SANS

A SANS Survey

SANS 2019 Incident Response (IR) Survey: It's Time for a Change

Written by **Matt Bromiley**

August 2019

Sponsored by:

ExtraHop

Analyst Program

Introduction

Information security rarely has a dull day. The past year delivered significant data breaches, impacting industries ranging from hospitality to legal to social media. We've seen a continuation of financially motivated threats, such as business email compromise (BEC), which continue to pillage and drain corporate bank accounts. Ransomware has brought multiple cities to their knees, earning threat actors significant funds in the process. Coupled with the ever-looming threat that a nation–state-sponsored threat actor might pull an organization into its crosshairs, there's little reason to cease vigilance in enterprise networks.

Vigilance requires the ability to be nimble and flexible, especially given the array of options available to threat actors these days. In surveys past, we commended our respondents on improving response times, increasing the use of threat intelligence, and upping the amount of automation and integration within their networks. However, the work is never done; we must constantly be improving. The aforementioned threats aren't necessarily new, but perhaps more refined. For example, some threat actors have moved from noisy, custom malware to "living off the land" with built-in Microsoft Windows capabilities. And in that spirit, we identify the theme for this year's survey: **It's time for a change**.

This year's survey shows *crucial* improvement in incident response (IR). We love some of this year's increases:

- Containment and remediation—two of the most important phases of incident response—saw shorter times.
- Incidents were detected internally at a much higher ratio.
- False positives declined, which we hope means organizations have gotten better at classifying their incidents.

However, even with these improvements, we continue to see problem areas from year to year. Many organizations still show severe gaps in visibility, a critical problem that needs to be front and center. It's tough to truly determine your security posture if you are blind to a portion of your environment. Many respondents again expressed concerns about levels of staffing and skills shortages, problems that may require out-of-the-box thinking.

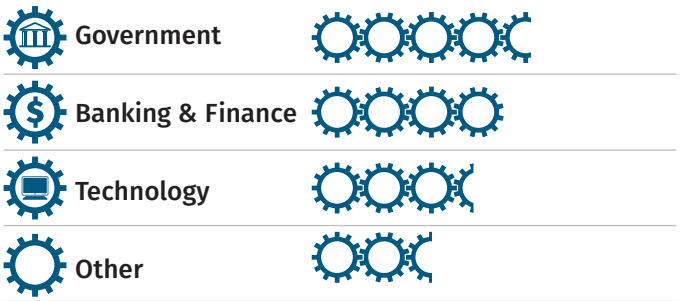
We also saw some different issues take priority in this year's survey, which is a healthy sign of maturity and growth within organizations. Host-based data is by far the largest source of incident data, and respondents indicated this data is largely integrated and automated off of—great news! We also examine an enormous opportunity for organizations to start weaving network-based data into their investigations.

In the pages that follow, we examine the key stats, takeaways and more from this year's IR survey. As you read, we challenge you to examine the issues presented and determine whether your organization shares the same concerns.

Survey Demographics

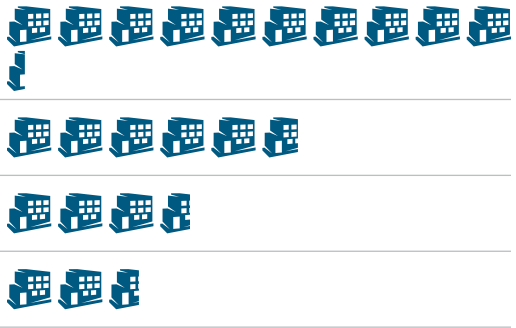
The response pool represented a global group of incident responders from within various organizations. Figure 1 provides a snapshot of those respondents.

Top 4 Industries Represented



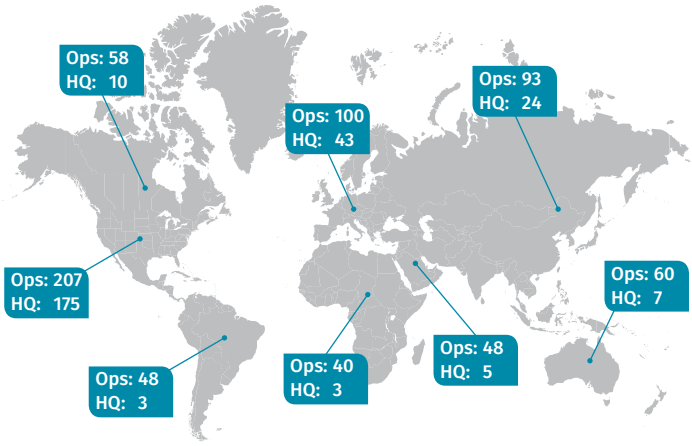
Each gear represents 10 respondents.

Organizational Size

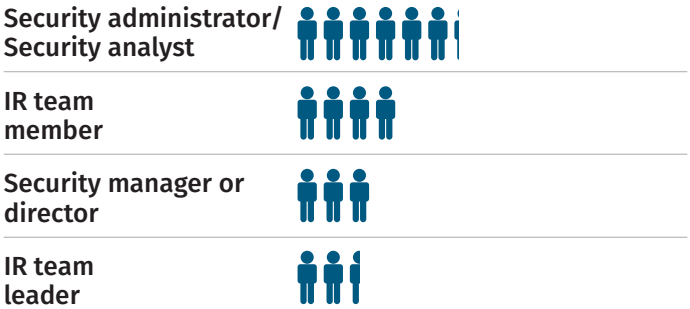


Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 10 respondents.

Figure 1. Key Demographic Information

Some Change Is Already Happening

Before we dig into areas of incident response that must change to continue improving, it's worth noting that this year's survey showed some positive movement in key areas. Organizations are moving into containment and remediation faster and are getting better at detecting incidents, as opposed to waiting for third-party notification. We also saw a strong representation in insider vs. external threats.

Key Time Frames

As we begin to analyze the 2019 IR survey results, we initially concentrate on one set of metrics that focuses on how incident responders are handling true positive incidents. After all, the one question that defines how well an IR or security team is doing is: How quickly are we detecting, responding to and resolving incidents?

Time from detection to remediation is often a strong metric to determine how well your IR team is handling its duties, but you can only adhere to this metric if the team has the tools necessary to do its job!

To determine whether IR teams saw a better or worse year, we begin by examining three key time frames that provide insight on how long it took organizations to take an incident from:

- Compromise to detection (aka the dwell time)
- Detection to containment
- Containment to remediation

We are happy to report that—for the second year in a row—we saw an improvement in the way teams responded to incidents. While dwell time remained flat (still at a healthy 53% detected within 24 hours or less), the most notable improvement is that 67% of respondents indicated that they moved from detection to containment within 24 hours—a 6% uptick from last year. While we'd like to see every organization detecting incidents within minutes, we're glad to see upward movement in how organizations are containing after detection; this is a critical phase of the IR life cycle.

