Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey

Results of the 2016 Incident Response Survey indicate that the IR landscape is ever changing. Advanced industries are able to maintain effective IR teams, but as shown in this report, there are still hurdles to jump to increase the efficiency of many IR teams. Read this report to learn more.
Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey

A SANS Survey

Written by Matt Bromiley
Advisor: Rob Lee
June 2016

Sponsored by
AlienVault, Arbor Networks, HPE, IBM Security, Intel Security, LogRhythm, NETSCOUT, and Veriato
The attacker’s landscape has changed yet again. What was once an era of advanced attackers seeking to gain access into an environment has been transformed by attackers who quickly smash and grab global hotel chains, for example, to pilfer millions of credit card numbers. Electricity in international countries is brought to a standstill as nation-states seek to prove a point. And in the blink of an eye, businesses are held hostage by ransomware. As the landscape has changed, opening new opportunities for breaches and lowering the attacker’s barrier to entry, organizations have started to respond and are realizing they must respond quickly.

Incident responders present an unusual challenge to an organization because they can measure their success by many metrics. One of these measures is how quickly the organization can detect, isolate and remediate infections in the environment. The longer an attacker has access to an environment, the more damage can be done.

Of the 591 respondents to qualify and take the 2016 SANS Incident Response Survey, approximately 21% cited their time to detection, or “dwell time,” as two to seven days, while 40% indicated they could detect an incident in less than one day. Conversely, 2% of organizations reported their average dwell time as greater than one year. Survey participants reported that 29% of remediation events occur within two to seven days, while only 33% occur in less than one day.

The survey also found that incident response (IR) teams have various blends of automatic and manual technology, which can be a bonus for teams with skilled members and a hurdle for teams with inexperienced practitioners. Other promising statistics indicate that 76% of respondents had dedicated internal IR teams, an uptick from our 2015 survey.1

Malware still maintains the top spot as the underlying cause of reported breaches, at 69%, but unauthorized access is recognized as a growing problem, with 51%, as attackers take advantage of weak, outdated remote access and authentication mechanisms. Organizations are also reporting that 36% of attacks are advanced persistent threats (APTs) or multistage attacks, indicating that advanced attack groups are still targeting organizations.

---

Despite the positive trends found in the survey, we still see IR teams with a shortage of skilled personnel, as reported by 65% of the survey participants. Teams expressed the need for more training and experience, with approximately 73% of organizations indicating they intend to plan training and staff certifications in the next 12 months. Furthermore, only 58% of organizations admit to reviewing and updating IR processes, either at periodic or event-based intervals.

Overall, the results of the 2016 survey indicate that the IR landscape is ever changing. Advanced industries are able to maintain effective IR teams, but as shown in this report, there are still hurdles to jump to increase the efficiency of many IR teams. These issues, along with best practices and advice, are discussed in the following pages.
Participants in the 2016 SANS Incident Response (IR) Survey included organizations as diverse as the incidents themselves. The respondent base represented multiple industries, varying organization sizes, worldwide representation and a full spectrum of IR capabilities.

Industries and Footprints

The survey results include multiple industries, with technology/IT and financial services representing the largest respondent pools, selected by 19% and 17%, respectively. Other top industries include government organizations, both military and nonmilitary.

These results represent a 3% difference from 2015, where government organizations represented 20% of the respondent base. The growth of privatized IR teams and capabilities follows a noticeable trend of organizations investing more in protecting their assets. Furthermore, technology and financial organizations are typically high-value targets that often build and maintain advanced security programs. Figure 1 illustrates the top 10 industries represented in the survey.

Figure 1. Top 10 Industries Represented

Although represented by significantly smaller slices of the respondents and not included in the top 10 industries represented, the hospitality and retail industries, which total just 4% of our sample, also are high-value targets because of the amount of personally identifiable information (PII) and PCI data they use. The “Other” category, making up 6% of our sample, includes such industries as cyber security, media, real estate and a variety of professional services.

The respondent pool for the survey also provided insight into the size of firms performing IR work: 36% of respondents work for organizations with more than 10,000 employees, representing large organizations with the capability of maintaining their own IR programs. Organizations with 1,000 to 10,000 employees are represented by 29%, while 36% work for places of business with fewer than 1,000 employees. Figure 2 provides a breakdown of responding organization sizes.

The 2016 survey also saw an uptick in global operations, with 71% of respondents having IR operations in the United States and 66% having IR teams in Europe and Asia. The growth shows that organizations are becoming more familiar with their assets and their responsibilities, and are developing the capability of responding to incidents globally. Furthermore, it shows an understanding of attackers’ lack of respect for international laws or regulations. While North American organizations remain high-value targets, European and Asian-Pacific organizations are also seeing an increase in attacks. Globally exposed data means organizations must be able to cope with the various risks and regulations associated with maintaining global operations and data in and across different countries.

