SANS

Analyst Program

Survey

SANS 2023 Incident Response

Written by **Megan Roddie** and **Terrence Williams**

September 2023

DEVO

©2023 SANS™ Institute

Executive Summary

Incident response (IR) capabilities continue to play a major role in an organization's security posture. The people, processes, and tools of an organization affect its ability to respond in the case of an attack. The purpose of the SANS 2023 Incident Response survey is to look at all the aspects involved in creating a robust IR program and attempt to gain insights into what is and is not working.

The last time SANS performed this survey was in 2019, before the pandemic had a major impact on the world and on the cybersecurity industry. At the time, the survey called for a change in the status quo—and based on what we saw when comparing this year's data with 2019 data, that change did occur. The work is not done, however. This year we use the survey findings to propose actionable methods to continue this positive momentum and mature IR capabilities even further. First, let's look at where we saw the positive change occurring. Even as we review the positives, remember that evidence shows that the industry still has room for improvement. Based on our analysis, the following key areas show IR moving in a positive direction:

- Organizations are more efficient and effective in the areas of containment and remediation.
- Organizations are improving automation efforts for remediating incidents.
- Organizations are integrating IR as part of the security operations center (SOC).
- Organizations are more regularly performing any assessments of their IR processes.

Looking at the challenges that remain despite these improvements, we see that organizations need to extend their efforts and set priorities around the following actions:

- Staff recruitment and retention
- Reevaluating responses to malware impacts

Throughout this survey, we look at how programs have evolved since the 2019 survey, where gaps remain, and how we can solve outstanding challenges. The response pool represented a global group of incident responders from within various organizations. Figure 1 provides a snapshot of those respondents.

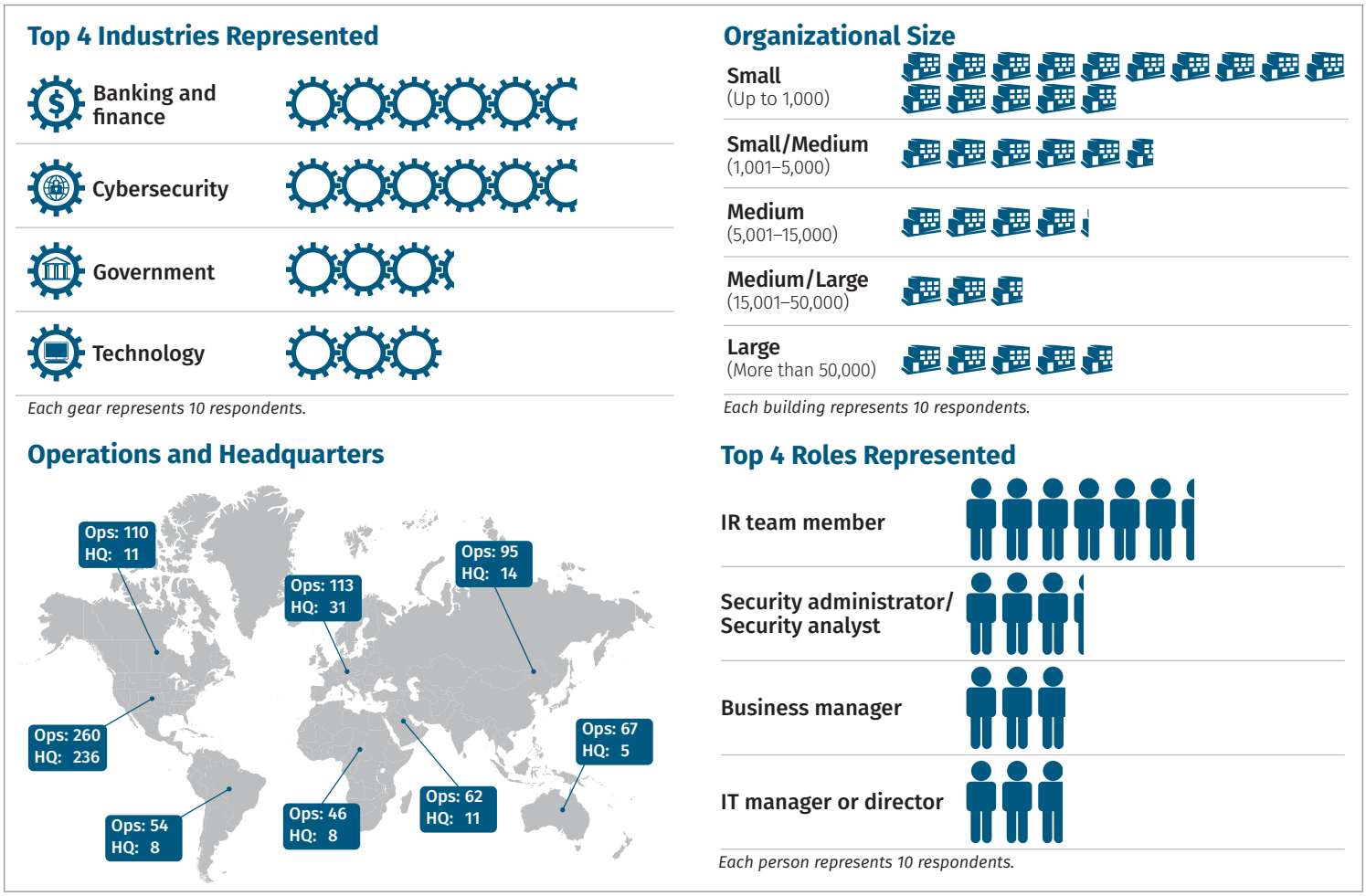

Figure 1. Key Demographic Information

Key Time Frames

The analysis of the 2023 IR survey results begins by focusing on how incident responders handle true positive incidents. One key metric is the time it takes organizations to identify, respond to, and remediate incidents. This question has become broader as organizations seek to avoid being featured in headlines related to the latest breach. The 2023 survey uses this year's data while also examining the results from the 2019 SANS Incident Response survey.