With regard to remediation, we saw a downturn in speed, meaning respondents indicated that they are taking longer to remediate than last year. However, this decline is not necessarily a bad sign. As shown Figure 2, which presents the three time frames, 89% of remediation efforts are occurring within 30 days. This time frame may seem long, but a month to remediate may actually be quick, depending on the nature of the incident and data to be replaced. Remediation can be a complex problem to solve, and we would rather see organizations take the time to perform the right remediation, rather than the fastest.

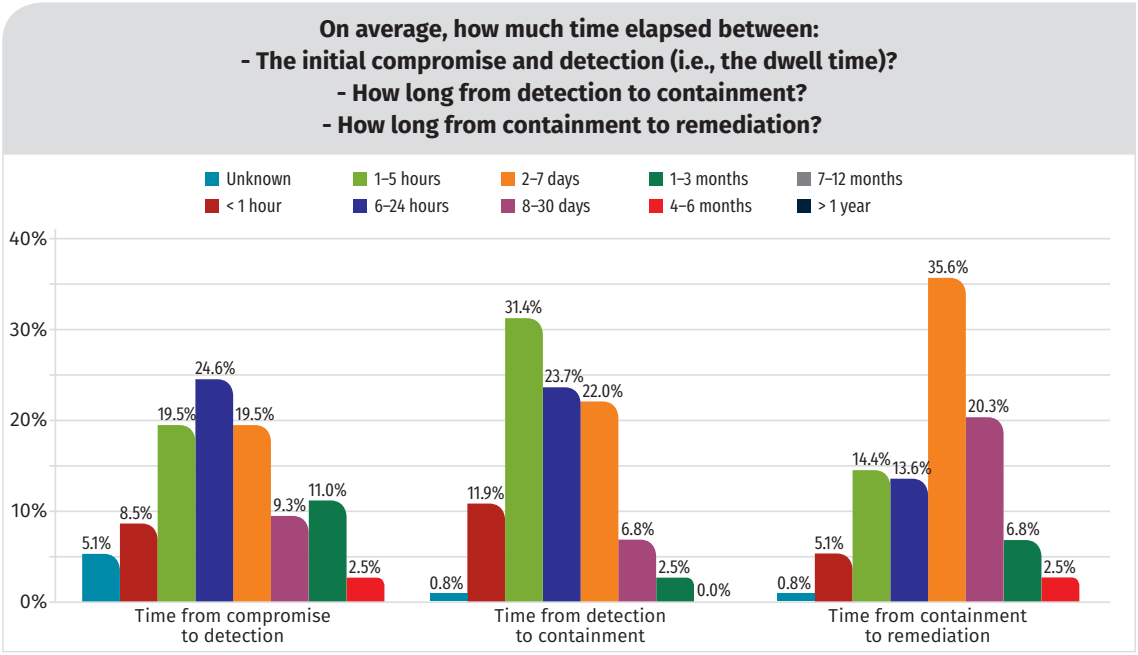


Figure 2. Compromise to Remediation Times[1]

Internal Breach Detection

While on the topic of detection, another area in which we hope to see improvement is in the number of organizations detecting their own incidents rather than relying on a third party for notification. A third-party notification likely means that an organization either has visibility gaps or is unable to properly detect an incident—these situations are not ideal and give threat actors an advantage in the form of time. Time is precious in incident response and is meant to be an advantage that IR teams quickly win back. Fortunately, this year proved that organizations are working hard to reclaim time as their advantage.

[1] Total responses for "7–12 months" and "> 1 year" were both 0.0%.

This was our first year to ask about incident notification, and we were pleased to see that a whopping 64% (see Figure 3) of respondents answered that 51% or more of their incidents were detected internally, as opposed to being identified by a third party. This change is a great starting point, and one that we hope trends upward.

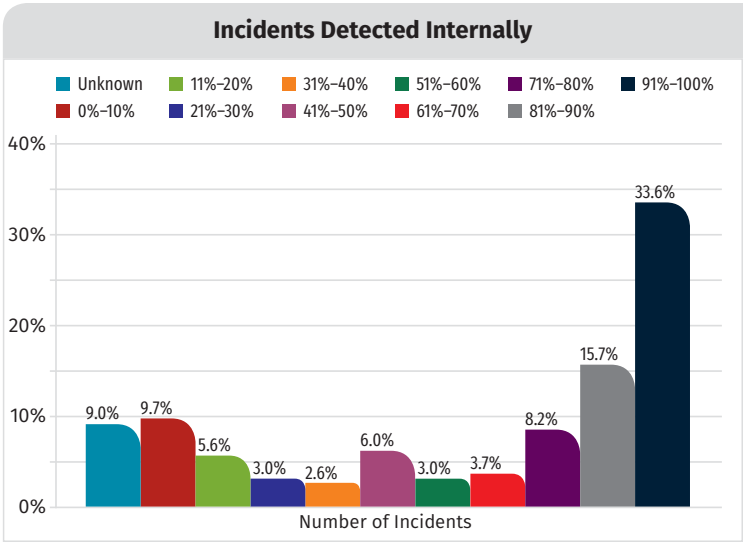


Figure 3. Internal Detection of Incidents

Knowing that most incidents are being detected internally—and thus the IR team is reclaiming the advantage of time—another important metric in determining IR success is identifying how many incidents resulted in breaches of information, systems or devices. The importance of this metric speaks to an organization's capability to track its IR activity and performance. Furthermore, the fewer incident-to-breach conversions an organization has, the more time the security team has to focus on proactive or detection measures.

Incidents Converting to Breaches

As shown in Figure 4, approximately 38% of incidents did not convert to a breach of any kind, a much appreciated 7% increase from last year. We hope this increase is because of improved detection capabilities, as opposed to a decrease in breaches or a lack of visibility. Meanwhile, an additional 39% of respondents who had incidents convert to breaches experienced 25 or fewer breaches. This is a slight uptick from last year, which to us translates to fewer breaches.