TAKEAWAY:
Attackers are not concerned with where your data is located; however, international regulations may change how your team can respond. Ensure that your IR team is aware of the regulations for each country in which your data may be at risk and how your organization may be able to legally respond.

3 The breakdown of organization size totals more than 100% due to rounding error.
Who’s Responding

Survey results indicate that where IR teams come from also remains varied. Approximately 9% of respondents indicated they worked for a forensics/IR consulting firm, a 4% growth from 2015. This activity is indicative not only of a larger respondent base, but also of consulting organizations expanding their IR capabilities to support their clients. Despite the growth in IR consulting, 76% of organizations reported having an internal IR team, a 3% increase from 2015.

One interesting industry observation is the repurposing of network, systems or IT personnel as incident responders. As organizations build out their internal IR teams, they are turning to current staff who already have intimate knowledge of the internal network and operations. These teams can often move fluidly within an environment; however, they may not have the deep technical skills to respond to an enterprise intrusion. We cover skill shortage issues in the section “Addressing the Real Issue.”

Approximately 43% of respondents identified themselves as security analysts or incident responders, roles that are often interchangeable and have shared duties. Organizations often turn to their peers or industry standards to identify roles and responsibilities, and as previously mentioned, will pull from roles already established within the organization. These roles may be structured internally in various tiers or titles; however, they represent a unified approach to IR. Just over 23% of respondents identified themselves as information security upper management, including CSO, CIO and CISO positions, as illustrated in Figure 3.

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

![Figure 3. Top 10 Respondent Roles](image-url)

---

As organizations are reinforcing their teams and protecting their assets, they are also gaining better visibility and an understanding of the state of their networks. A majority of organizations, 87%, say they responded to at least once incident within the past 12 months. Of these incidents, only 59% resulted in at least one actual breach. Approximately 21% of organizations say they have responded to at least 100 incidents; however, only 4% of these incidents have resulted in actual breaches. Lastly, approximately 48% of respondents say they have investigated 25 incidents or less, with approximately 47% of those incidents resulting in an actual breach. Figure 4 provides additional insight into incident and breach reporting.
These percentages represent a growth in both incidents and breaches from 2015. While this growth may be indicative of increased attacks, it is likely largely attributed to the increased detection capabilities of IR teams. As mentioned, these capabilities add value to IR teams, but they also increase the number of incidents an organization may respond to.

**Breach Payloads**

Year over year, malware infections continue to be a major underlying factor in enterprise breaches. Distinguishing between malware as a root cause of an incident or as a tool used by an attacker helps an organization understand the tactics, techniques and procedures (TTPs) associated with threat actors. In the 2016 survey, respondents said malware was seen in 69% of incidents. Unauthorized access and data breach each saw significant percentage jumps as the underlying cause of breaches, reported by 51% and 43%, respectively. Interestingly, DDoS attacks, in which attackers seek to disrupt business operations using network-based attacks, saw a significant decline, down a total of 10% to 33% (see Table 1).

The statistics presented in Table 1 are certainly indicative of shifting attacker TTPs. Because malware is utilized by widespread attacks such as drive-by downloads, as well as by advanced attackers, it is likely some overlap exists between malware and other types of underlying causes. Indeed, 36% of respondents attributed the underlying nature of breaches to advanced persistent threat (APT) or multistage attacks, a 2% increase from 2015. These groups, as well as those represented in the Other (5%) category, may indicate the usage of malware in enterprise environments is higher.

---

**Table 1. Changes in Underlying Causes of Breaches**

<table>
<thead>
<tr>
<th>Nature of Breach</th>
<th>2015</th>
<th>2016</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware infections</td>
<td>62.1%</td>
<td>69.4%</td>
<td>7.3%</td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>42.5%</td>
<td>51.2%</td>
<td>8.7%</td>
</tr>
<tr>
<td>Data breach</td>
<td>38.5%</td>
<td>43.4%</td>
<td>4.9%</td>
</tr>
<tr>
<td>Advanced persistent threat or multistage attack</td>
<td>33.3%</td>
<td>35.7%</td>
<td>2.4%</td>
</tr>
<tr>
<td>Insider breach</td>
<td>28.2%</td>
<td>25.2%</td>
<td>-3.0%</td>
</tr>
<tr>
<td>DDoS as the main attack</td>
<td>27.6%</td>
<td>21.7%</td>
<td>-5.9%</td>
</tr>
<tr>
<td>Unauthorized privilege escalation</td>
<td>21.3%</td>
<td>21.7%</td>
<td>0.4%</td>
</tr>
<tr>
<td>DDoS diversion attack</td>
<td>15.5%</td>
<td>11.2%</td>
<td>-4.3%</td>
</tr>
<tr>
<td>Destructive attack (aimed at damaging systems)</td>
<td>14.9%</td>
<td>14.0%</td>
<td>-0.9%</td>
</tr>
<tr>
<td>Other</td>
<td>1.7%</td>
<td>5.4%</td>
<td>3.7%</td>
</tr>
</tbody>
</table>

---

As shown in Table 1, 2016 saw a 9% increase in unauthorized access as an underlying cause. This activity is representative of attackers discovering and exploiting vulnerabilities in enterprise remote access solutions, such as VPN or remote desktop applications, to gain entry into an environment. Due to business or resource constraints, many organizations still maintain single-factor authentication mechanisms on remote access tools, which have proven easy for attackers to penetrate. Once in an environment, implementations of single sign-on (SSO) ensure that attackers need not log in again.