To determine whether IR teams have improved since the previous survey, we examine three key time frames that provide insight into how long it takes organizations to handle incidents (see Figure 2):

- Compromise to detection (also known as *dwell time*)
- Detection to containment
- Containment to remediation

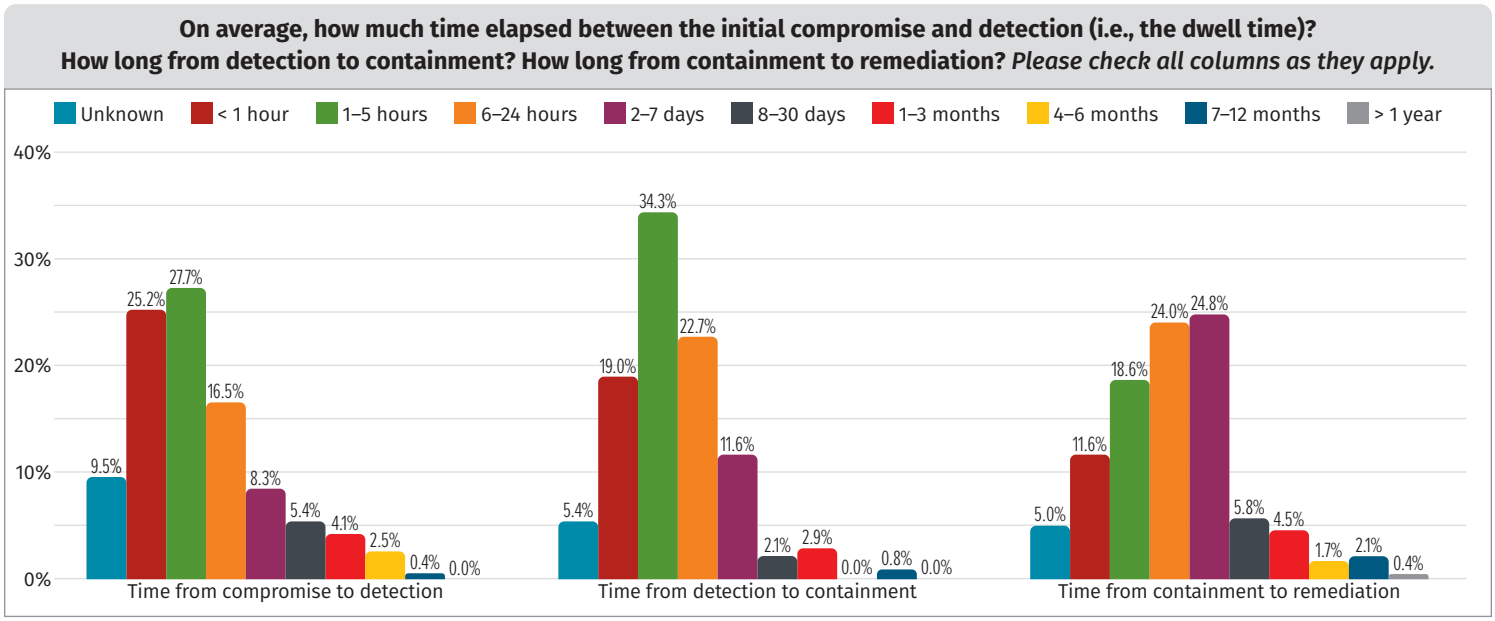

Figure 2. Key Time Frames in Incident Handling

The previous report showed a decrease, from 2018 to 2019, in time to containment and time to remediation. In this year's dataset, we once again see improvement in response times for incidents. Over the past three years, organizations have demonstrated an increased ability to detect incidents within 24 hours, with a 17% increase since the 2019 survey.

During the time period covered in the previous survey, the dwell time remained flat at a steady 53% detection rate. The increased ability to detect incidents within 24 hours appears to have led to a 9% increase in efficiency for the time from detection to containment. Containing the incident after detection is a critical phase of the IR process, and organizations have demonstrated its importance by containing 76% of incidents within 24 hours.

Organizations' remediation efforts continue to trend upward. As shown in Figure 2, organizations are remediating 54% of incidents within 24 hours after containment of the incident. The combination of detection, containment, and remediation metrics all trending upward shows that organizations have placed an increased emphasis on creating efficient IR processes.

Incidents by the Numbers

As previously stated, organizations have improved their responses to incidents. Now let's look at what types of incidents they were responding to.

Organizations are proving that their internal IR processes have become more refined through the increase of incidents detected internally. Ideally, we would like to see organizations show an upward trend of incidents not responded to and a downward trend of false-positive rates. From 2019 to 2023, incidents not responded to trended upward by 10%. However, the false-positive rate increased from 2019 to 2023. See Table 1.

Table 1. False Positives per Incidents Detected

Year	% Incidents Detected	% False Positives	% False Positives per Incidents Detected
2023	80.6%	95.8%	77.2%
2019	88.9%	75.9%	67.5%

The previously mentioned refined processes are in contrast with the false-positive rates that show that 23% of organizations are dealing with a 75% to 100% false-positive rate, based on organizations' self-reporting of incidents to which they responded. The desired outcome as organizations refine their processes is a noticeable downward trend in false-positive rates and false positives detected per instance.