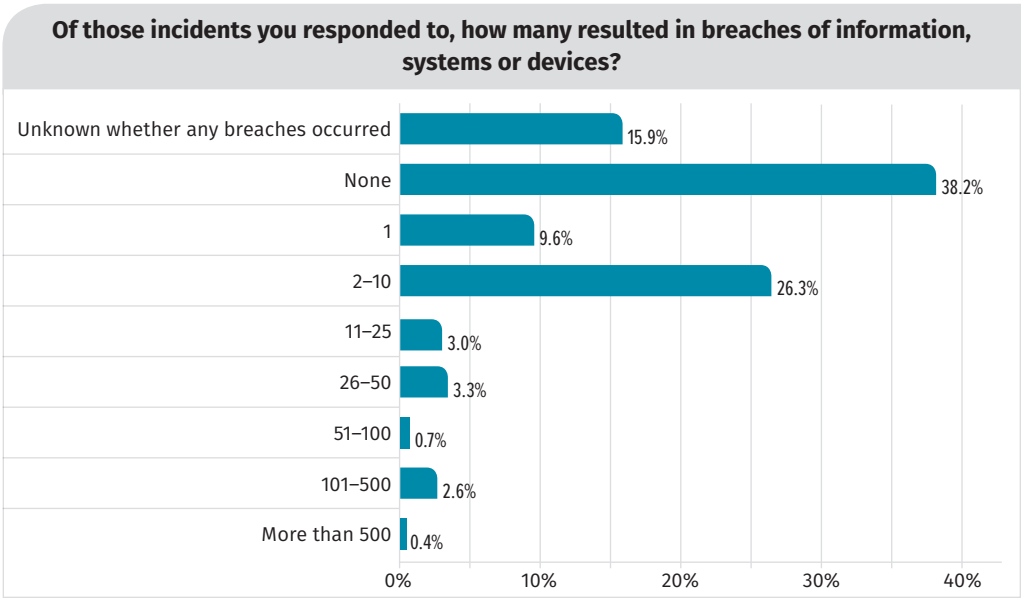


Figure 4. Incidents Turned Breaches

We also asked respondents to identify what components were involved in those incidents that did convert to breaches. Year after year, malware infections continue to rule as the primary component of breach conversion. This year was no different, as malware stayed *almost flat* at approximately 63% of breaches. However, in this year's survey we made some key wording changes and split the Unauthorized Access grouping into internal and external, and the results reflect this important distinction. Approximately 54% of respondents indicated that unauthorized access by an external party contributed to a breach, while only 31% was from a trusted insider.

The distinction of insider vs. external party when it comes to unauthorized access is a critical consideration for IR and security teams. The preparation, landscapes and potential damage differ extremely between the two groups. We hypothesized that unauthorized access was a more significant external party tactic, technique or procedure (TTP), and respondents proved that theory correct. We look forward to seeing how these various components scale out through future surveys.

Figure 5 provides details of these statistics.

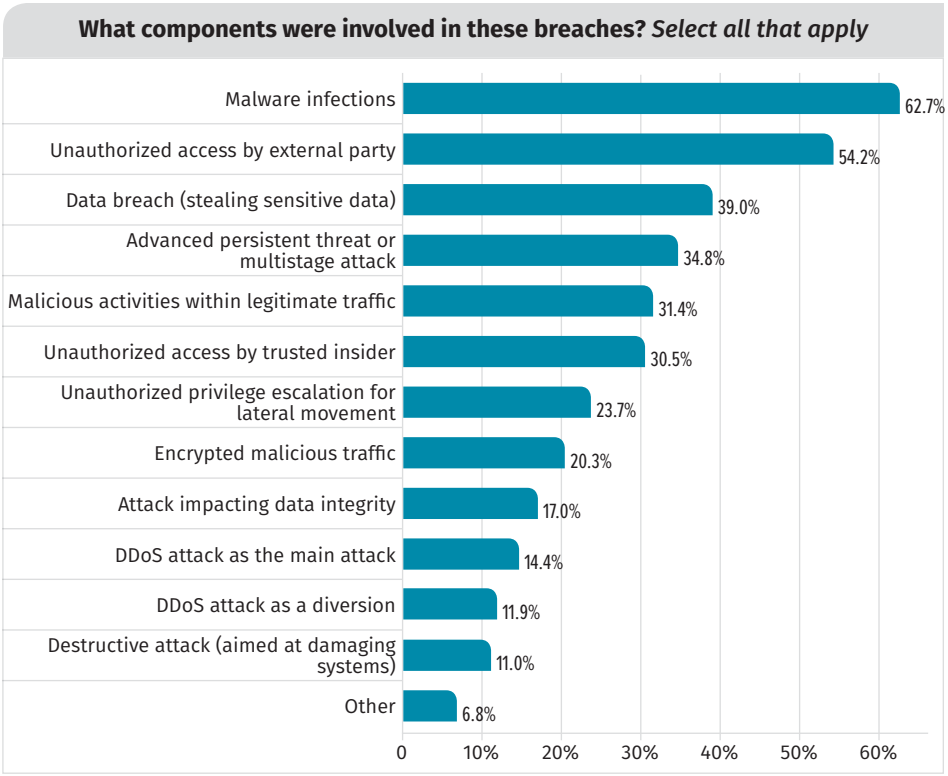


Figure 5. Factors Contributing to Breaches

System Remediation

The next natural step after incident identification and breach conversion is to work toward system remediation. As previously discussed, many of our organizations are completing remediation within 30 days. But how are these remediations taking place? Moreover, is there something to which we can attribute such great growth in incident containment? When compared with the 2018 survey, remediation efforts saw a lot of up and down movement between which tasks organizations have automated and which are still completed manually. For example, approximately 46% of respondents in 2018 manually blocked command-and-control (C2) IP addresses, compared with only 35% this year. We'll happily take an 11% reduction in the name of efficiency.

However, there are areas where respondents moved upward, indicating they are performing more manual operations than before. In 2018, for example, only 46% of respondents had to manually remove rogue files from the infected system, compared with approximately 52% this year. Approximately 58% of respondents this year would need to manually update policies and rules based on investigations (compared with only 52% in 2018). See Figure 6 on the next page.

The preceding statistics represent the key highlights and takeaways with regard to incident detection, breach conversion and remediation. However, one area that we declined to focus on heavily—because it will be addressed subsequently—is that an appreciable number of respondents are still "Unsure" of what has happened or *is happening* within their environments. For example, nearly 16% of respondents were unsure whether any of their incidents turned into breaches.