Data Exfiltration

As organizations have reported an increase in breaches year over year, the types of data that have been exfiltrated from enterprise environments have also changed accordingly. This year saw noticeable changes in survey responses, moving away from customer information to other profitable types of data, again indicative of shifting attacker motivations.

Employee information remained the most common type of data stolen from environments, according to 48% of participants. Intellectual property, such as source code, was cited by 35%, an increase of 5% from 2015. PCI data, such as payment card numbers, saw a significant jump from 14% in 2015 to 21% in 2016 (see Table 2).

The increase in PCI data theft has certainly been noticed by the information security community, with multiple breaches of large hotel, restaurant and casino chains occurring in 2015. Reputable hotel chains such as Mandarin Oriental, Hilton Worldwide and Starwood Hotels have all suffered data breaches in the past 15 months, potentially affecting millions of customers and credit card numbers.

### Table 2. Data Types Exfiltrated in 2015 and 2016

<table>
<thead>
<tr>
<th>Nature of Data Exfiltrated</th>
<th>2015</th>
<th>2016</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee information</td>
<td>41.2%</td>
<td>48.3%</td>
<td>7.1%</td>
</tr>
<tr>
<td>Individual consumer customer information</td>
<td>35.8%</td>
<td>32.1%</td>
<td>-3.7%</td>
</tr>
<tr>
<td>Intellectual property (source code, etc.)</td>
<td>29.7%</td>
<td>34.6%</td>
<td>4.9%</td>
</tr>
<tr>
<td>Proprietary customer information</td>
<td>26.7%</td>
<td>27.4%</td>
<td>0.7%</td>
</tr>
<tr>
<td>Legal data</td>
<td>14.5%</td>
<td>12.0%</td>
<td>-2.5%</td>
</tr>
<tr>
<td>PCI data</td>
<td>13.9%</td>
<td>20.5%</td>
<td>6.6%</td>
</tr>
<tr>
<td>PHI data</td>
<td>12.1%</td>
<td>11.5%</td>
<td>-0.6%</td>
</tr>
<tr>
<td>Other regulated data</td>
<td>11.5%</td>
<td>12.0%</td>
<td>0.5%</td>
</tr>
<tr>
<td>(SOX, non-PHI personally identifiable info)</td>
<td>11.5%</td>
<td>13.2%</td>
<td>1.7%</td>
</tr>
</tbody>
</table>

The increase in PCI data theft has certainly been noticed by the information security community, with multiple breaches of large hotel, restaurant and casino chains occurring in 2015. Reputable hotel chains such as Mandarin Oriental, Hilton Worldwide and Starwood Hotels have all suffered data breaches in the past 15 months, potentially affecting millions of customers and credit card numbers.

---


9 www.starwoodhotels.com/html/HTML_Blocks/Corporate/Confidential/Letter.htm?EM=VTY_CORP_PAYMENTCARDSECURITYNOTICE
Attackers have also taken notice of the value of PCI data and have shifted their malware as a result. Verizon’s 2015 Data Breach Investigations Report (DBIR)\(^\text{10}\) indicates that in PCI investigations in 2010, many point-of-sale (POS) investigations involved attackers stealing credentials via keyloggers. Fast-forward to 2016, and the Verizon DBIR\(^\text{11}\) report found 91% of POS cases now involve memory-scraping malware that allows attackers to be exponentially more successful at stealing PCI data.

### The Attack Surface

Coupled with tracking data exfiltration, organizations can also gain insight into the types of systems that are being targeted. Participants indicated that 77% of systems involved in investigations are typically corporate-owned computing device assets, such as laptops and smartphones. A close second and third are internal network devices (on-premises) and data centers, with 73% and 67% representation, respectively. As illustrated in Figure 5, enterprise assets typically all face the same high threat levels, while personal assets, such as social media accounts or third-party platforms, are represented in far fewer investigations (56% and 55%, respectively).

### What systems are involved in your investigations?

Check only those that apply. Please indicate whether your capabilities for these investigations exist in-house, are outsourced, or both.