Most organizations are responding to incidents that are routinely detected internally by their own monitoring and detection tools. Figure 3 shows that approximately 47% of organizations reported 75% to 100% of the incidents responded to as internally detected. Compared to 2019, this metric is holding steady across the years.

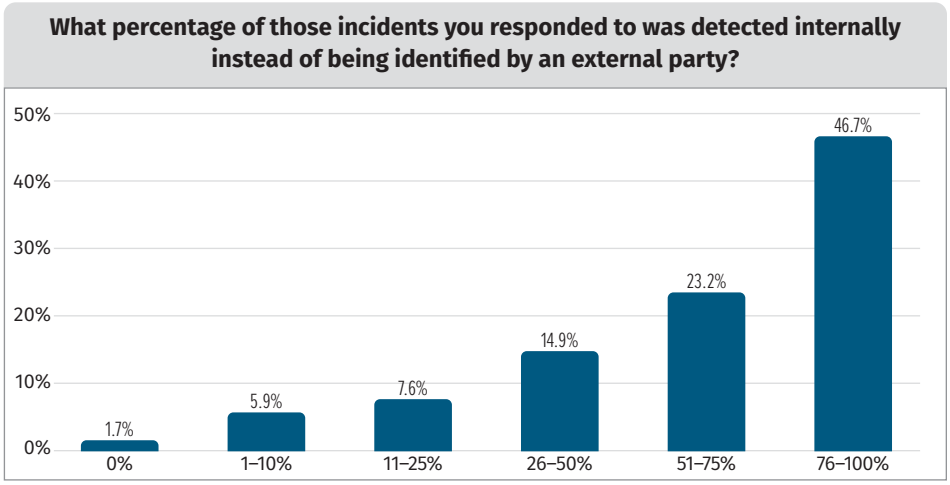

Figure 3. Incident Detection by Internal Party

Incident Rates

In this survey, we sought to identify the impact the cloud environment has on IR processes. The cloud environment proved to be a heightened target of incidents for organizations, with 18% of organizations surveyed identifying that 75% to 100% of their incidents occurred within a cloud environment. Unsurprisingly, more organizations report more incidents in the cloud since the COVID-19 pandemic led to an incredible uptick in organizations leveraging the cloud for their workloads.

The sources of compromises have remained consistent over the survey; however, some categories have shown growth. Business email compromise (BEC) is a leading source of compromise, with a reported rate of 42%. This isn't surprising, considering that email serves as a prime target for phishing attacks, which attempt to exploit users within an organization.

In the 2019 survey, with no separate option for ransomware, malware infections accounted for a commanding 62% of sources of compromise. This year we specifically highlighted ransomware to understand its impact on organizations. Combined, malware infections and ransomware accounted for 55% of the sources of compromise this year, with ransomware having a reported rate of 20%. The rise of ransomware in recent years indicates a changing landscape that encourages organizations to prioritize the impact of malware on their operations.

Impact of Incidents

The positive patterns of incident response that organizations demonstrated helped reduce the number of incidents that resulted in breaches. The containment and remediation phases have proven effective for organizations, as only 62% of organizations reported that 0 to 10 incidents led to a breach. Although this marks a decrease from the 2019 figure of 74%, it's important to note the increased incident count and the shift in the threat landscape due to the pandemic, which has led to a vast number of employees working remotely.

This changing threat landscape is evident when evaluating the systems that have been involved in the reported breaches. See Figure 4.