What processes do you have in place for remediating incidents? Indicate whether the process is conducted manually, through automated systems that are integrated, or a combination of both. ***Choose only those that apply to your organization.***

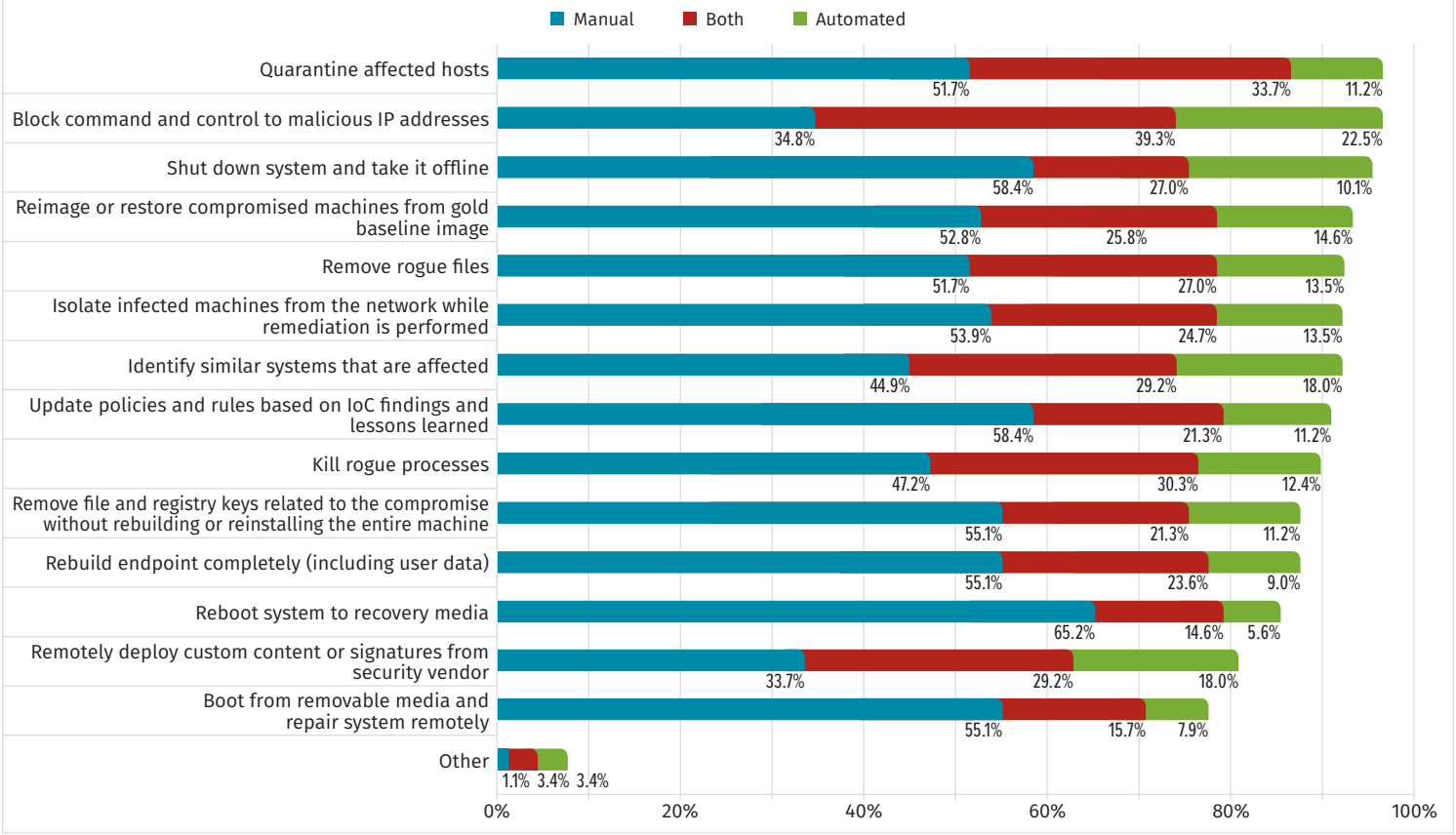


Figure 6. Incident Remediation Processes

Given the complexities of the various regulations and standards that most organizations adhere to today, we had hoped to see these numbers diminish in this year's survey. Alas, we are still experiencing gaps in visibility that need to be addressed. With that in mind, in the following sections we focus heavily on areas where IR teams could improve.

Action Items

Some promising figures in this year's survey show that organizations are detecting and remediating faster than in previous years. We are also seeing better incident-to-breach management. However, this is no time to rest on one's laurels.

Admitting the Problem

We want this year's survey to be a call to action, or a reason for readers to make the changes they've been putting off for so long. The first step, as always, is admitting the problem. Based on this year's survey, we identified a few notable areas where we think some organizations can begin to make some improvements.

Getting the Right Data First

One topic within IR that we are always particularly interested in is what type(s) of artifacts are available and how responders are using them. This year's survey indicated a clear preference for using and obtaining security appliance and host-based data to