<table>
<thead>
<tr>
<th>System Type</th>
<th>In-House</th>
<th>Both</th>
<th>Outsourced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate-owned laptops, smartphones, tablets and other mobile devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal network (on-premises) devices and systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data center servers hosted locally</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business applications and services (e.g., email, file sharing) in the cloud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web applications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate-owned social media accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded, or non-PC devices, such as media and entertainment boxes, printers, smart cars, connected control systems, etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee-owned computers, laptops, tablets and smartphones (BYOD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data center servers hosted in the public cloud (e.g., Azure or Amazon EC2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee social media accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third-party social media accounts or platforms</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5. Systems Involved in Investigations

---


Every year, IR teams should be evaluating their contribution to securing the organization and protecting its assets. This offers the team an opportunity to represent its value to the organization and justify expenses for training and equipment. The SANS IR survey captures several metrics that holistically offer insight as to whether IR teams are improving, remaining stagnant or slipping year over year.

Tracking Yourselves

IR teams should ensure that they have mechanisms in place to effectively evaluate the team on a calendar basis, such as monthly, quarterly or annually. Successful, advanced teams also focus on incident-based evaluations, realizing that the team’s growth is also based on experience rather than calendar milestones. In this year’s survey, only 20% of respondents indicated that their IR team reviews and updates IR processes after each major incident. Conversely, 39% of respondents indicated their IR processes are updated periodically, while 42% of respondents indicated that they do not currently assess IR processes, although 32% are planning to do so in the future (see Figure 6).

*Figure 6. Frequency of Effectiveness and Maturity Assessments*
Of the participants who indicated that they assess their IR processes at certain intervals, this year’s survey revealed that assessment and evaluation methods vary. The largest percentage (47%) of respondents reported that they measure improvements on metrics such as accuracy, response time and reduction of attack surface. Approximately 28% of respondents say they use well-defined metrics to update an IR plan. It is unclear, however, whether reported metrics are industry standards, peer-based best practices or internally designed metrics. Figure 7 provides a look at how respondents assess the effectiveness and maturity of their IR processes.

**Takeaway:**
IR teams should be evaluating themselves on metrics such as incident detection or dwell time to determine how quickly they can detect and respond to incidents in the environment. Through well-crafted assessments, teams should find weaknesses in responsiveness and focus on strengthening those areas.

**Compromise to Remediation**

One core metric an IR team can use to evaluate its effectiveness is the length of time between incident detection and remediation. That time frame can be separated into two quantified statistics IR teams should consider:

- Mean time from compromise or infection to incident detection (also known as the dwell time)
- Mean time from detection to remediation

In this year’s survey, the largest number of respondents (21%) selected 2–7 days as the most popular dwell time, indicating attackers potentially had access to an environment for up to a week. This time frame was also the most popular for detection-to-remediation time frames, chosen by 29%.
Conversely, 11% of respondents reported that detecting an incident may take four months or longer, but only 5% of respondents indicated that remediation takes that long—an interesting statistic showing organizations are able to remediate faster than they can detect (see Figure 8). This is likely due, in part, to remediation being performed with the help of dedicated teams and automated tools.

Detecting the Incident

As IR teams focus on improving their processes and increasing the value returned to the organization, one consideration is how teams have integrated their detection methods. IR teams should receive alerts quickly and be able to discern between false and true positives efficiently, with a focus on lowering dwell time.

This year’s survey indicated that intrusion devices, such as IDS and IPS, and firewalls are most highly integrated in security ecosystems, at 57%. Otherwise, this year’s survey saw a decline or little-to-no change in integrated detection capabilities. This flat result may reflect a larger participant pool, or may suggest that organizations are focusing resources and IR team development elsewhere. Ideally, IR teams would like to see highly integrated detection capabilities that allow the team to respond to incidents quickly. Despite security device integrations, teams are still facing issues of being able to effectively parse the data presented to them from their devices. In March 2012, Gartner analyst Neil MacDonald published a report called “Information Security Is Becoming a Big Data Analytics Problem.” In it, he noted that businesses have a staggering array of security data: network packet data, multisource security event data, monitoring information, account management logs and more.¹²