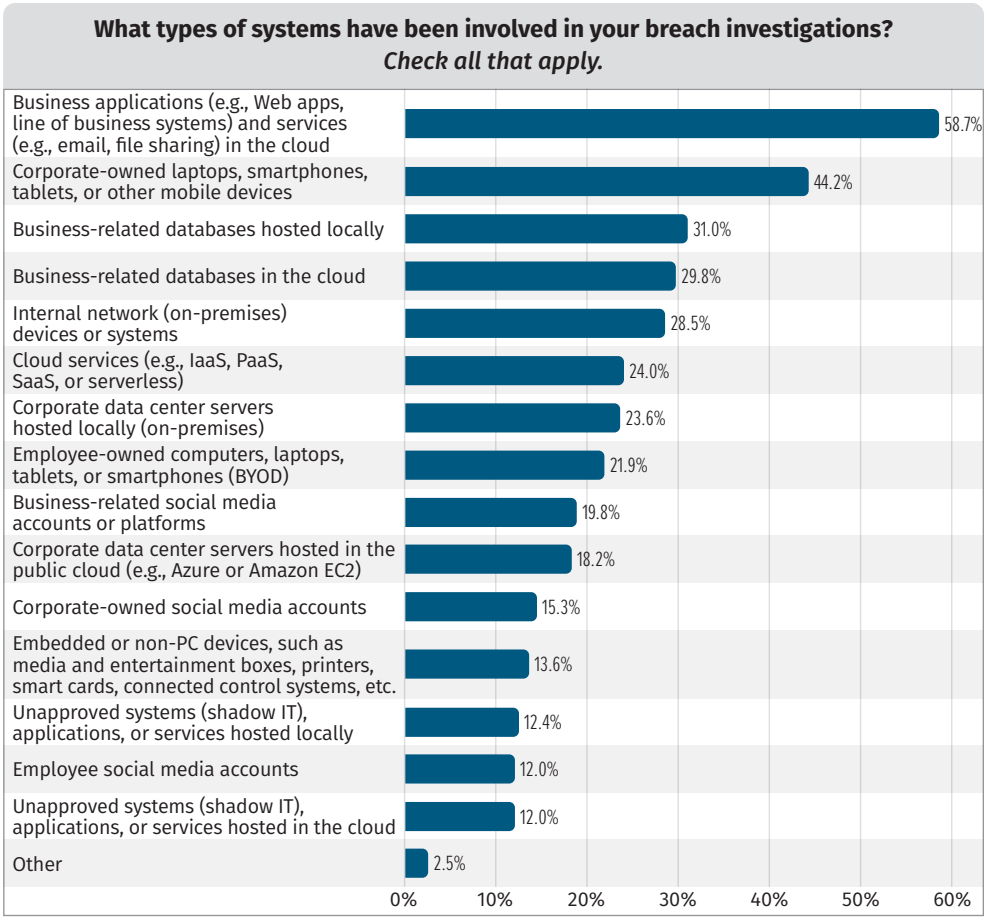

Figure 4. Systems Involved in Breaches

Business applications (e.g., web apps, line-of-business systems) and services (e.g., email, file sharing) in the cloud and on corporate-owned laptops, smartphones, tablets, or other mobile devices led the systems involved in a breach at 59% and 44%, respectively. These two categories show a downward trend when compared to 2019, although these categories still led at 72% and 71%, respectively. Organizations have made significant progress in curbing unapproved or unauthorized systems, evident by the downward trends across categories as compared to the 2019 survey. Over the years, there has been a 6% reduction in the number of unapproved systems (shadow IT), applications, or services hosted in the cloud.

It is encouraging to see the refinements that organizations have made over the years. Unfortunately, room for improvement still exists. The 2019 survey identified returning threat actors with the same tactics, techniques, and procedures (TTPs) as a source of concern for organizations. This year's findings remind us that we are not learning sufficiently from past incidents. Forty-three percent of respondents reported they suffered from returning threat actors with the same or similar TTPs. We expected that metric to decrease as organizations became more efficient in their containment and remediation efforts, but the actual result was quite the opposite, showing an 11% increase over the figures from 2019.

Organizations are improving automation efforts to address incident remediation. The current survey shows a positive decrease, by 15%, in manual efforts to remove rogue files. We expect this trend to continue positively as systems deployed in these efforts advance. However, there remains a manual component, with 40% of updates to policies and rules based on indicator of compromise (IoC) findings and lessons learned still being carried out manually. This indicates a progression in automating the processes to expel threat actors from the environments, while manual efforts persist in preventing their intrusion.

Incident Handling

According to the data, respondents show a high adoption rate of a handful of technologies that they utilize to identify impacted systems during an investigation. The most highly integrated capabilities for acquiring evidence are endpoint detection and response (EDR) capabilities (60%); security information and event management (SIEM) (52%); intrusion prevention/detection system, firewall, and unified threat management (IPS/IDS/firewall/UTM alerts) (50%); and log analysis (48%).

Although few respondents showed SIEM and EDR as technologies that are not integrated within their impacted systems identification, organizations reported high manual processes that align with the capabilities of SIEM and EDR technologies. Manual processes, such as updating policies and rules based on IoC findings and lessons learned (40%), isolating infected machines from the network while remediation is performed (37%), and removing file and registry keys related to the compromise without rebuilding or reinstalling the entire machine (37%) align with the integration of EDR capabilities. Organizations can automate these manual processes by utilizing the IoC findings and lessons learned and integrating them into EDR solutions.

The leading evidence types for incident handling include active data on victimized computers; host, domain, and URL reputation data; indicator of compromise (IoC) threat intelligence data; related alarms from IPS, antivirus, network detection, and SIEM; and vulnerability data. The percentages for acquirable evidence types range from 59% to 70%, but some needed evidence types are not acquirable, which may present challenges in incident handling.

Malware Analysis Capabilities

The survey shows a shift in organizations' approach to malware analysis, as they increasingly adopt commercial technologies, leading to a decline in the use of dedicated internal teams or individuals for this purpose. In 2019, 88% of organizations invested in dedicated internal teams or individuals. In 2023, this number decreased to 83% (see Table 2). The reduction in the use of teams or individuals aligns with a 9% rise in the adoption of commercially provided sandbox (internal) systems for collection and analysis. Similarly, there has been a 2% uptick in the utilization of third-party (external) services. It's encouraging to observe organizations gravitating toward optimal solutions, even though this shift comes at the cost of an internal knowledge base. See Figure 5.

Table 2. Internal vs. External Malware Analysis

	2019	2023
Dedicated (internal) malware analysis team or individual	88.2%	83.3%
Commercially provided sandbox (internal) for collection and analysis	76.3%	84.5%
Third-party (external) services	76.3%	78.2%
Other	7.5%	27.6%

The year's survey results indicate that organizations need to be more proactive about their incident handling and malware analysis capabilities. By prioritizing the acquisition of leading evidence types and the integration of SIEM and EDR capabilities, organizations can improve their ability to handle incidents effectively and efficiently. Additionally, organizations should consider the use of third-party services for malware analysis to ensure that they have access to specialized expertise.