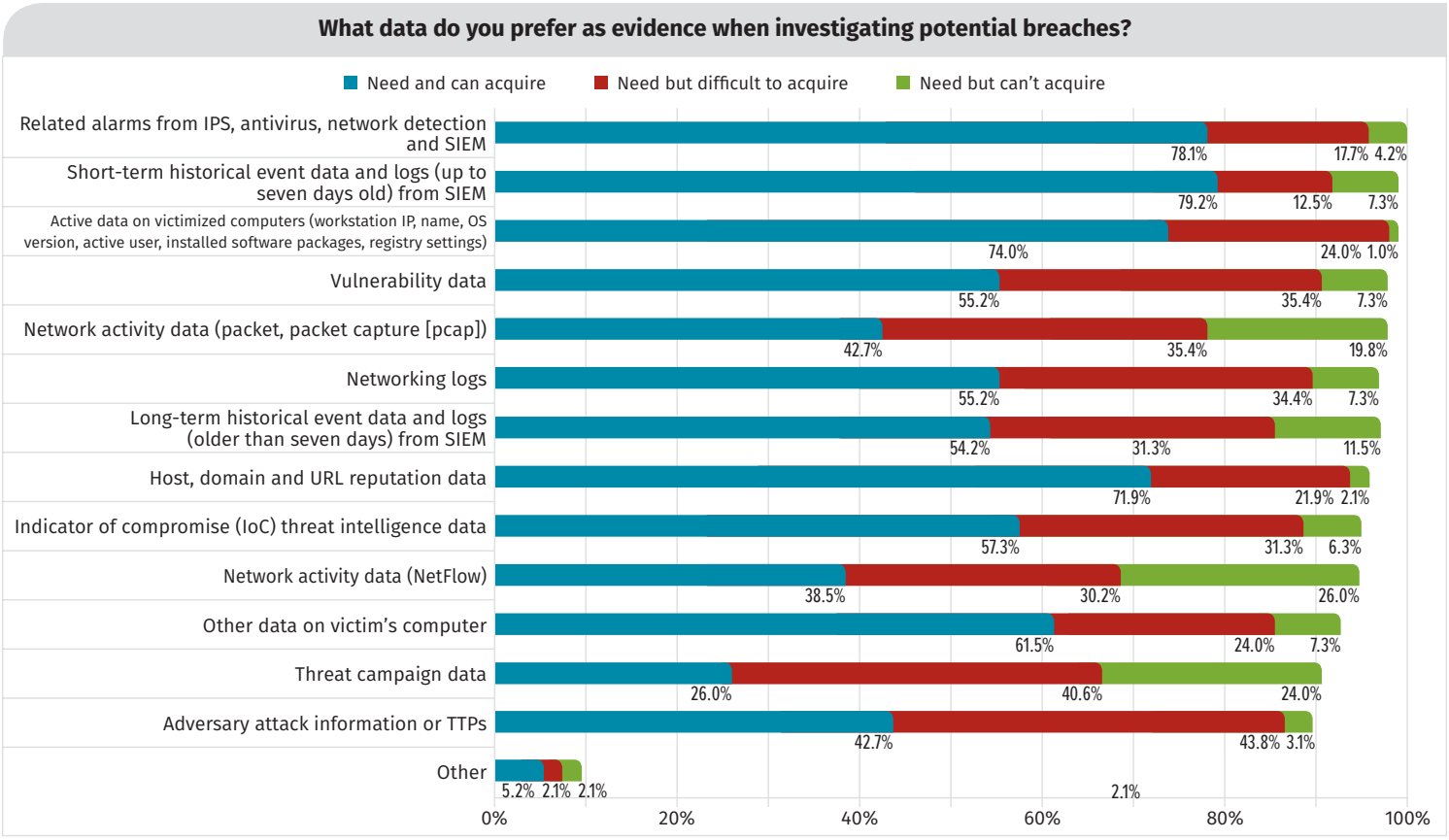


Figure 7. Sources of Evidence for Investigations

support investigations. As shown in Figure 7, a SIEM enables security teams to easily acquire most data, including short-term historical event logs, related alerts from security devices and active data on a victim system.

Respondents admittedly had the most trouble collecting network artifacts, such as NetFlow or PCAP. In our experience, network-based artifacts are sometimes more difficult to collect because of storage reasons or sheer number of collectors needed. For example, it's much easier to cover 1,000 endpoints via host-monitoring than to deploy 100 network sensors to cover those same endpoints via network egress points.

During the results analysis, we hypothesized that the reliance on post-processing data likely resulted from a preference of the types of tools being used and integrated within the environment. Security appliances such as an IDS, IPS, firewall, log analytics or a SIEM (which may be a combination of multiple sources) are the most integrated, at more than 60% of respondents. Capabilities such as decrypting internal and/or boundary traffic are some of the least integrated, which might be due to regulations or the complications of implementing effective encryption man-in-the-middle (MITM). See Figure 8 on the next page.

An organization's reliance on one or two sources of data for incident detection and response is not necessarily a sign of right or wrong. Typically, incident responders look for any and all data that can be used to fill a visibility gap, ranging from arbitrary system logs to network traffic when it's available.

Does your organization use any of the following tools or capabilities to identify impacted systems?
If so, please indicate how integrated each capability is with your overall IR. Leave blank those that don't apply.

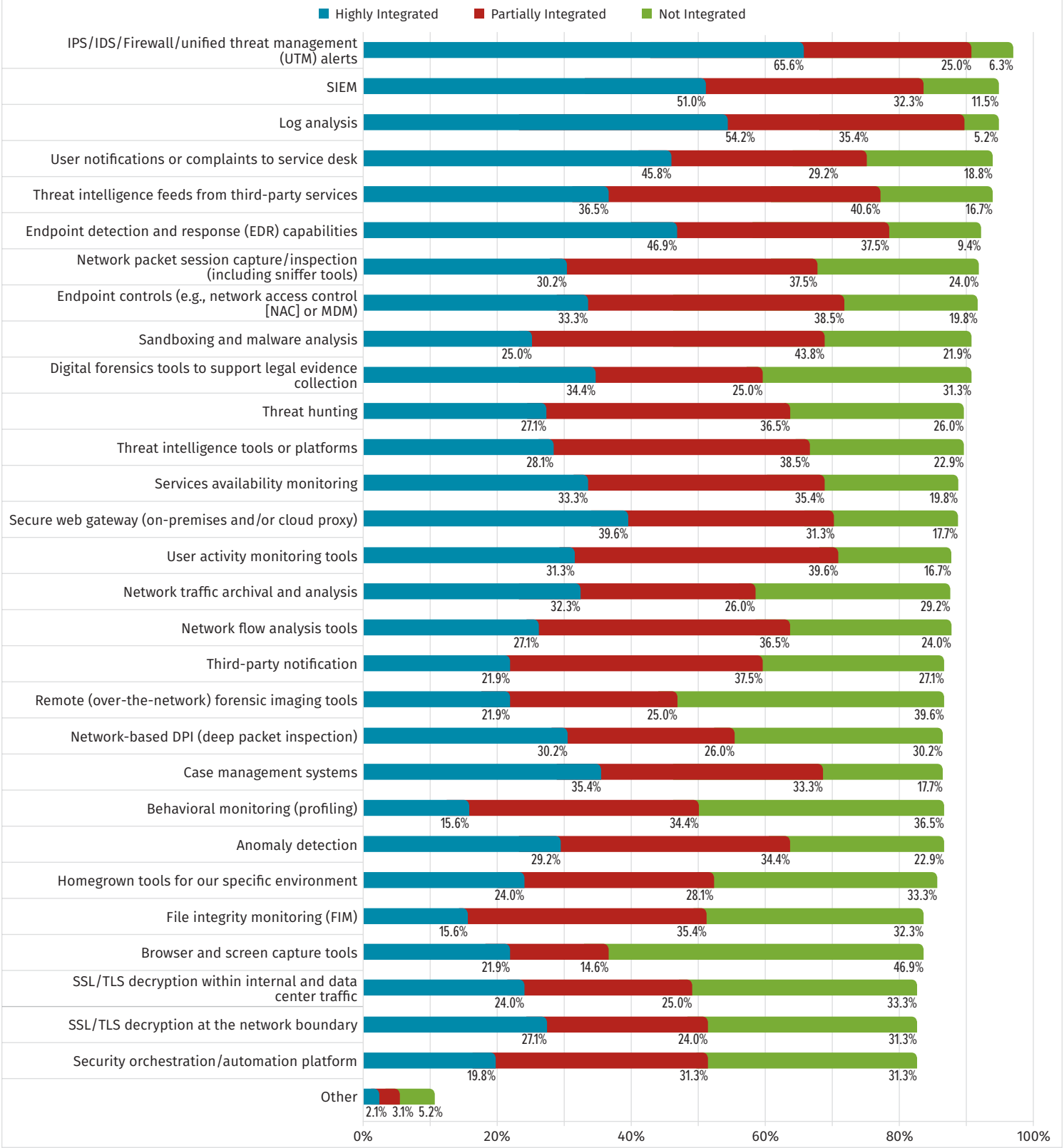


Figure 8. Tools/Capabilities Used to Identify Impacted Systems

Given the spread of integration in Figure 8, it should be obvious that a preference exists for security appliances and alerting mechanisms to identify impacted systems. However, we would like to see a larger contribution from newer, informative detection capabilities such as file integrity or behavioral monitoring, both having high levels of integration as reported by only 16% of respondents. While this number may seem low, it represents an opportunity for forward-planning organizations that might be seeking to implement newer detection and response technology or tools.