Table 3 displays the capabilities used to identify affected systems, with the top three in each category highlighted.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Highly Integrated</th>
<th>Partially Integrated</th>
<th>Not Integrated</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS/IDS/Firewall/UTM alerts</td>
<td>56.6%</td>
<td>28.7%</td>
<td>7.9%</td>
<td>93.3%</td>
</tr>
<tr>
<td>Log analysis</td>
<td>40.8%</td>
<td>40.2%</td>
<td>10.9%</td>
<td>91.8%</td>
</tr>
<tr>
<td>Security information and event management (SIEM) correlation and analysis</td>
<td>41.6%</td>
<td>30.8%</td>
<td>16.7%</td>
<td>89.1%</td>
</tr>
<tr>
<td>User notification or complaints</td>
<td>31.1%</td>
<td>41.1%</td>
<td>16.1%</td>
<td>88.3%</td>
</tr>
<tr>
<td>Network packet capture or sniffer tools</td>
<td>26.7%</td>
<td>40.5%</td>
<td>19.4%</td>
<td>86.5%</td>
</tr>
<tr>
<td>Host-based intrusion detection system (HIDS) agent</td>
<td>32.3%</td>
<td>34.0%</td>
<td>19.6%</td>
<td>85.9%</td>
</tr>
<tr>
<td>Network-based scanning agents for signatures and detected behavior</td>
<td>36.7%</td>
<td>32.3%</td>
<td>17.0%</td>
<td>85.9%</td>
</tr>
<tr>
<td>Network flow and anomaly detection tools</td>
<td>25.2%</td>
<td>42.2%</td>
<td>18.5%</td>
<td>85.9%</td>
</tr>
<tr>
<td>Endpoint detection and response (EDR) capabilities</td>
<td>32.0%</td>
<td>33.4%</td>
<td>18.8%</td>
<td>84.2%</td>
</tr>
<tr>
<td>Services availability monitoring</td>
<td>28.2%</td>
<td>38.7%</td>
<td>17.3%</td>
<td>84.2%</td>
</tr>
<tr>
<td>Third-party notifications and intelligence</td>
<td>22.0%</td>
<td>38.7%</td>
<td>23.2%</td>
<td>83.9%</td>
</tr>
<tr>
<td>User activity monitoring tools</td>
<td>24.9%</td>
<td>36.4%</td>
<td>22.0%</td>
<td>83.3%</td>
</tr>
<tr>
<td>Endpoint controls (e.g., NAC or MDM)</td>
<td>27.0%</td>
<td>29.9%</td>
<td>25.5%</td>
<td>82.4%</td>
</tr>
<tr>
<td>Network traffic archival and analysis tools</td>
<td>27.3%</td>
<td>34.9%</td>
<td>19.6%</td>
<td>81.8%</td>
</tr>
<tr>
<td>SSL decryption at the network boundary</td>
<td>21.1%</td>
<td>31.4%</td>
<td>29.0%</td>
<td>81.5%</td>
</tr>
<tr>
<td>Third-party tools specific for legal digital forensics</td>
<td>24.0%</td>
<td>29.3%</td>
<td>27.3%</td>
<td>80.6%</td>
</tr>
<tr>
<td>Intelligence and analytics tools or services</td>
<td>25.2%</td>
<td>36.1%</td>
<td>19.1%</td>
<td>80.4%</td>
</tr>
<tr>
<td>File integrity monitoring (FIM)</td>
<td>16.4%</td>
<td>31.7%</td>
<td>31.7%</td>
<td>79.8%</td>
</tr>
<tr>
<td>Browser and screen capture tools</td>
<td>16.7%</td>
<td>27.3%</td>
<td>34.9%</td>
<td>78.9%</td>
</tr>
<tr>
<td>Homegrown tools for our specific environment</td>
<td>21.4%</td>
<td>33.4%</td>
<td>24.0%</td>
<td>78.9%</td>
</tr>
<tr>
<td>Behavioral monitoring (profiling)</td>
<td>13.8%</td>
<td>28.7%</td>
<td>35.5%</td>
<td>78.0%</td>
</tr>
<tr>
<td>Visibility infrastructure to optimize connected security systems</td>
<td>16.4%</td>
<td>38.1%</td>
<td>21.4%</td>
<td>76.0%</td>
</tr>
<tr>
<td>Other</td>
<td>1.5%</td>
<td>2.1%</td>
<td>4.7%</td>
<td>8.2%</td>
</tr>
</tbody>
</table>
Threat Intelligence

Another avenue through which IR teams can decrease their response times and protect their organizations is to utilize threat intelligence (TI).13 In this year’s survey, a promising 72% of participants indicated they were using TI feeds to support their IR teams. Respondents reported receiving their TI via varying methods: 15% purchased a standalone feed, while 40% use TI feeds included in one or more tools their organization has purchased. Approximately 18% of respondents indicated they used open source threat intelligence feeds, as illustrated in Figure 9.

However, despite the high number of participants utilizing threat intelligence, Table 3 provides evidence that only 80% of respondents use intelligence and analytics tools and the biggest portion (36% of respondents) are only partially integrated with the IR teams.

13 An in-depth discussion of threat intelligence is outside the scope of this paper. For more information on the state of cyber threat intelligence, see “Who’s Using Cyberthreat Intelligence and How?” www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767
This year’s survey also asked participants to describe the types of threat intelligence they are using and the sources of each type. As expected, answers varied from IP addresses to adversary or attacker attribution (see Figure 10).

The statistics in Figure 10 indicate that many organizations rely on a blend of internal and third-party intelligence. However, two key factors may be influential in future surveys:

1. As IR teams continue to grow and develop, one would expect to see a higher level of internally discovered intelligence.