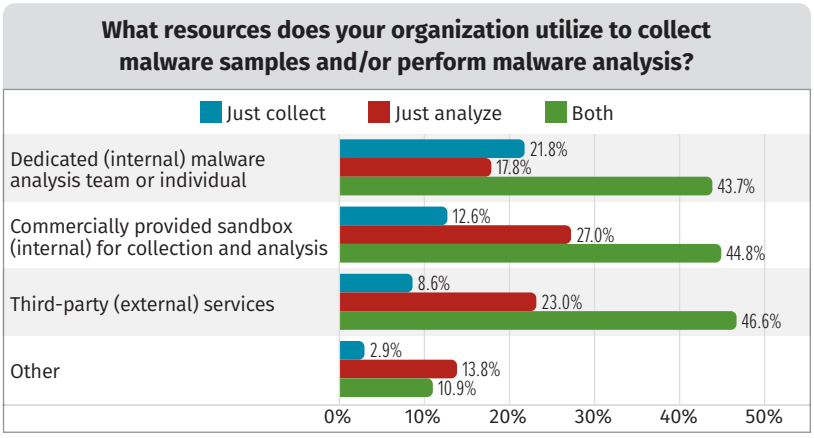

Figure 5. Resources Used to Collect Malware Samples and/or Perform Malware Analysis

It is important to note that the changing landscape of incident handling and malware analysis capabilities requires organizations to be adaptable and flexible in their approach. As threats continue to evolve and become more complex, organizations must be prepared to adjust their strategies and incorporate innovative technologies and methodologies to effectively address these threats.

Security Budget Allocation

In this year's survey, we examined budget and staffing trends more closely. We wanted to understand the extent to which organizations are supporting their IR teams from a funding perspective. Also, because incident responders themselves have a major impact on the IR program's performance, it is important to understand how organizations staff their teams and support those employees.

Respondents were asked what percentage of their security budget they dedicated to the IR team. Of those who knew the budget allocation, most respondents said that they allocated less than 30% of the current budget for security (to the IR team specifically). Given the scope of what is involved in securing an organization, this is not necessarily surprising, because many teams and products require funding. More interesting is the trend of what respondents allocate now versus what they expect to allocate in the next 12 months. Although not a significant change, there was a slight increase in allocation for IR, indicating organizations are investing more in their IR teams. See Figure 6.

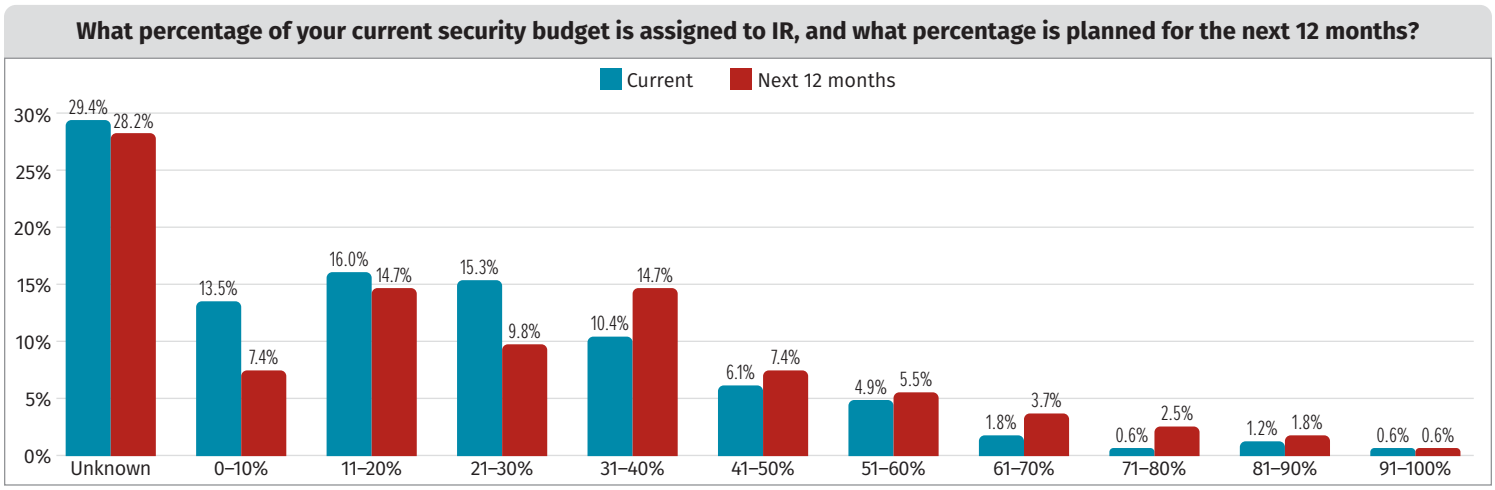

Figure 6. Percentage of Security Budget Assigned to IR

Staffing

Depending on the size of an organization, it may or may not staff its IR team internally. Back in 2019, we looked at whether IR and SOC teams were being staffed internally or partially or fully outsourced. At that time, we saw that more than half of organizations staffed both teams internally. From the perspective of IR teams, we saw little change in the percentage of organizations outsourcing those responsibilities. Interestingly, however, this current survey shows a slight increase in the outsourcing of SOC responsibilities. Across both surveys, IR teams were more often in-house than SOC teams (see Figure 7). One reason for this may be that organizations think the third parties are better suited for triaging alerts, whereas the criticality of incident response and the sensitivity involved make it preferable to keep IR in-house. Another possibility is the financial aspect of outsourcing. It may be more affordable to outsource an SOC, whereas the specialty nature of IR and the retainer model often can lead to large expenses. Regardless of the cause, it's interesting to see that in-house staffing of IR teams is more common than in-house staffing of SOC teams.