Furthermore, anytime organizations rely on post-processed data from an appliance or tool, there is an extremely strong chance that they will be able to take advantage of various automation and integration features. We view this as a significant benefit for incident responders, because it provides a mechanism via which organizations can further integrate additional tooling and automate procedures. (We discuss tool integration in the "Working with What You Have" section later in this paper.)

Action Items

Successful incident response relies on visibility between multiple datasets. Make sure your IR teams have access to all the data points they need.

What Do We Really Need?

One of the more concerning patterns we have noticed from year to year involves an identification of key impediments to effective incident response. Figure 9 shows that once again, a shortage of staffing and skills (57%) and a lack of budget for tools (48%) continue to reign as the key impediments to effective incident response. In fact, 57% of respondents identified staffing shortages and skills shortages as the primary impediment, whereas items such as lack of visibility into cloud-based IT scored only 20%.

In our next challenge to our readers, we encourage you to seek out whether your organization has other inefficiencies that can be focused on and altered before increasing headcount. We're not arguing that some teams

What do you believe are the key impediments to effective IR at your organization? ***Select your top five choices not in any particular order.***

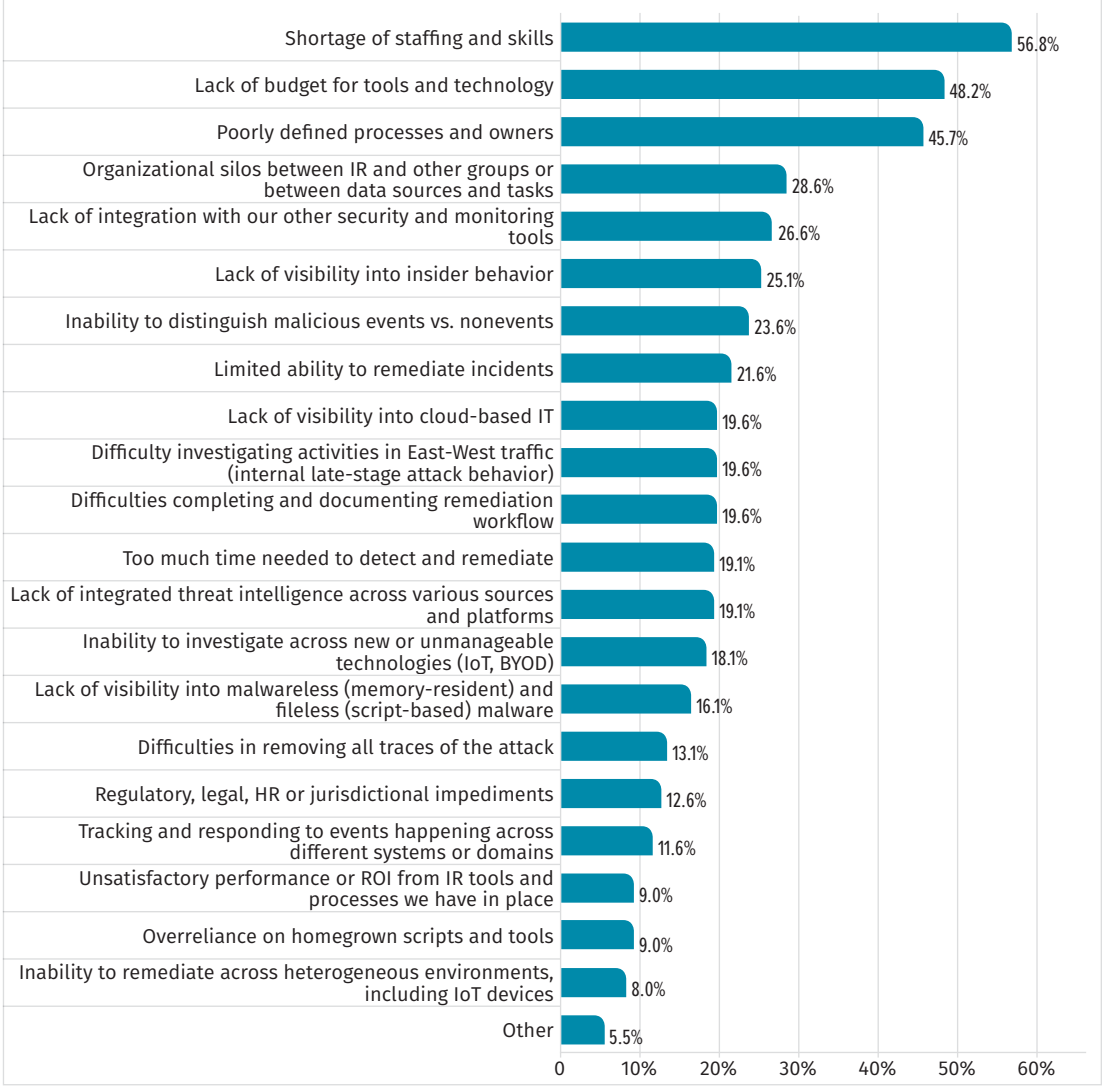


Figure 9. Key Impediments to Effective IR

are short on humans; that's a well-known issue. Our argument instead is that many organizations often have multiple issues that need tending; headcount requires funds, planning and hiring. Instead, look for opportunities to improve your team as it currently is. We look at some thoughts on how to accomplish this in the "Working with What You Have" section.

By saying that a shortage of staffing is a key impediment to incident respondent, we could make an argument that if we simply hired someone, our problems would go away. This is seldom the case; in fact, there's more to work on than headcount.

Fool Me Once...

The last area of concern we identify before we start to focus on how and where we can make improvements is the need to think of incident response as a cumulative, ever-growing practice within your organization. To assess whether IR teams are working in a cumulative manner, last year we introduced a question that focused on repeat breaches. The results were shocking and provided a lot of insight into some of the shortfalls of incident response. This year's results provided some of the same, albeit somewhat improved, results.

In this year's survey, we asked respondents if they had suffered multiple breaches by the same threat actor, and if so, to what degree. Approximately 32% of respondents indicated that yes, a threat actor had returned with either the same or similar TTPs. Only 5% of respondents indicated that a threat actor returned but with different TTPs. Figure 10 illustrates these details.