2. As organizations gain experience with threat intelligence firms, they try to realize return-on-investment for their purchases. If internal teams are able to supplement this knowledge, third-party reliance may decline.
Remediating the Incident

Similar to detecting the breach, teams can also measure their effectiveness on remediating incidents. Remediation efforts often require significant amounts of planning to gauge the impact on the business, the cost, actual implementation time and workday disruptions. That being said, IR teams who can insert themselves into the remediation process early in an investigation can help ensure that the organization is remediating efficiently.

The results of this year’s survey indicate that remediation practices are still largely manual. This is expected, considering the level of effort that has to go into performing physical IT tasks, such as replacing a user’s workstation or rebuilding a server. However, a 2015 Gartner survey\(^\text{14}\) found that teams are willing to automate a portion of remediation tasks if the right tools are available. Current automated remediation techniques often rely on tools such as antivirus or digital loss prevention (DLP) to automatically alert about and/or block suspicious activity. Table 4 displays the practices that respondents have in place to remediate incidents. The top three practices in each category are highlighted and indicate that organizations use a myriad of remediation techniques in their environments.

\(^{14}\) Maverick* Research: Is It Time to Fire Your Security Team and Hire the Machines?  
www.gartner.com/doc/3137817/maverick-research-it-time-security [Subscription required.]

<table>
<thead>
<tr>
<th>Practice</th>
<th>Manual</th>
<th>Automated</th>
<th>Both</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolate infected machines from the network while remediation is performed</td>
<td>66.6%</td>
<td>8.4%</td>
<td>18.1%</td>
<td>93.1%</td>
</tr>
<tr>
<td>Reimage/Restore compromised machines from gold baseline image</td>
<td>63.3%</td>
<td>13.0%</td>
<td>16.6%</td>
<td>92.8%</td>
</tr>
<tr>
<td>Block command and control to malicious IP addresses</td>
<td>43.4%</td>
<td>16.0%</td>
<td>32.8%</td>
<td>92.2%</td>
</tr>
<tr>
<td>Shut down system and take it offline</td>
<td>66.6%</td>
<td>5.1%</td>
<td>19.9%</td>
<td>91.6%</td>
</tr>
<tr>
<td>Quarantine affected hosts</td>
<td>51.8%</td>
<td>16.0%</td>
<td>22.3%</td>
<td>90.1%</td>
</tr>
<tr>
<td>Identify similar systems that are affected</td>
<td>50.3%</td>
<td>12.0%</td>
<td>25.9%</td>
<td>88.3%</td>
</tr>
<tr>
<td>Remove rogue files</td>
<td>41.3%</td>
<td>15.1%</td>
<td>31.6%</td>
<td>88.0%</td>
</tr>
<tr>
<td>Kill rogue processes</td>
<td>46.4%</td>
<td>14.2%</td>
<td>25.0%</td>
<td>85.5%</td>
</tr>
<tr>
<td>Remotely deploy custom content or signatures from security vendor</td>
<td>31.9%</td>
<td>25.0%</td>
<td>24.7%</td>
<td>81.6%</td>
</tr>
<tr>
<td>Remove file and registry keys related to the compromise without rebuilding or reinstalling the entire machine</td>
<td>53.3%</td>
<td>9.3%</td>
<td>18.4%</td>
<td>81.0%</td>
</tr>
<tr>
<td>Update policies and rules based on IOC findings and lessons learned</td>
<td>55.4%</td>
<td>8.7%</td>
<td>16.6%</td>
<td>80.7%</td>
</tr>
<tr>
<td>Reboot system to recovery media</td>
<td>61.1%</td>
<td>7.5%</td>
<td>12.0%</td>
<td>80.7%</td>
</tr>
<tr>
<td>Boot from removable media and repair system remotely</td>
<td>56.0%</td>
<td>8.4%</td>
<td>11.4%</td>
<td>75.9%</td>
</tr>
<tr>
<td>Other</td>
<td>2.7%</td>
<td>2.1%</td>
<td>1.2%</td>
<td>6.0%</td>
</tr>
</tbody>
</table>

Table 4. Practices in Place to RemEDIATE Incidents
For the future, IR teams should focus on improving their operations and processes. Furthermore, IR teams should perform self-evaluations and discover new methods to increase their security posture. The best place for a team to begin improving its capabilities is through self-reflection. Analysis of previous engagements, lessons learned and key statistics provides excellent indicators of a team's maturity. Teams should try to lower their dwell, containment and remediation times, where possible, from incident to incident.

In this year’s survey, approximately 46% of participants indicated their security operations center’s (SOC’s) ability to respond to events was either immature or unknown, while only 15% reported their organizations as mature, as shown in Figure 11.

Without proper detection methods in place, it can be difficult for a team to respond to events. Previous detection and threat intelligence response analyses have indicated that while some teams may have the technology or information available, a lack of integration may be impeding the teams’ success. A 2014 Ponemon report found that integration is a critical element of success to identify, verify and resolve cyber attacks.15

Figure 11. SOC Maturity

15 www.idgconnect.com/blog-abstract/9689/top-tips-enterprise-incident-response
To effectively respond to events, organizations must also have mature SOCs. Detection is even more difficult if organizations don’t have mature visibility into their networks. However, only 16% of respondents considered their network visibility infrastructure mature, with 82% reporting their infrastructure as either immature or maturing (see Figure 12).

**Figure 12. Network Visibility Maturity**

Developing visibility into an organization’s network infrastructure can be a long and arduous process that requires years of budgeting and planning. However, even with the correct technology at hand, IR teams still suffer from a lack of knowledge about how to analyze the data.

**TAKEAWAY:**

Identify why you feel your IR team is immature or still maturing. Be sure your team agrees with you, and then put the appropriate growth measures into place.
### Addressing the Real Issue

One of the more important takeaways from this year’s IR survey is the focus on organizational impediments. Staffing shortages and/or a lack of skills are the greatest impediments to effective IR teams for 65% of participants. This figure has dropped only 2% from 2015 and remains a clear leader. Respondents recognize other impediments as well, such as lack of visibility, budgetary shortages and difficulty in discerning between types of attackers, as illustrated in Figure 13.

<table>
<thead>
<tr>
<th>Impediments to Effective IR Teams</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staffing and skills shortage</td>
</tr>
<tr>
<td>Not enough visibility into events happening across different systems or domains</td>
</tr>
<tr>
<td>Budgetary shortages for tools and technology</td>
</tr>
<tr>
<td>Clearly defined processes and owners</td>
</tr>
<tr>
<td>Organizational silos between IR and other groups or between data sources or tasks</td>
</tr>
<tr>
<td>Difficulties in detecting sophisticated attackers and removing their traces</td>
</tr>
<tr>
<td>Too much time taken to detect and remediate</td>
</tr>
<tr>
<td>Lack of procedural reviews and practice</td>
</tr>
<tr>
<td>Lack of ability and resources to support deployment of multiple security systems</td>
</tr>
<tr>
<td>Lack of comprehensive automated tools available to investigate new technologies, such as BYOD, Internet of Things and use of cloud-based IT</td>
</tr>
<tr>
<td>Integration issues with our other security and monitoring tools</td>
</tr>
<tr>
<td>Inability to distinguish malicious events versus nonevents</td>
</tr>
<tr>
<td>Legal/HR/Jurisdictional impediments</td>
</tr>
<tr>
<td>Lack of provisions for dealing with an insider incident</td>
</tr>
<tr>
<td>Difficulties completing and documenting remediation workflow</td>
</tr>
<tr>
<td>Unsatisfactory performance or ROI from IR tools we have in place</td>
</tr>
<tr>
<td>Regulatory impediments</td>
</tr>
<tr>
<td>Overreliance on homegrown scripts and tools</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>

**Figure 13. Impediments to Effective IR Teams**

### TAKEAWAY:

IR teams are aware—and are calling out—that skilled people are their greatest deficiency, year over year. Organizations need to make budgetary allotments to provide analysts with additional training and experience.
Figure 13 provides evidence that IR teams are cognizant of their weaknesses and are calling for help. Despite advances in technology and minor improvements in integrations, teams are still short of experienced analysts to help interpret the data received by the myriad sources available to the SOC. In fact, 73% of participants responded that additional training and certification of staff is the top improvement to be made in their IR program in the next 12 months. Additional improvements include clearer definition of IR processes and owners, and better security correlation analytics capabilities (see Figure 14).

What improvements in IR is your organization planning to make in the next 12 months? *Select all that apply.*

- Additional training and certification of staff
- Better definition of processes and owners
- Better security analytics and correlation across event types and impacted systems
- Improved utilization of current enterprise security tools already in place
- More automated reporting and analysis through security information and event management (SIEM) integration
- Improved visibility into threats and associated vulnerabilities as they apply to the environment
- Improvements to incident response plan and procedures for handling insider incidents
- More integrated threat intelligence feeds to aid in early detection
- Better response time
- Dedicated visibility and monitoring infrastructure to support security systems
- Full automation of detection, remediation and follow-up workflows
- Other
Conclusion

This year’s survey showed promising improvements in internal IR capabilities, as well as diverse industry and global representation. Detection and dwell times declined, indicating IR teams are improving. However, despite granular improvements, organizations continue to doubt their overall IR capabilities and security maturity.

A goal for any IR team should be a focus on restating its value to the organization and continuing to protect the business. Advanced IR teams often assess their processes, find weaknesses or deficiencies and address them quickly. By taking the next step and proactively identifying ways to mature their response capabilities, IR teams continue to prove value and promote the security posture of the organization.

Once again, our survey results indicate the need for more specialized IR skills. As discussed, many employees often wear multiple hats day-to-day, or find themselves repurposed from a support role to an IR role. These individuals are seeking skills to help them respond to incidents—IR response capabilities. Having skilled responders can help ensure an efficient program that is customized for the unique attributes of the organization.

Organizations have shown improvements in technology integrations; however, they still struggle with successfully analyzing the amount of data collected and detecting anomalies in their environments. This challenge, coupled with a shortage of technical and/or response skills, means IR teams should be cautious that the right people are placed on the IR team. A shortage of technical IR staff certainly does not have an immediate fix; however, investments in people can help the organization quickly make up lost ground.

We have seen a change in attackers’ TTPs in the past 12 months. Critical business applications, such as remote access tools, are constantly exploited by attackers to gain and maintain access to an environment. Use of malware, such as ransomware, has grown exponentially, as have infection rates, due to its effectiveness and profitability. Attackers are leveraging PowerShell malware to increase the attack surface. As the landscape changes, IR teams need to be aware of current attacker trends and should be asking questions about their environment. What is normal, what is not? Beginning to think about trends today helps protect your organization tomorrow.
Matt Bromiley, a SANS GIAC Advisory Board member who holds the GCFA and GNFA certifications, is an up-and-coming FOR572 instructor. A senior consultant at a major incident response and forensic analysis company, he has experience in digital forensics, incident response/triage and log analytics. His skills include disk, database and network forensics, as well as memory analysis and network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, sharing with others and working on open source tools.

Rob Lee is the curriculum lead and author for digital forensic and incident response training at the SANS Institute. With more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention and incident response, he provides consulting services in the Washington, D.C. area. Before starting his own business, Rob worked with government agencies in the law enforcement, defense and intelligence communities as a lead for vulnerability discovery and exploit development teams, a cyber forensics branch, and a computer forensic and security software development team. He also worked for a leading incident response service provider and co-authored *Know Your Enemy: Learning About Security Threats*, 2nd Edition.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Secure Japan 2018</td>
<td>Tokyo, JP</td>
<td>Feb 19, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels February 2018</td>
<td>Brussels, BE</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2018</td>
<td>Dallas, TXUS</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS New York City Winter 2018</td>
<td>New York, NYUS</td>
<td>Feb 26, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>CyberThreat Summit 2018</td>
<td>London, GB</td>
<td>Feb 27, 2018 - Feb 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Francisco Spring 2018</td>
<td>San Francisco, CAUS</td>
<td>Mar 12, 2018 - Mar 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Singapore 2018</td>
<td>Singapore, SG</td>
<td>Mar 12, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Spring - Tysons 2018</td>
<td>McLean, VAUS</td>
<td>Mar 17, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich March 2018</td>
<td>Munich, DE</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Canberra 2018</td>
<td>Canberra, AU</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2018</td>
<td>Austin, TXUS</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Spring 2018</td>
<td>Boston, MAUS</td>
<td>Mar 25, 2018 - Mar 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2018</td>
<td>Orlando, FLUS</td>
<td>Apr 03, 2018 - Apr 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Abu Dhabi 2018</td>
<td>Abu Dhabi, AE</td>
<td>Apr 07, 2018 - Apr 12, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Pre-RSA® Conference Training</td>
<td>San Francisco, CAUS</td>
<td>Apr 11, 2018 - Apr 16, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London April 2018</td>
<td>London, GB</td>
<td>Apr 16, 2018 - Apr 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich 2018</td>
<td>Zurich, CH</td>
<td>Apr 16, 2018 - Apr 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2018</td>
<td>Baltimore, MDUS</td>
<td>Apr 21, 2018 - Apr 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Blue Team Summit &amp; Training 2018</td>
<td>Louisville, KYUS</td>
<td>Apr 23, 2018 - Apr 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Seattle Spring 2018</td>
<td>Seattle, WAUS</td>
<td>Apr 23, 2018 - Apr 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh April 2018</td>
<td>Riyadh, SA</td>
<td>Apr 28, 2018 - May 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Doha 2018</td>
<td>Doha, QA</td>
<td>Apr 28, 2018 - May 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta Two</td>
<td>Crystal City, VAUS</td>
<td>Apr 30, 2018 - May 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Automotive Cybersecurity Summit &amp; Training 2018</td>
<td>Chicago, ILUS</td>
<td>May 01, 2018 - May 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC504 in Thai 2018</td>
<td>Bangkok, TH</td>
<td>May 07, 2018 - May 12, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2018</td>
<td>San Diego, CAUS</td>
<td>May 11, 2018 - May 18, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud Security Summit &amp; Training 2018</td>
<td>OnlineCAUS</td>
<td>Feb 19, 2018 - Feb 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>

Last Updated: February 14th, 2018