 48% of respondents) and costs associated not only with the tools and their maintenance, but also with having the trained personnel to use these tools for operations and analysis (chosen by 47%).

<table>
<thead>
<tr>
<th>Current Analytics and Intelligence Capabilities</th>
<th>Very Satisfied/ Satisfied</th>
<th>Not Satisfied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance and response time</td>
<td>58.4%</td>
<td>33.0%</td>
</tr>
<tr>
<td>Ability to quickly correlate events to users</td>
<td>54.8%</td>
<td>38.1%</td>
</tr>
<tr>
<td>Ability to identify compromised credentials and phishing attacks</td>
<td>51.3%</td>
<td>40.1%</td>
</tr>
<tr>
<td>Reduction of false positives and/or false negatives</td>
<td>50.3%</td>
<td>39.6%</td>
</tr>
<tr>
<td>Producing or having a library of appropriate queries/ meaningful reports</td>
<td>45.7%</td>
<td>41.6%</td>
</tr>
<tr>
<td>Ability to alert based on exceptions to what is “normal” and approved</td>
<td>44.7%</td>
<td>42.6%</td>
</tr>
<tr>
<td>Relevant event context (intelligence) to separate and observe “abnormal behavior” from normal behavior</td>
<td>43.7%</td>
<td>42.6%</td>
</tr>
<tr>
<td>Costs for tools, maintenance and personnel</td>
<td>43.1%</td>
<td>46.7%</td>
</tr>
<tr>
<td>Integration of intelligence with security response systems for proper response</td>
<td>42.1%</td>
<td>43.1%</td>
</tr>
<tr>
<td>Single consistent view across disparate systems and users, including cloud services and mobile devices</td>
<td>40.6%</td>
<td>48.7%</td>
</tr>
<tr>
<td>Visibility into actionable security events across disparate systems and users, including cloud services and mobile devices</td>
<td>40.6%</td>
<td>48.2%</td>
</tr>
<tr>
<td>Training/expertise required to operate intelligence systems/ conduct analysis</td>
<td>39.6%</td>
<td>47.7%</td>
</tr>
</tbody>
</table>
Use Cases

For security teams actively using analytics platforms, what are the top three use cases driving the tools and services today? We asked a similar question in the 2013 survey and got some interesting results that align with this year’s data:

1. Finding new or unknown threats was the top “#1” ranking in this year’s survey by a wide margin, with 40% citing this as the primary use case, similar to the 2013 answers of “external malware-based threats” and “advanced persistent threats,” which together accounted for 39% of the #1 rankings.

2. Detecting insider threats was considered the second top use case by 23% of the respondents (10% ranked it as the top use case), which places it higher than its 2013 fourth-place ranking.

3. Overall, the top picks were finding unknown threats (55%), detecting insider threats (40%), improving visibility into network and endpoint behaviors (36%), and finding external malware-based threats (31%).

Figure 11 shows the breakdown from the 2014 survey.

These use cases indicate that, when used properly, intelligence and analytics are improving an organization’s ability to respond to threats faster, and some organizations are getting real value in finding unknown or hard-to-locate threats like insider activity.
Looking Ahead

Training and staffing topped the list of future investments organizations will make to fill the gaps in their security analytics and intelligence programs, with 67% selecting this option. This staffing requirement may trend down somewhat if usability, visibility and correlation between datasets improve over time, although organizations will always need IT professionals who know what’s normal to distinguish abnormal behavior.

More likely, the human element will shift in nature, away from the personnel needing to know the nuts and bolts mechanics of just running the tools toward personnel actually using the tools to analyze the data, acquire valuable information and then provide intelligence from the analysis. See Figure 12.

The high ranking of improving response capabilities and investing in SIEM tools aligns closely with the overlaps between SIEM platforms and analytics tools this survey has shown us. While SIEM is still considered a separate category of security tools by most, more and more of these instruments are consuming and analyzing bigger data sets, producing reports focused on longer-term data analysis and behavioral baselines, and integrating threat intelligence from numerous sources. When implementing analytics and threat intelligence, all these categories will need upgrades in the coming months and years to keep pace with the threat landscape we’re facing now.

Figure 12. Future Investments in Analytics/Intelligence
Based on the results of this year’s survey, there are several key takeaways for the security community. Organizations that are deploying analytics and intelligence properly are experiencing faster response and detection times, as well as greater visibility. However, many are confused about how to integrate and automate their intelligence collection processes, which vendors to turn to for help, and how to differentiate tools and services.

Despite this confusion, the use of tools-based threat intelligence (for example, through the SIEM or SIEM integration with an intelligence feed) is growing. Vendors providing a variety of tools can capitalize on connecting the dots between their tools for big picture analytics, while security vendors with tools that gather intelligence information are integrating with partners and providing APIs for further integration.

We are definitely moving in the right direction. The use of analytics and threat intelligence to ferret out complex and stealthy threats from advanced attackers and insiders is improving security for some; automation is improving; and intelligence providers are also helping with the tricky problems of correlating event and threat intelligence data for their customers. Overall, these tools and services are providing value to consumers, and they should continue to improve response and visibility over time.
Dave Shackleford is the founder and principal consultant with Voodoo Security, a SANS analyst, instructor and course author, and a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert and 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 is the author of the Sybex book Virtualization Security. Recently, Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.