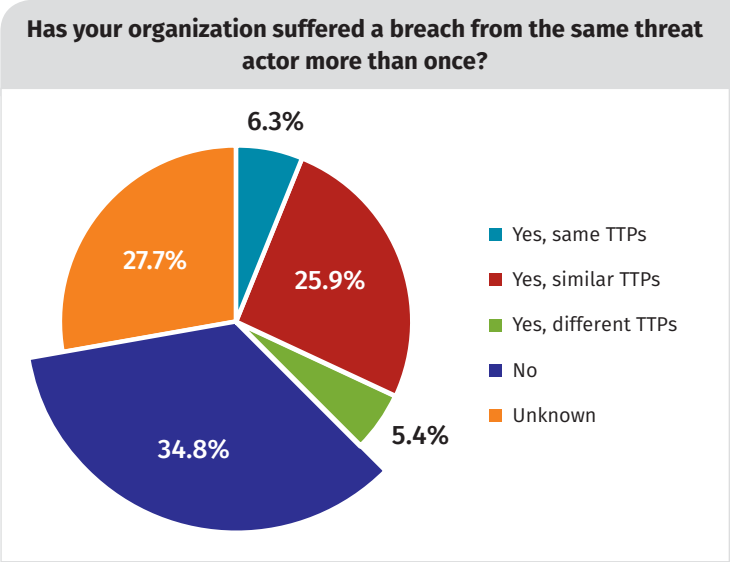


Figure 10. Returning Threat Actors

It's worth pointing out that the 35% who answered no hopefully were able to successfully kick out the threat actor before the actor could retaliate, or were able to perform a holistic remediation effort. However, for the organizations that saw a threat actor return with the same TTPs, we sincerely hope that they caught the returning threat actor significantly earlier than on the first visit. This would prove that the IR team is using knowledge to improve security posture.

Action Items

If threat actors are unable to complete their entire mission in your organization, they will likely be back. Use what you have learned from previous investigations to ensure that the same tactics and techniques don't return.

Working with What You Have

Now it's time to look forward and focus on areas where, within your organization, you can make short-term improvements. We used this year's IR survey to assist in identifying areas where teams may be lacking, and thus ready for an improvement or upgrade. As you read through this section, we challenge you to identify if there are areas within your organization that could use a deeper dive into processes and how you can put your best foot forward.

Growing from the Past to Protect the Future

A natural starting place to try and find efficiencies within your environment is to track and use IR metrics. Metrics can be helpful in identifying low- or high-performing teams, inefficient processes or things that "work really well" within the organization. The possibilities are endless—but you must start recording and using the data!

In this year's survey, approximately 26% of respondents indicated that they are not assessing the effectiveness or maturity of their IR processes, compared to almost 72% of respondents who do have some metric (whether it's an internal measurement or a comparison against public metrics, such as NIST). It makes sense that those teams that track and evaluate their performance and plans—and then cycle the lessons they learned back into the team—will be more effective over time. Figure 11 illustrates how respondents measure their performance.

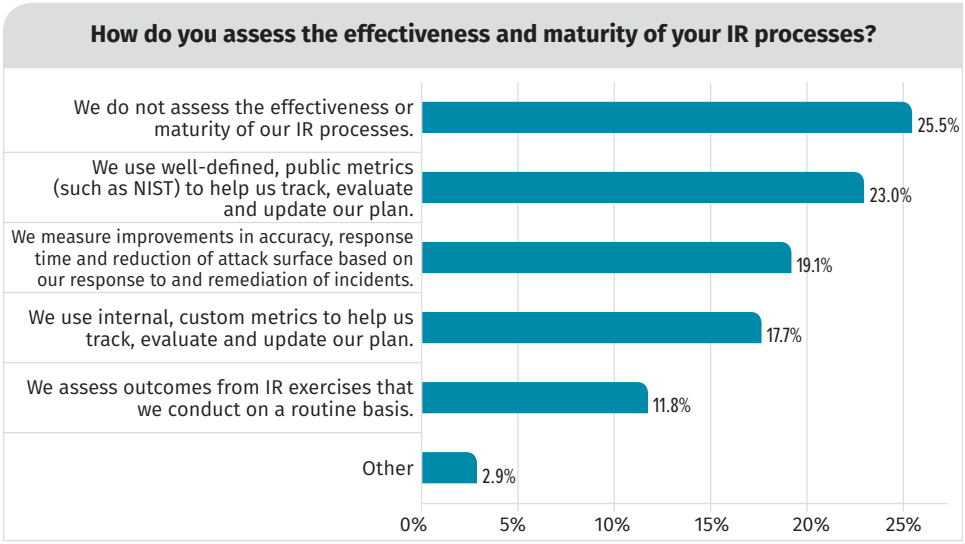


Figure 11. IR Process Maturity and Effectiveness

With this year's survey, we gave respondents the opportunity to specifically state how they have assessed their IR plans and made improvements as a result of these assessments. A few of their high-level quotes, listed here, are perfect examples of how an organization can, if it hasn't already, work to improve IR processes.

- ***"After reviewing our policy after incident response activities, we decided that our policy did not reflect the necessary actions. Policy had to be updated to reflect the actions that must be taken to respond appropriately to an incident."***
- ***"Proper measurement helps to tune false positives."***
- ***"We assessed new methods of attack and used this information to add in additional checks for these new attack vectors. This includes new checks or modifying existing checks to look for the vulnerabilities."***

Whose Responsibility Is It, Anyway?

Another area where, in our experience, a lot of organizations can realize immediate improvements lies in clarifying roles and responsibilities to avoid confusion and duplication. While this is a potential outcome of assessing IR processes, clarifying the roles and responsibilities can sometimes be as easy as simply asking who's in charge of what. Furthermore, it is important to understand how the teams are integrated and how they work with each other.

One survey question to help us get to the root of understanding of who is responsible for what involves understanding just how much of IR and the SOC is in-house vs. outsourced. As shown in Figure 12, a healthy percentage of respondents indicated that both IR and SOC were completely in-house, at 64% and 52%, respectively. In fact, only a *tiny* percentage of respondents had fully outsourced IR (2%) or SOC (5%).

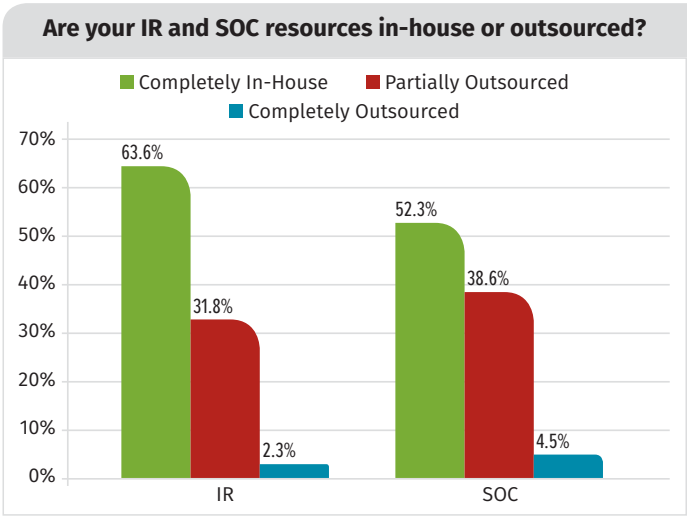


Figure 12. IR and SOC Resources: In-house vs. Outsourced

Given a healthy percentage of in-house IR and SOC teams, we also wanted to identify the level of integration of these teams. As shown in Figure 13, one-third of respondents indicated that incident response is fully integrated with cross-trained members.