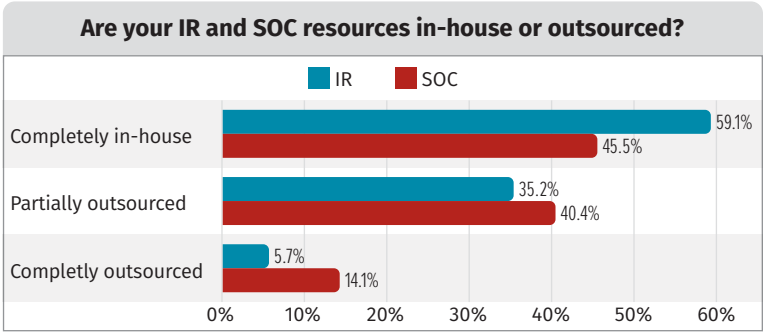

Figure 7. In-House vs. Outsourced IR and SOC

Examining the integration of both these teams reveals a positive trend. Between 2019 and 2023, full integration remained steady. One change we saw is that some responses indicated a lack of integration, replaced with teams where either the IR team operated under the SOC or vice versa but with dedicated employees in each role (see Figure 8). We consider this to be a positive trend due to the benefits of cross-collaboration between teams. With the support of the SOC, incident responders can gain valuable insight and support from staff who are often more hands-on in the day-to-day environment.

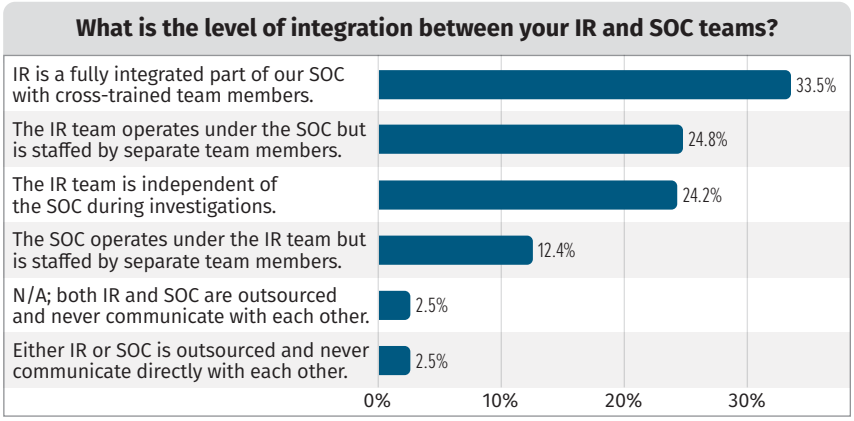

Figure 8. Level of Integration Between IR and SOC Teams

The last point the survey looked at regarding budgeting and staffing was how organizations approach the hiring and training of staff members, as well as why employees choose to leave an organization. First, we wanted to understand what hiring managers are seeking when reviewing candidates. The top attribute desired from candidates is industry experience. This is not surprising given that experience is the best way to develop skills in the field, if choosing between someone who has never had practical experience and someone who does.

More interesting is what organizations are looking for from an education perspective. Although university degrees traditionally have been highly valued across industries, the security industry is putting a heavier weight on security certifications now, with the same percentage of respondents indicating certifications are top attributes as they did with experience (66%). Only 49% of respondents, however, considered academic experience as a top attribute of candidates. Several respondents provided custom responses highlighting the importance of analytic skills, attention to detail, and a personal interest in cybersecurity.

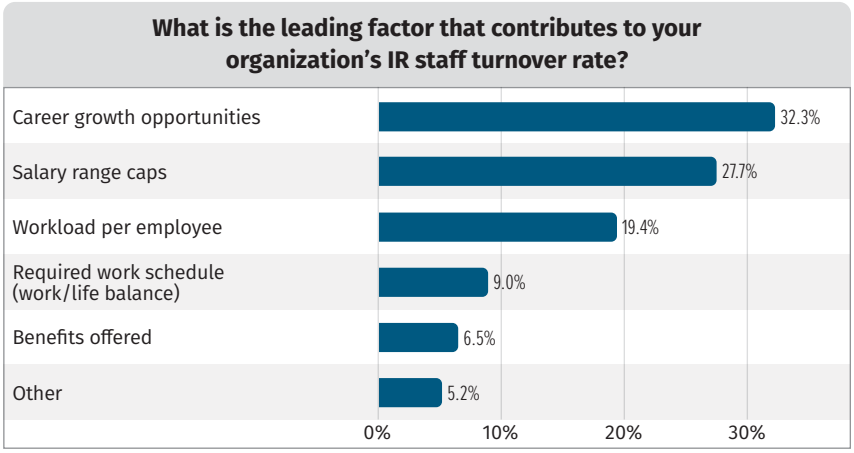

Figure 9. Leading Factors Contributing to IR Staff Turnover

One of the biggest challenges that comes with staffing an IR team is keeping those employees. With the talent gap in the industry and the specialized skills of incident responders, it can be a challenge to retain talent because many opportunities will arise for people with that skill set. To determine why organizations are losing their incident responders, we asked respondents why some of their staff members pursued other opportunities. The results showed that the primary causes of staff turnover were career and salary growth opportunities, with the workload assigned being a secondary factor (see Figure 9). Seemingly, the benefits offered did not greatly impact turnover rates across the board. This shows that if organizations want to retain employees, they should focus less on supplementary benefits and more on providing a role in which employees can grow, along with a salary that will grow, too. To reduce the impact of the workload assigned to users, we should look at the benefits of automation, as discussed later in this report.

Assessment, Improvement, and Impediments

Among other things, this section examines how organizations learn from incidents to make their programs better. In 2019, 26% of respondents indicated they were not performing any assessments of their IR processes. In a positive trend, that number has decreased, with only 19% of respondents falling into this group in 2023 (see Figure 10). Those who did assess their programs have focused their efforts on leveraging internal, custom metrics and also public ones such as NIST to identify areas where they could improve.