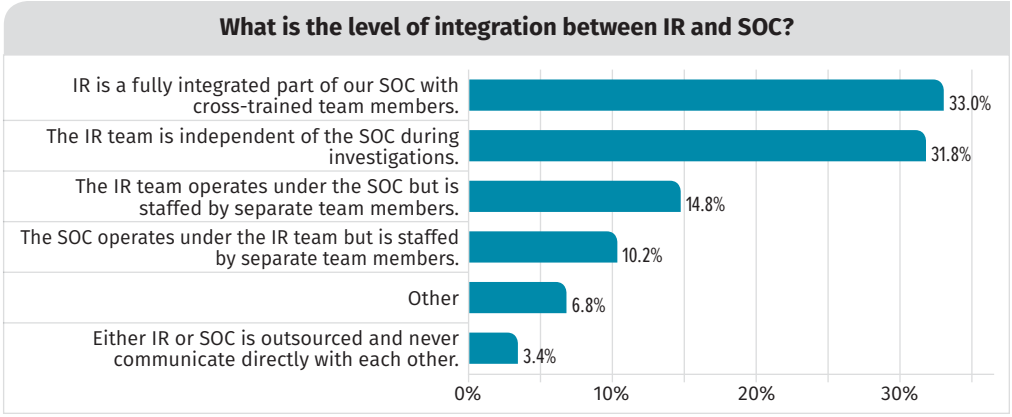


Figure 13. IR/SOC Integration Levels

This is the ideal situation because team members can rotate in and out, back each other up and offer support in conventional ways. A small portion of respondents, only 3%, indicated that either IR or SOC is outsourced and never communicate with each other. While this is a very low percentage, we'd ideally want to see IR and SOC in heavy communication, with cross-training and integration. Because these two teams form a strong methodology to threat detection, response and remediation, it is necessary that they are in constant contact.

Action Items

Clearly identify the responsibilities of your IR and SOC teams. When organizations know who is responsible for what duties, they can act swiftly and with confidence.

Lightening the Load

Last, but certainly not least, we also spent some time in this year's survey looking for clues that organizations are moving toward—or wanting to move toward—automated incident response. Note that automated incident response does not mean a complete takeover of an incident response role; instead, it means finding ways to augment human analysts so they can focus on the hard problems, not the boring and more routine tasks. Fortunately, approximately 65% of respondents indicated that their biggest hurdle right now is time and resources, not money. Granted, budget takes a close second at 51%, followed by various maturity and platform requirements (see Figure 14).

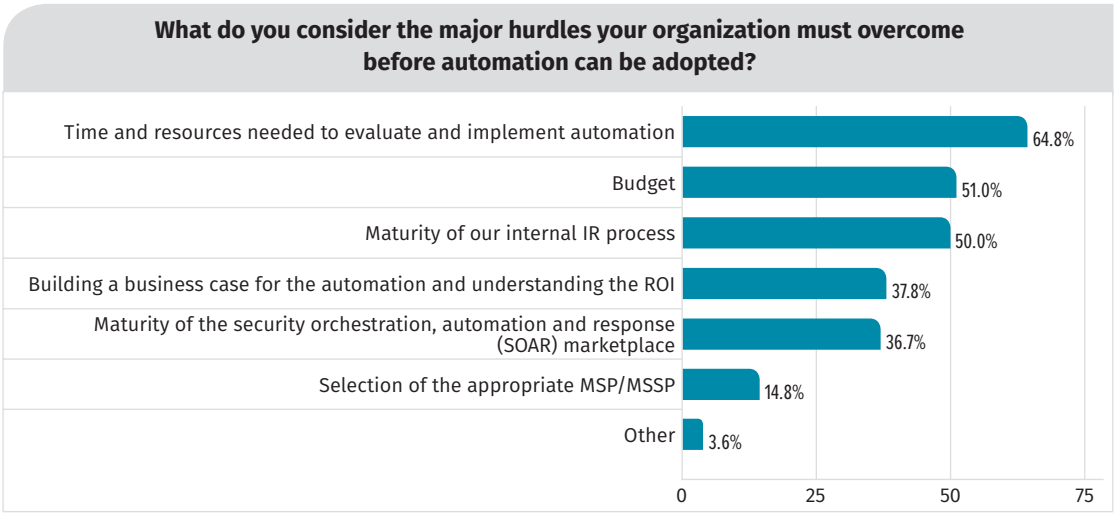


Figure 14. Hurdles to Automation Adoption

Our desire is that IR automation will actually solve some of the problems identified in Figure 14. Better-integrated processes will hopefully free up the time and resources needed to evaluate and implement automation. It's a vicious cycle, but an investment in automation will free up your resources to work on fixing the other areas we've described.

Final Thoughts

In this year's survey, our theme—"It's Time for a Change"—was meant to be a call to action for our respondents and readers. Too often we have seen organizations postpone or downright cancel security improvements that could have drastically improved their capability to detect and respond to security incidents. The IR and/or security teams (if they are separate) are left holding the responsibility of protection. However, this lack of action can lead to enterprise atrophy, as blame—instead of responsibility—is shifted. Thus, we must look to devising a solution with what we have—not what we want.

Year after year, many of our respondents call out the same roadblocks to success—the top three consistently being **time**, **staff** and **money**. However, an increase in one does not guarantee a relaxation in others. Moreover, an increase of one of these does not necessarily increase your security posture. Instead, let's focus on the questions we may be able to address:

- Does our organization use all of the available data points (such as endpoint data or network traffic) in an efficient manner?
- How do we evaluate the IR team currently, and how do we measure these metrics?
- For any security functions we are outsourcing, how do we integrate them into the overall security and response capabilities?
- What areas within security and IR teams could we automate, integrate or significantly improve on?

Let's make one thing clear: Not all problems can be fixed internally. When needed, bring in outside help, hire more qualified staff and implement technologies to make your organization more secure. However, recognize the actual problem first. We challenge our respondents and readers to take the next year and answer these questions for their organizations. Focus on gaps in visibility, automate manual tasks and get your various teams talking.

It's time for a change. And the time to start is now.

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching FOR508 (Advanced Digital Forensics, Incident Response, and Threat Hunting) and FOR572 (Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response). He is also an IR consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory, and network forensics, incident management, threat intelligence, and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching, and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

ExtraHop
Rise Above the Noise.