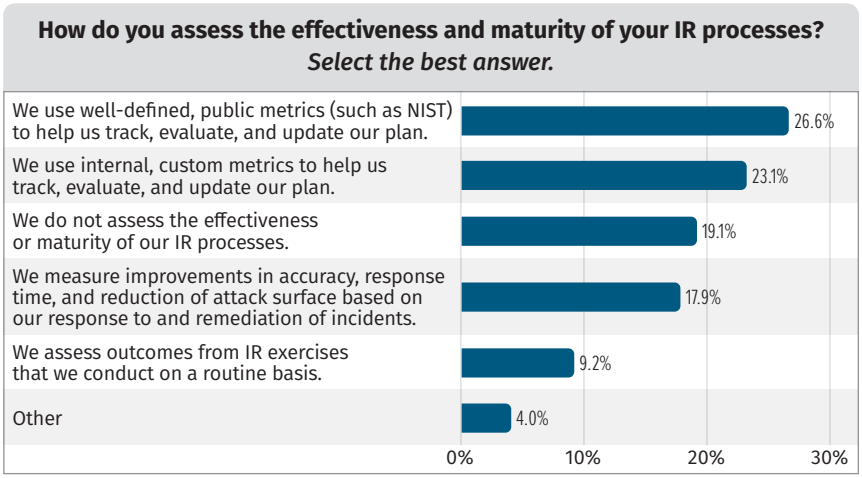

Figure 10. Assessing the Effectiveness and Maturity of IR Processes

Even when organizations find ways to improve, there are impediments to implementing these changes and increasing the effectiveness of an IR program. The responses we received regarding the impediments organizations face show a different picture from what we saw in 2019. Although lack of budget remained one of the top challenges organizations face, staff shortages as well as poorly defined processes were less of an issue. We did, however, see an increase in responses pointing out challenges in other areas. For example, various issues tied to dealing with diverse technology stacks (such as IoT, cloud, and OT) were highlighted by more respondents than in 2019. Additionally, respondents identified remediation as a struggle, with the ability to thoroughly remediate incidents and the time needed to respond to incidents as the primary challenges.

So, the question is, given assessments as well as known impediments, how are organizations planning to solve these challenges? In an attempt to uncover this, we asked organizations what improvements they have in mind for the next 12 months (see Figure 11). Interestingly, we saw a reduced number of improvements being focused on compared to what was reported in 2019. This could be because those planned improvements from 2019 were implemented and therefore no longer required (although the data cannot prove that theory). Most notably, the intent to hire additional staff as well as improvements related to automation remained steady among the drop in other focus areas.

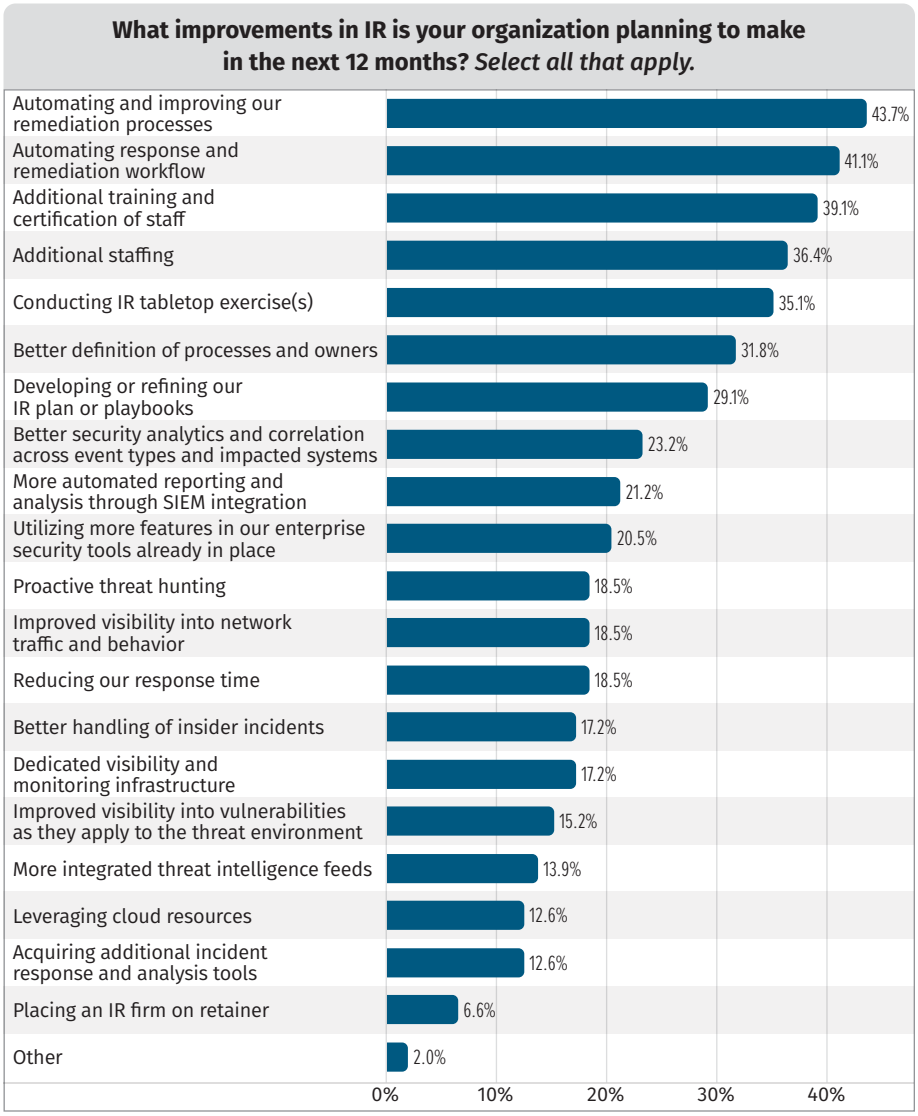

Figure 11. IR Improvements Planned in the Next 12 Months

When asked about the biggest hurdles preventing organizations from implementing automation, the differences in responses from 2019 show that some challenges have been resolved while others remain. Time and resources, budget, and IR process maturity all received a lower percentage of respondents, indicating these as being hurdles as compared to 2019. The only challenge that became more prevalent was the maturity of the security orchestration, automation, and response (SOAR) marketplace (see Figure 12). This may indicate that organizations have moved beyond internal challenges only to find that the marketplace does not offer the solutions they think will suit their organizational needs. For this to change, the marketplace, rather than organizations, will need to evolve. With a heavier focus on automation and increasing capabilities in security technology, the hope is that the marketplace will adapt over the coming years to fill this gap. Overall, the biggest challenges organizations are facing were similarly ranked based on percentage of responses as compared to 2019.

Automation is currently being considered as a way to make IR teams more efficient and help solve the talent gap. What do you consider the major hurdles your organization must overcome before automation can be adopted? *Select all that apply.*

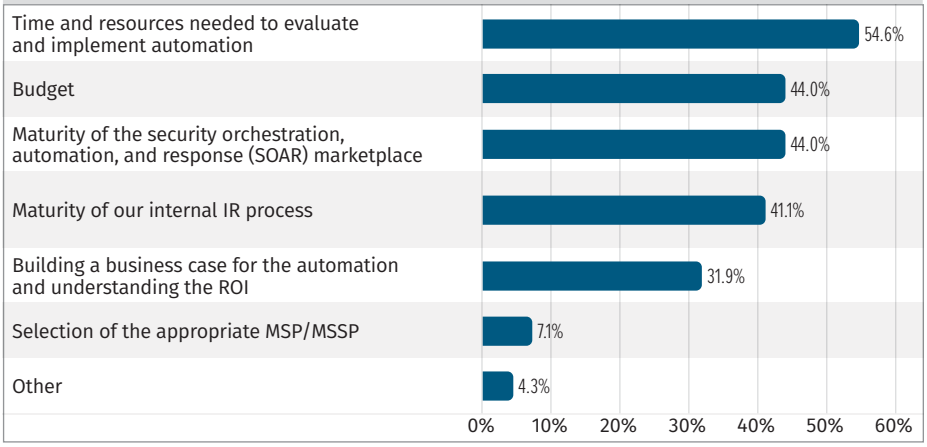

Figure 12. Hurdles to Automation Adoption

Conclusion

The 2023 Incident Response Survey provides a thorough and informative view of the ongoing evolution within the cybersecurity landscape. The data shows significant progress while also highlighting opportunities for further advancements, especially in the face of persistent and evolving threats.

When examining the sources of compromise over the years, we've noted certain categories experiencing growth. Specifically, business email compromise has emerged as a leading source of compromise, at a reported rate of 42%. This development aligns with the known vulnerability of email as a primary target for phishing exploits. Comparatively, the combined percentage of malware infections and ransomware, which separately were not an option in the 2019 survey, accounted for 55% of compromises this year. The distinct emergence of ransomware, at a 20% reported rate, reflects the rising threat it presents, requiring organizations to reevaluate and prioritize their responses to malware impacts.

Progress in incident response is apparent in both the containment and remediation phases, with better incident detection and quicker response times. Despite organizations' determined efforts to streamline IR processes, the data signals the importance of continued vigilance, especially with repeated instances of similar TTPs from returning threat actors.

Evidence acquisition and malware analysis capabilities demonstrate an imperative for a more robust integration of SIEM and EDR capabilities, as well as the utilization of leading evidence types for incident handling. With the trend toward third-party services for malware analysis, the need for external expertise in an increasingly complex threat environment is clear. However, organizations still have the opportunity to fully leverage these capabilities to their fullest potential.

Assessments of IR processes have followed a positive trajectory, with fewer organizations neglecting to conduct them. Nonetheless, the survey also revealed various impediments to improving IR programs, such as the challenges of diverse technology stacks and effective remediation. The dynamic nature of cybersecurity underscores the critical importance of adaptability and flexibility, even as organizations have made strides in addressing these internal challenges.

Organizations continue to express a strong interest in improvements, particularly in automation and staff augmentation. However, the reduction in the total number of overall planned improvements suggests the need to overcome external hurdles, notably concerning the maturity of the SOAR marketplace. For organizations to progress further, the market must evolve to provide the necessary solutions. From a staff augmentation perspective, organizations need to take the lessons learned from their own organization as well as observations from this survey to understand how to attract talent in the industry and retain that talent.

In essence, the 2023 Incident Response Survey highlights the progress made and the challenges that still lie ahead. We can take pride in the advancements accomplished, but we must not rest on our laurels. As the cybersecurity landscape ceaselessly evolves, we too must persist in our efforts. The lessons learned from past incidents and the insights gleaned from this survey will undoubtedly guide us toward a more secure future. By integrating advanced tools, improving our evidence acquisition, continuously assessing our processes, and embracing automation, we will continue to enhance our resilience against an ever-changing spectrum of cyber threats.

Sponsor

SANS would like to thank this survey's sponsor: