The State of Incident Response 2017

Research conducted by VIB

SPONSORED BY DEMISTO

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Over the past few years, the number of incidents which cybersecurity professionals must respond to has increased dramatically. The challenge of responding to the increased threat level has left many organizations struggling to find the personnel and tools to keep their systems secure. As a result, many organizations struggle to achieve success in blocking attacks or responding to incidents within an acceptable time. Manually executed response plans, disjointed management of the response procedures, and a lack of an effective means of collaborating between affected parties have led to many serious, costly breaches that could have been easily contained.

Demisto recently sponsored an independent, third-party survey conducted with security professionals around the world working for companies ranging from less than **500 employees** to greater than **20,000 employees**. More than **200 responses** were analyzed. The purpose of the survey was to discover challenges faced by incident response teams and how they are addressing them (or not) currently. This is the first industry study to span and cover all aspects of incident response, including SOC location, training issues, tools utilization, and what metrics are being tracked.

The survey revealed new data that companies are struggling to keep up due to lack of resources, both on the security tools side and personnel side. For example, more than **40 percent** of respondents said their organizations are not prepared to measure incident response, **and only 14.5 percent of respondents are measuring MTTR (Mean Time To Respond)**. The study also discovered that while organizations are hit with an average of nearly **350 incidents** per week, **30 percent** of respondents reported that they have no playbooks, runbooks or other documentation for incident response actions.

The survey also validated the known security staff shortage issues, with some new findings. More than **90 percent** of the respondents indicated that they feel the pain of finding experienced employees with the necessary skill sets. The survey found it takes an average of **9 months** from the initiation of a hiring requisition until the new hire is fully trained. Since the need is frequently identified long before the hiring process officially begins, companies are without a resource – from the point where a need is identified until the point they have fully trained analysts – for almost a year. To make matters worse, more than one-third of the staff leaves within **3 years**. The knowledge and experience acquired by these employees during their time with the company goes out the door with them.

The survey also confirmed with new information another major challenge that companies face – the sheer volume of alerts and the inability to prioritize them. According to respondents, **40.4 percent** feel that there are significantly more alerts than can be handled by their staff, while **47.4 percent** report it is hard to know which alerts to prioritize. The survey also discovered that **52.7 percent** are in constant fire-fighting mode and are unable to keep their processes and playbooks updated, making them more vulnerable to future threats.

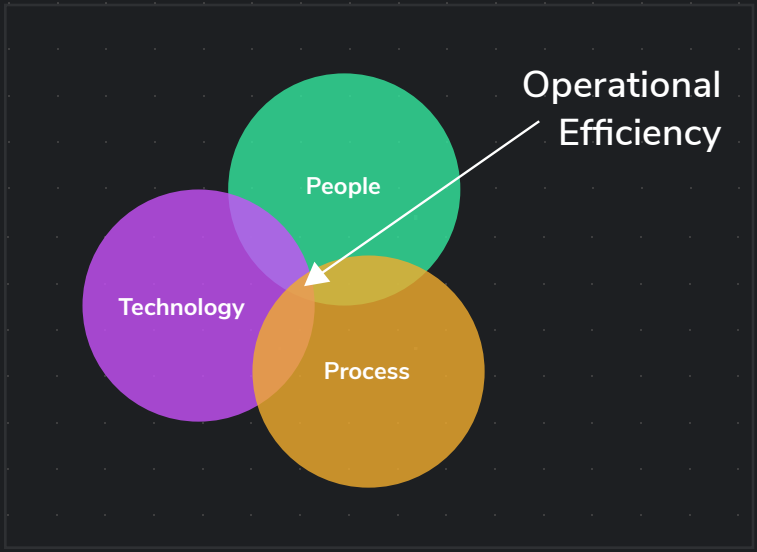
When asked about the areas where automation can help, 54 percent of respondents asserted that security operations and incident response are the two top priorities for them at this time. The survey results revealed that organizations need a new security operations approach combining effective incident management, security orchestration and collaborative investigation. To ensure that the time of experienced and skilled analysts is effectively utilized and that their knowledge and experience don't walk out the door with them, organizations need the ability to perform collaborative, interactive investigations to scale the incident response function effectively within a security operations center.

1. INTRODUCTION

Threats have evolved over the years. Hackers today are more likely to have expert skills and be part of a well-funded, organized group, rather than individuals hacking a specific target from the confines of their basement or den. Attacks have become increasingly sophisticated and complex, hackers have become more patient, damages have become more expensive to re-mediate, and attacks can persist over several months or even years.

Incident response continues to evolve to meet the current and emerging threats. It is no longer enough to wait until an incident occurs to determine how to respond. Cybersecurity professionals must plan for an attack without knowing when it will occur, how it will be initiated or what the hacker's goal maybe. Furthermore, they must be proactive about educating users, conducting post-incident forensics, and ensuring compliance with all mandatory regulations.

The key to effective incident response is having the right combination of people, technology and processes. However, this study revealed that many organizations are far from having this right combination. For example, when asked how many people in the respondents' organizations were dedicated solely to incident response, 17.6 percent responded that there were none and 22.3 percent stated that there were only one or two.



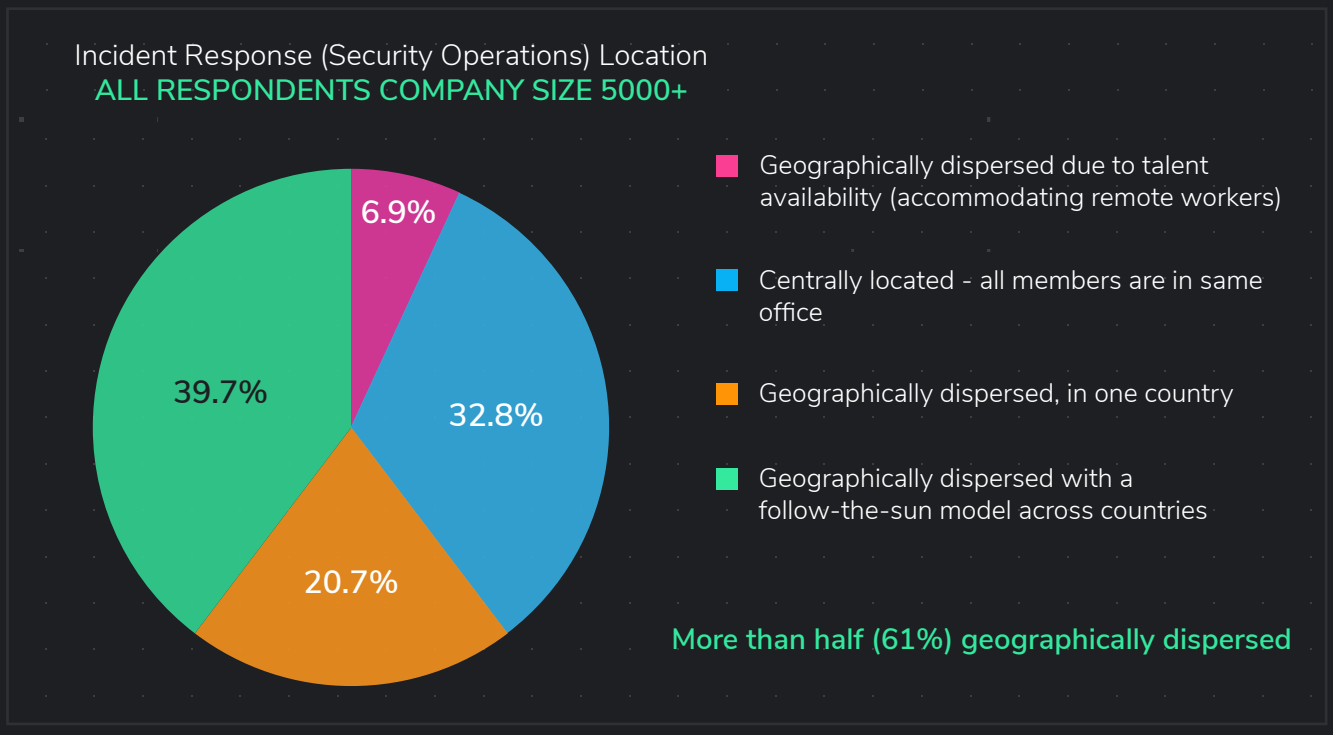
Approximately 49 percent of respondents reported that their processes and playbooks were not automated; some still rely on fillable forms, manual processes or checklists.

Without the effective utilization of technology, processes and people, operational efficiency will be compromised. When asked about the number of incidents occurring weekly, respondents reported dealing with an average of 346.42 incidents per week — and requiring an average of 2.28 days to resolve an incident. Clearly, this study confirms there is still a great deal of work to be done to harness the power of combining technology, people and processes.

2. THE STATE OF SECURITY OPERATIONS CENTER: THE INCIDENT RESPONSE FUNCTION

SOC LOCATION: INCIDENT RESPONSE FUNCTION

Where the incident response team is located can affect operational efficiency. According to our survey, **56.4 percent** of the respondents reported that all staff members involved in incident response were located in the same office. Approximately **19 percent** stated that the team was geographically dispersed within the same country, but **18.6 percent** reported that the team was geographically dispersed across the globe and used a "follow-the-sun" model. Only **5.9 percent** reported that the geographical dispersal was based on the need to accommodate remote workers due to the availability of talent. When this data is broken down further, it reveals that the **problem is worse for larger companies with employee count of 5000 or higher-more than half (61 percent) of larger companies are geographically dispersed.**



The primary problem presented by an incident response team that is geographically dispersed is that it hinders collaborative efforts. With so many tools available for instant communications, it might seem odd that geographic separation can be an issue. However, there are several underlying factors that demonstrate the problems that can arise when all team members are not in the same location.

The first issue is that mutual knowledge suffers from separation. Team members may begin with the same basic knowledge, but mutual knowledge also involves an awareness that other team members have the same information. This allows team members to communicate more effectively because they have shared experiences and stand on common ground. When an incident occurs, dispersed team members may find collaboration difficult due to a lack of knowledge concerning what other members might not know. Technology can complicate matters; emails, phone calls and text messages lack the nuances that are present in face-to-face meetings. Nuances can be particularly important if team members are from different cultures or have different native languages.

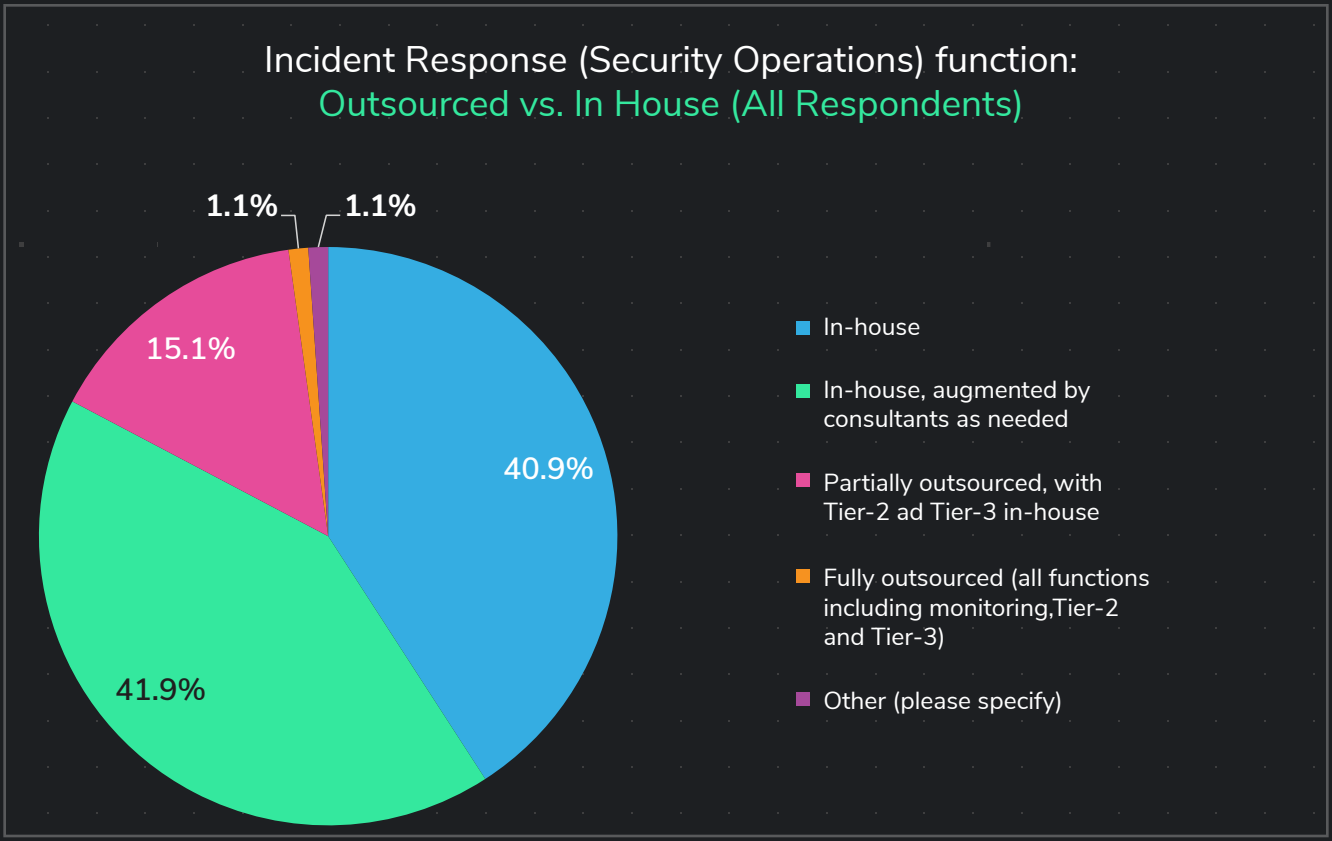
Dispersal can also affect working relationships. Team members at remote locations can feel emotionally isolated from their colleagues and begin to view the team in terms of "we" and "they." Remote workers may not feel that they are truly part of the team and be resentful when "they" attempt to collaborate or take ownership of the incident.

In addition, having the team geographically dispersed decreases the likelihood that all team members are "on the same page." Members working at remote locations often have different information, but they are frequently unaware of any discrepancy. Discrepancies may result from an update to the response plan that was not transmitted to all team members, an overlooked electronic communication, or a lack of feedback from or to the remote workers.

Solving the challenges of dispersed teams requires a bit of effort and creativity. The most effective way to communicate and collaborate is face-to-face. This is followed by video chats and audio communications. The least effective method is the written word. Employing all methods can help ensure that any gaps have been bridged, resulting in a stronger team.

SOC FUNCTION: OUTSOURCED VS. IN HOUSE

When asked whether their organizations had an in-house SOC, outsourced operations or used a combination method, only **1.1 percent** of respondents reported that they had completely outsourced all SOC functions. Almost **41 percent** stated that they handled all functions in-house, while **41.9 percent** reported that they augmented their in-house operations with consultants on an as-needed basis. Just more than **15 percent** outsourced certain functions while keeping others in-house.



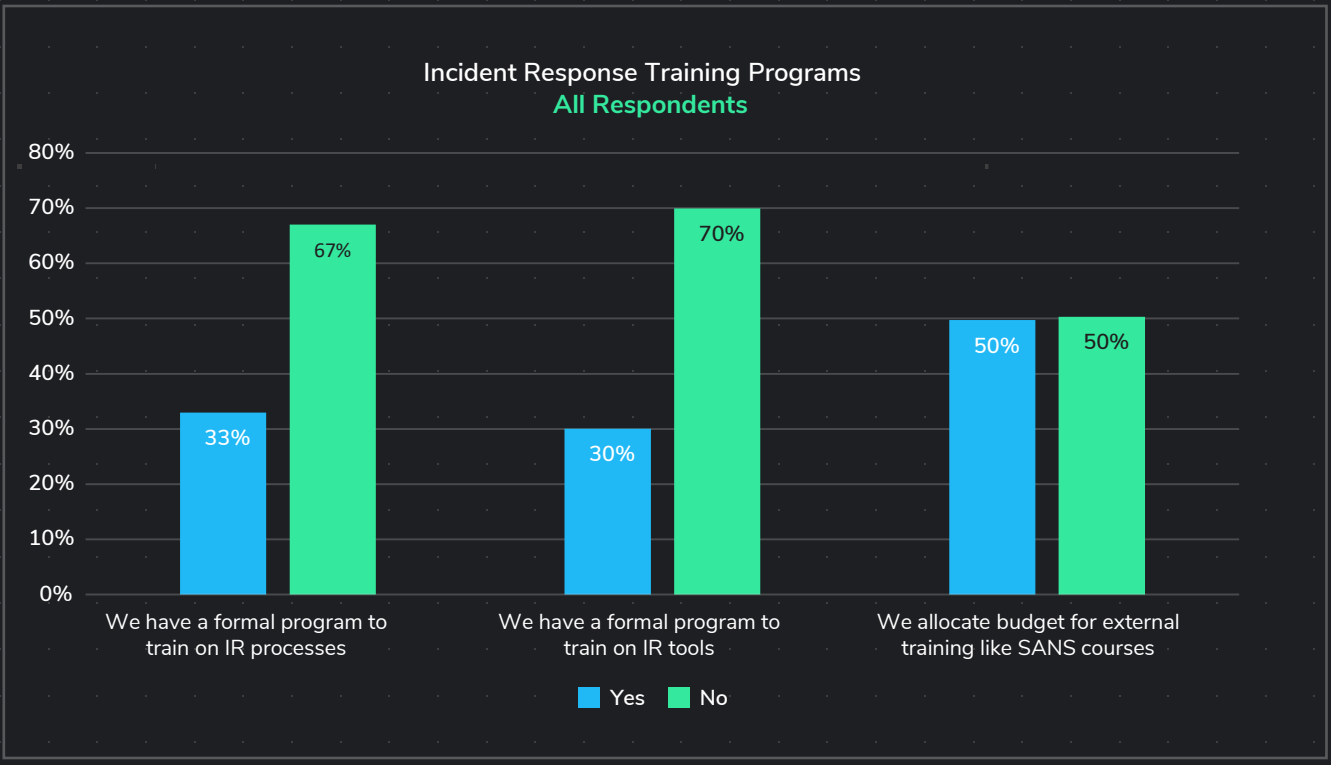
Advantages and disadvantages exist for outsourced as well as in-house SOCs. Creating an in-house SOC can be costly and time-consuming, talent may not be available, and it can be a challenge to acquire the various data needed. On the other hand, in-house analysts have the knowledge and perspective to truly understand what they are trying to defend. This knowledge may enable in-house analysts to handle triage and prioritization more efficiently.

Outsourcing can be a viable option for many companies. Vendors specializing in cybersecurity recruit trained analysts with top-notch skills. They can often deliver results faster than in-house analysts and are typically more up-to-date on threats lurking in cyberspace. However, an organization may not be able to have round-the-clock-access to analyses or data, and self-service functions may be limited.

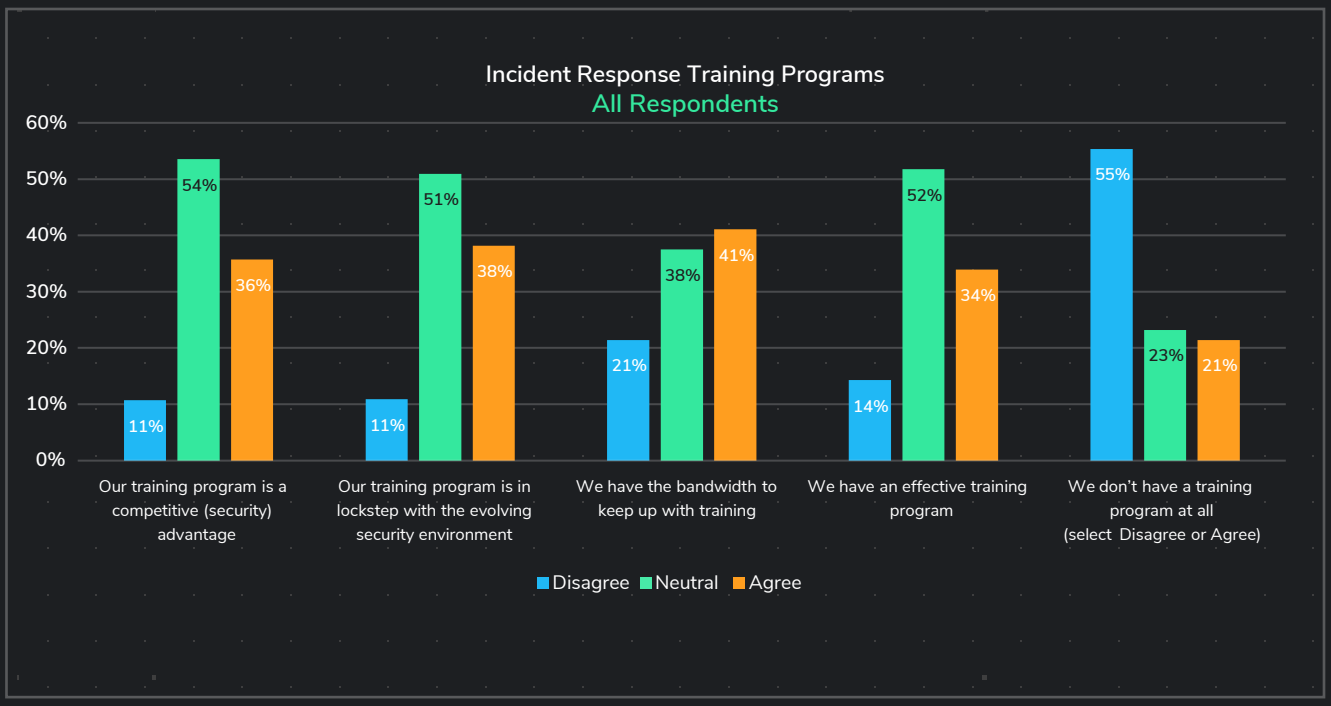
SOC TRAINING: INCIDENT RESPONSE TRAINING PROGRAMS

Adequate training is a critical part of an effective response to incidents. However, although the survey revealed that many organizations are taking steps to ensure that all employees are properly trained, the results indicated that there is significant room for improvement.

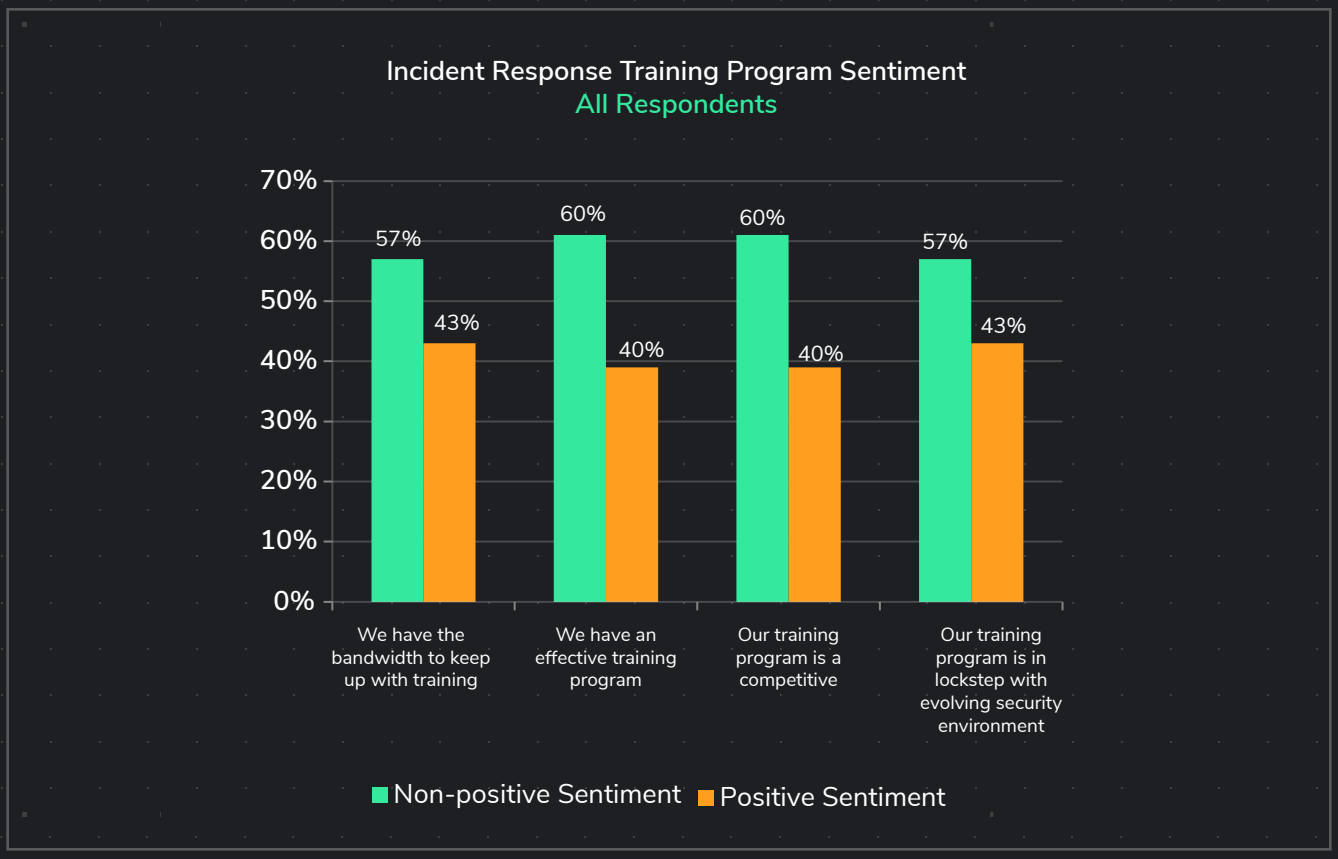
Of all the respondents, only approximately 33 percent stated that their organizations had a formal training program for incident response processes, while 70 percent reported lacking having a formal training program for incident response tools.



Almost 50 percent of all respondents indicated that their company allocated funds for external training. However, only fewer than 36 percent of all respondents agreed that their training programs gave them a competitive advantage, were in step with the evolution of security, and were effective; and only approximately the same number indicated that they had the bandwidth to stay current with training. Almost a quarter of the survey respondents stated that their organizations did not have any type of training program for incident response processes.



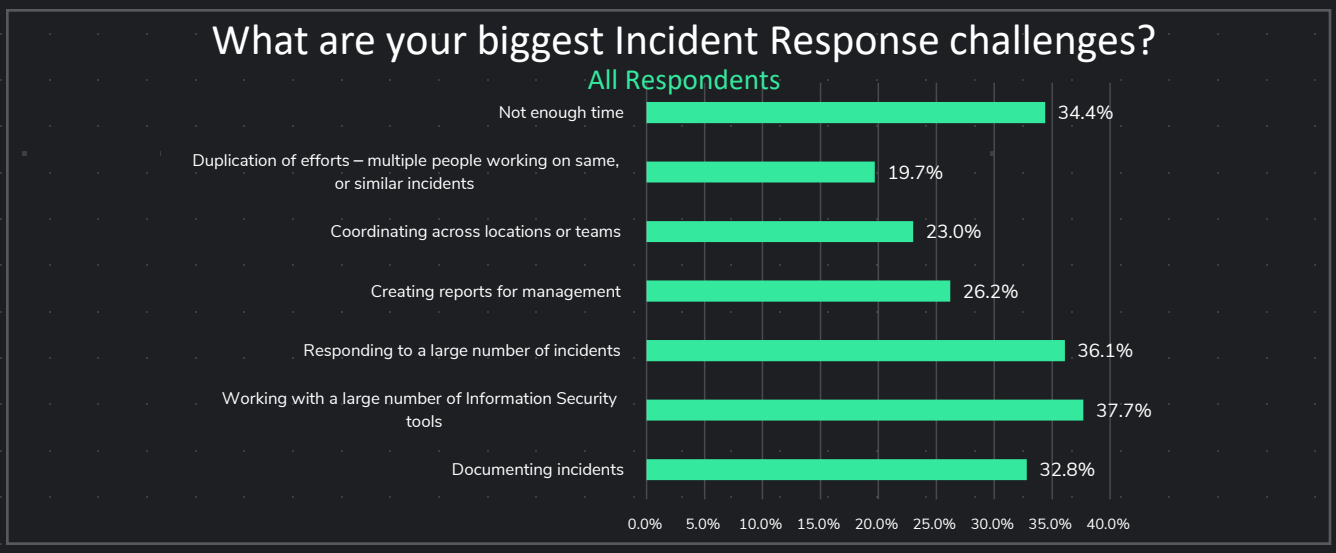
When asked further about the training programs in place at their organizations, a significant majority of respondents indicated that they do not have a positive feeling about their Incident Response training program.



SOC CHALLENGES: INCIDENT RESPONSE CHALLENGES

Investigation time is inversely related to tool availability and capability. Automated tasks can be done manually (slowly and with higher opportunity for missteps). Incident volume isn't fixed so IR is almost always a prioritized "top of stack" approach meaning other incidents, observations wait for investigation.

- Anonymous Survey Respondent



Not surprisingly, most respondents reported a wide range of challenges that they faced when responding to incidents. **"Not enough time" and "Responding to large number of incidents" as responses received high percentages as expected. But surprisingly the #1 challenge identified by respondents was "Working with large number of IS tools."** When asked to break it down based on the severity of the challenge, the response data got more interesting.

More than 83 percent claimed that insufficient staffing was “fairly” or “very” challenging, while approximately 86 percent gave the same ratings to not having enough time. Almost 69 percent reported that it was fairly or very challenging to capture and analyze information from individual analysts and teams, but more than 83 percent reported that it was challenging to improve processes and/or results. Interestingly, 52.6 percent of the respondents stated that it was not too challenging to track and assign incidents. When it came to reporting up the chain of command, more than 50 percent stated that it was not too challenging, 13 percent found it very challenging, and the rest considered it fairly challenging.

SOC PARTNERSHIPS: INCIDENT RESPONSE TEAM AND OTHER IT DEPARTMENTS

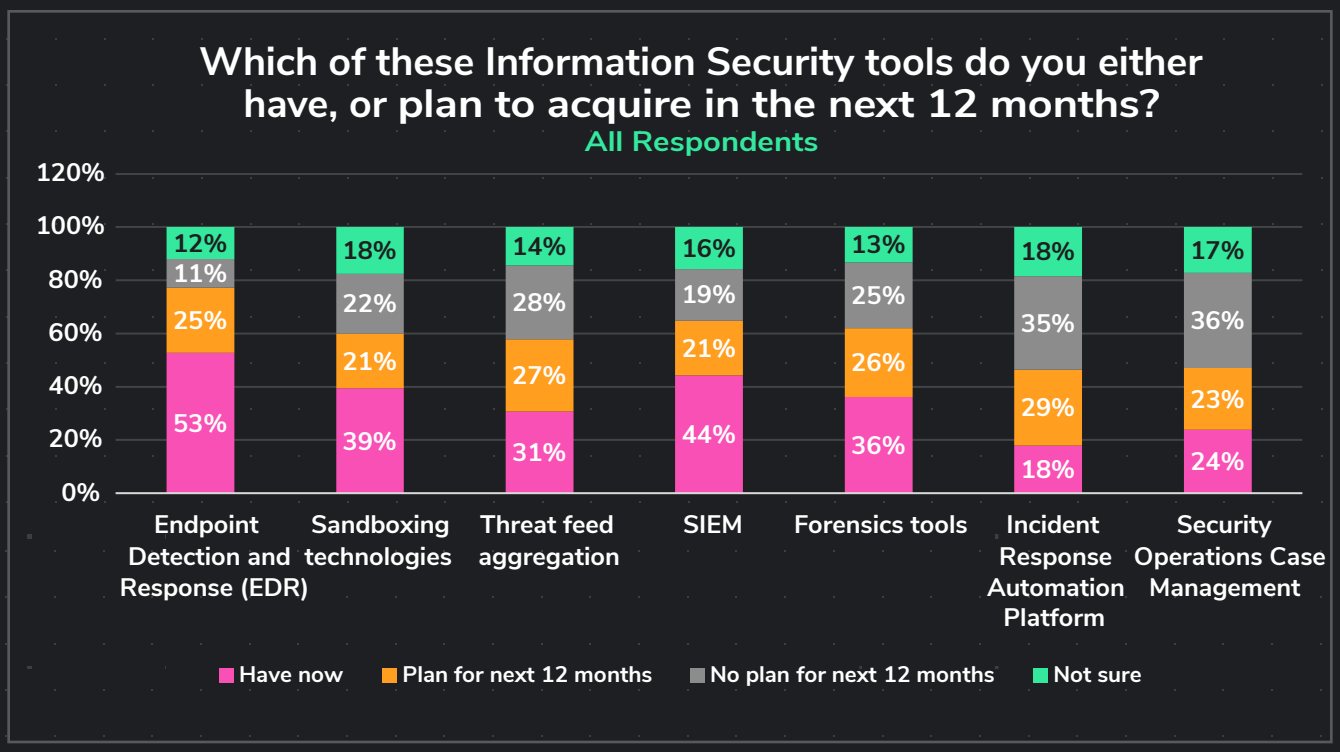
Difficulties encountered when attempting to collaborate or coordinate efforts, as well as data silos, can increase the time it takes to respond to alerts. When the SOC (security operations center) and NOC (network operations center) are integrated, the efficiency of the incident response team can be substantially enhanced. From the results of the survey, it can be determined that interdepartmental cooperation and coordination needs to be improved in many organizations. For example, when asked about their biggest challenges related to incident response, almost 20 percent cited duplication of efforts, while 23 percent stated that it was challenging to coordinate response across teams or locations.

> *We would like to have our existing offshore NOC be able to take on security incident response, but we lack the logging/alerting/monitoring infrastructure to make this effective.*
>
> - Anonymous Survey Respondent

When answering the question of which IR processes that respondents felt would be of immediate benefit, one participant stated that having the company’s offshore NOC take more responsibility for security would be helpful. Having the NOC handle containment during incident response would be one example of making good use of resources that are already capable of instigating network-wide operational changes.

SOC FOCUS: PREVENTION VS. RESPONSE

Preventing attackers from gaining access to the system is always better than repairing the damages that they cause. However, with new threats appearing daily, it is impossible to gain the intelligence needed to guard against every specific attack. In addition, many breaches go undetected for a substantial length of time. For all of these reasons, organizations are becoming more aware about the need to detect hidden threats that are already in their networks and have increased their efforts to collect threat intelligence. Unfortunately, many of the participants responding to the survey indicated that they lacked the right tools for the job.



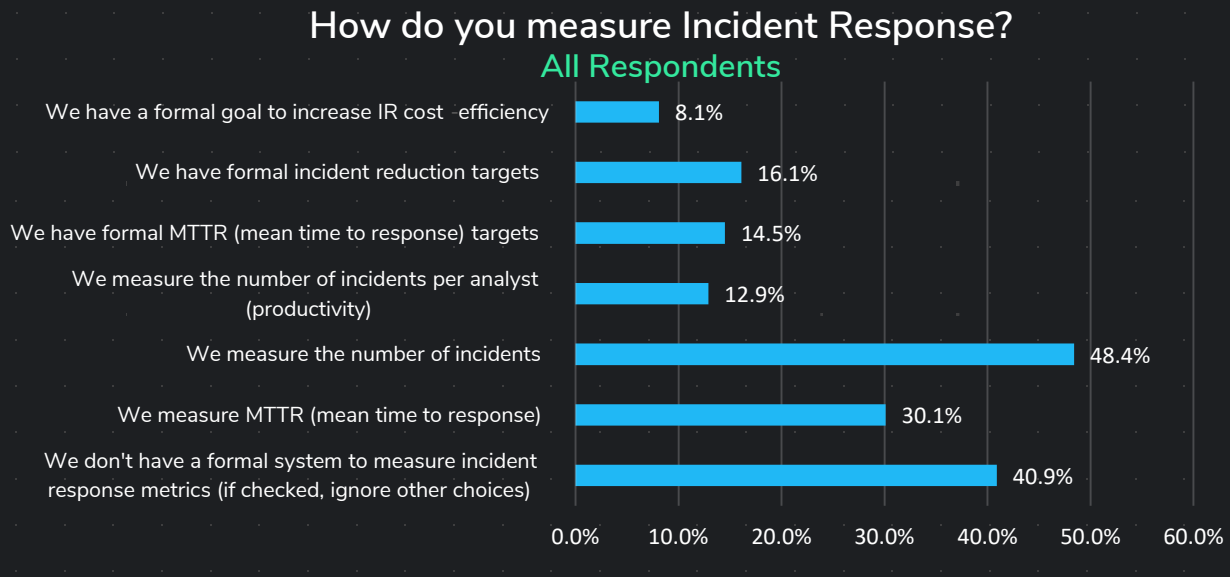
While nearly 70 percent reported that they currently had no tools for threat feed aggregation, nearly 28 percent stated that they had no plan to acquire such a tool during the next year. When asked about the time it had taken to implement threat feed aggregation tools, the average was 3.1 months for those who had completed implementation, but 46 percent of the respondents stated that they were “still trying” to complete the implementation after 12 months. (Refer to Section 5: The State of Incident Response Tools for more details)

When it came to threat hunting, the results were even more disappointing. Although 47.3 percent of the respondents believed that automating threat hunting would provide immediate benefits, barely 12 percent had actually automated their threat hunting.

SOC METRICS: MEASURING INCIDENT RESPONSE

> *We have a procedure to follow and review this quarterly with our team, but we do not measure this.*
>
> - Anonymous Survey Respondent

When asked how they measure incident response, survey participants indicated that there is a great deal of variance in how organizations accomplish this task. Approximately **41 percent** stated that they had no formal system for measuring incident response, while **48.4 percent** measured the number of incidents and **12.9 percent** measured the number of incidents per analyst. Slightly more than **30 percent** measured the mean time to response, but only **14.5 percent** had formal MTTR targets. Approximately **16.1 percent** had established formal targets for incident reduction, and **8.1 percent** had formal goals to increase the cost-efficiency of incident response efforts.



SOC BUDGET: WHAT ARE THEY SPENDING ON INCIDENT RESPONSE?

> *It's not a separate line item, just part of the overall budget.*
>
> - Anonymous Survey Respondent

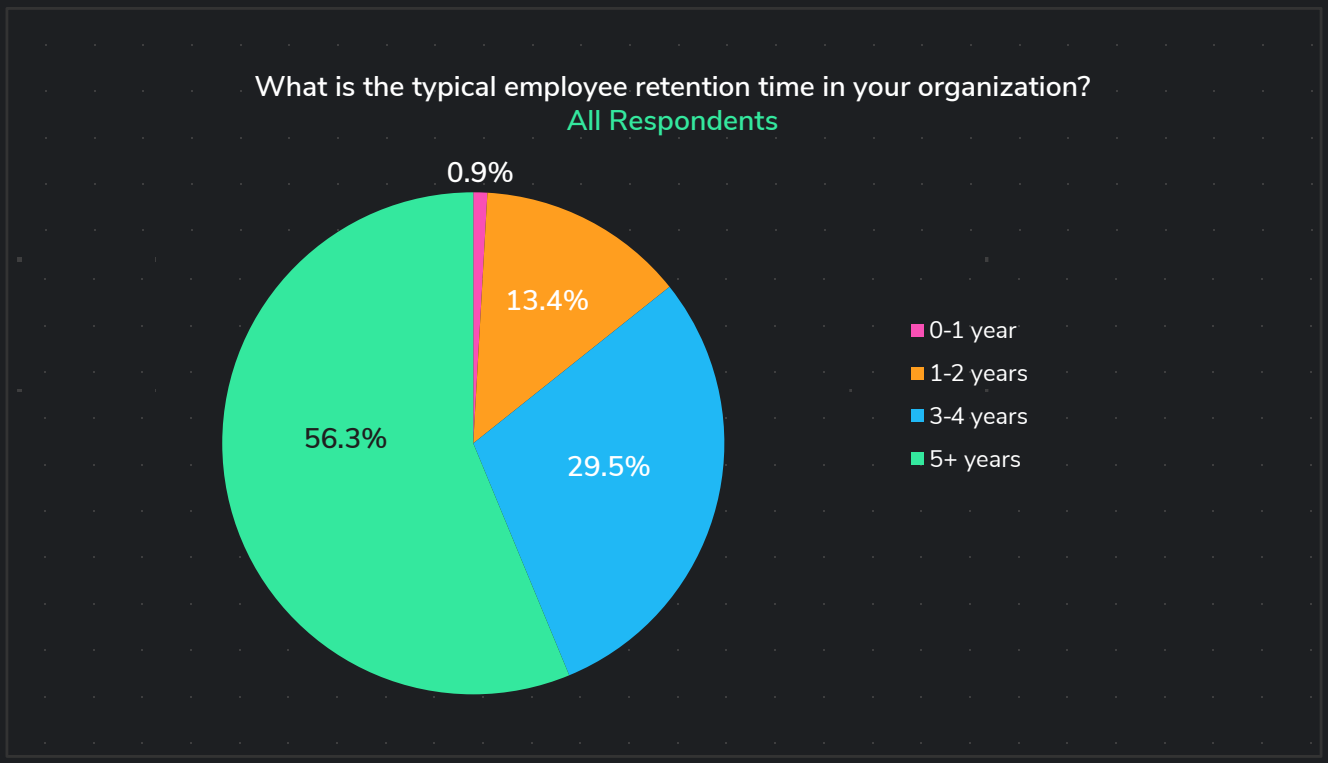
CISOs are still struggling to decide how to allocate available funds for security products. They face two primary issues. The first is a lack of visibility into the return on investment that each security product can provide. It can be difficult or impossible to determine whether products are being used effectively or providing the expected results. The second issue is the lack of historical data. Many organizations lack data on the types of attacks that they faced during the previous year or cannot identify trends to determine the types that the company will likely encounter in the future. However, according to the survey, approximately **43.5 percent** of the respondents stated that there is no separate budget for incident response. Of those reporting that they had a separate IR budget, **20.9 percent** stated that it was no more than **5 percent** of their total budget for information security; only **5.2 percent** estimated that the IR budget was more than **10 percent** of the total budget for information security.

These survey results indicated that a platform providing insight into all of the security products used by the organization is needed. A platform providing security automation and orchestration acts as a hub that has all security products plugged into it, offering the ability to build a security scorecard for the incident response function. This gives the CISO greater insight and helps them make informed decisions when it is time to allocate funds for various products.

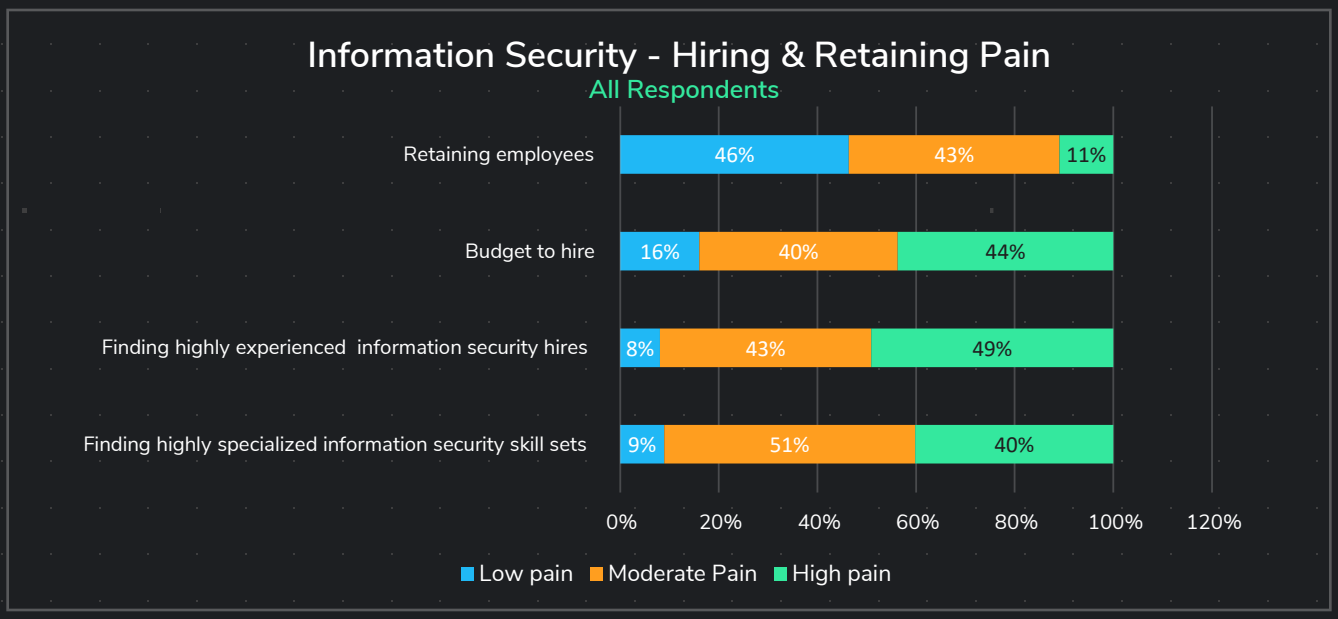
3. THE STATE OF INCIDENT RESPONSE TEAMS

EMPLOYEE HIRING, TRAINING AND RETENTION

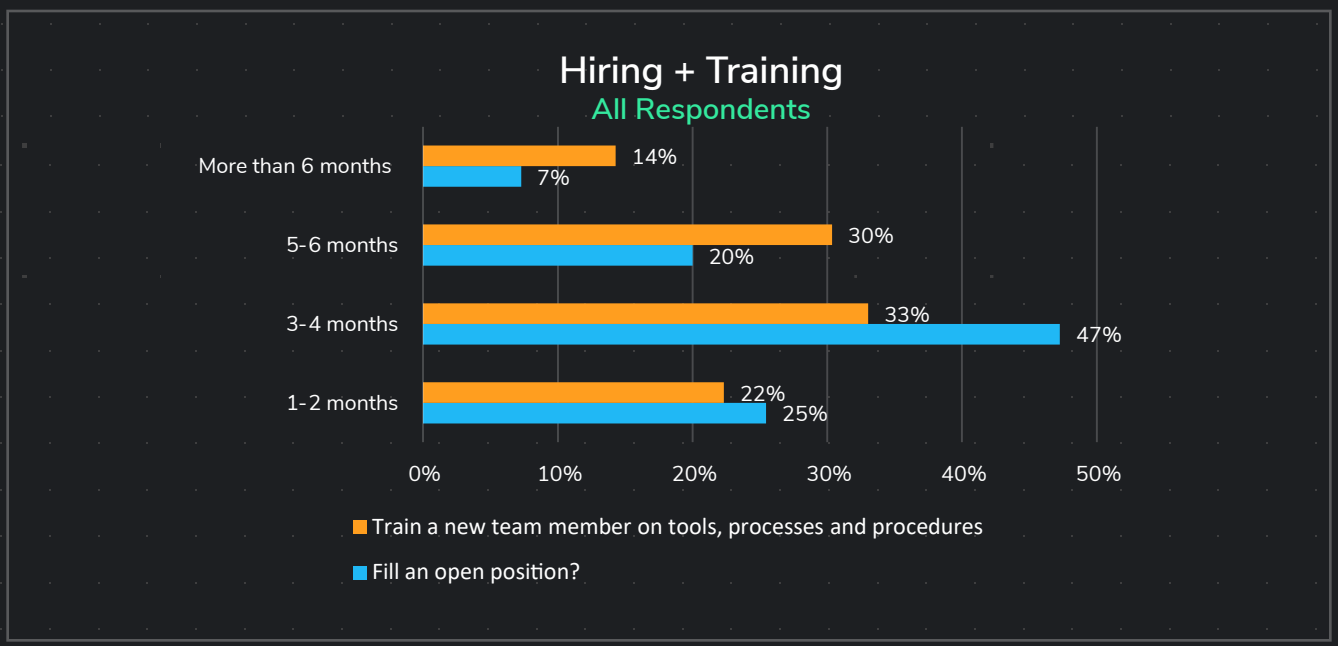
> *Corporate needs to care more about retention, or outsource the whole thing.*
>
> - Anonymous Survey Respondent



Finding and retaining talent remains a problem for most IR managers. According to our survey, only **56.3 percent** of the respondents reported a typical retention rate of at least five years. Approximately **29.5 percent** had a retention time of three to four years, but **14.3 percent** reported a retention time of less than two years.



When examining the time required to recruit and train a new employee, it becomes apparent that retention is critical to operational efficiency. More than **90 percent** of the respondents stated that they would categorize finding employees with the necessary skill sets and finding experienced candidates as moderate or high pain levels.



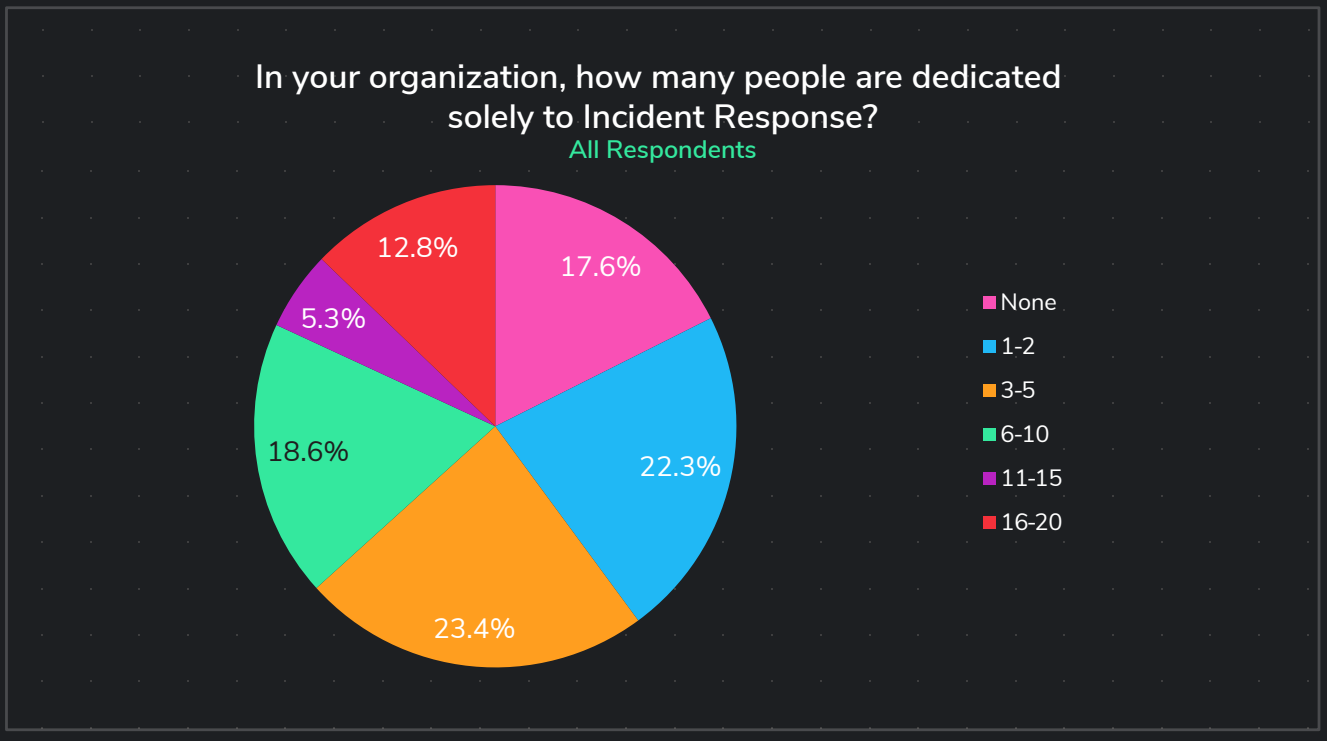
More than **47 percent** reported that it took between three and four months to fill an open position, **20 percent** needed between five and six months and more than **7 percent** stated that it took longer than six months. Since the need is frequently identified long before the hiring process officially begins, the pain of being short-staffed may begin much sooner. Therefore, the time between identifying the need and full actualization might be a good metric to establish.

*The weighted average was approximately **nine months** from the initiation of a hiring requisition until the new hire was fully trained.*

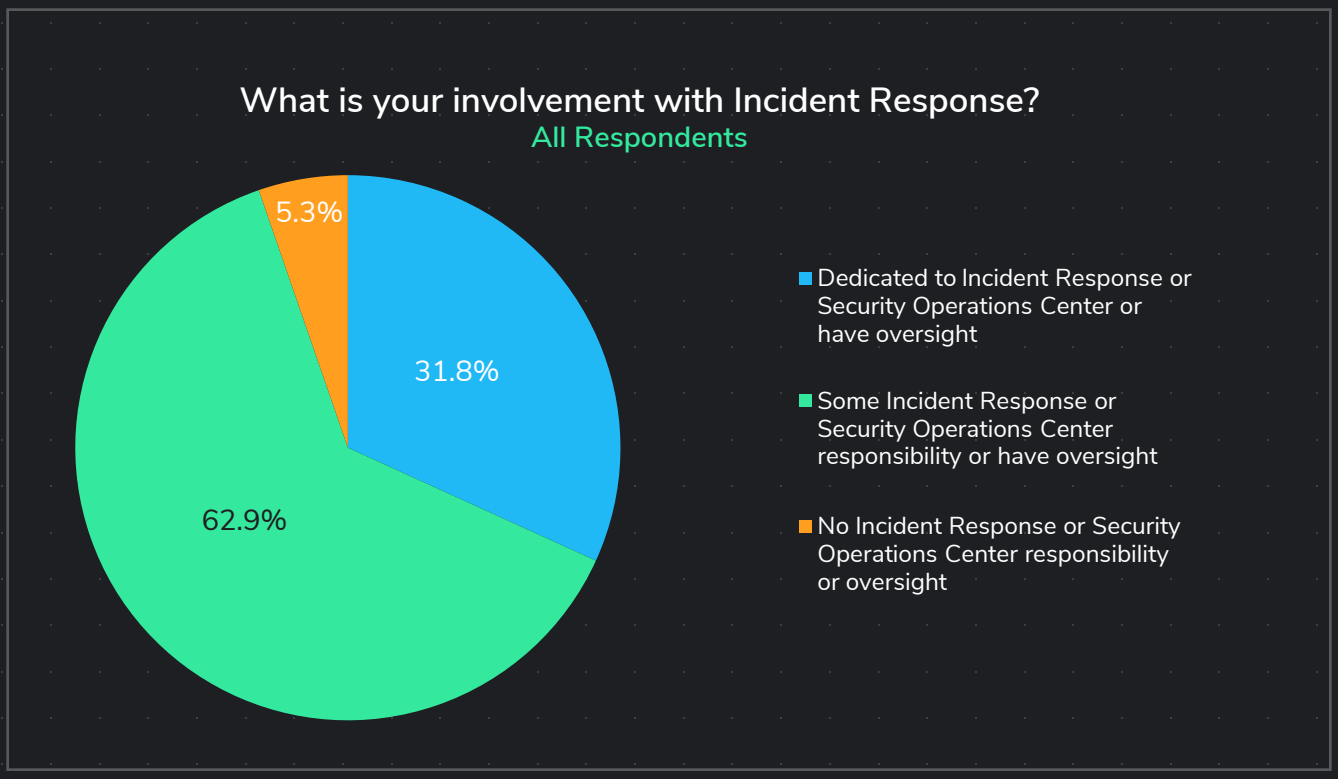
Approximately **14.3 percent** reported that it took more than six months to train a new hire, **30.3 percent** needed five to six months and **33 percent** stated that it took three to four months to train every new team member.

INCIDENT RESPONSE FUNCTION AND RESPONSIBILITY

A security operations center is responsible for more than just incident response. In some organizations, staff members are dedicated to IR, but in others, IR personnel perform a variety of other duties as well. According to the survey, **17.6 percent** have no staff members who handle only incident response, **45.7 percent** have fewer than five people dedicated to IR and **18.1 percent** have between **11 and 20 staff members** who are dedicated to IR.



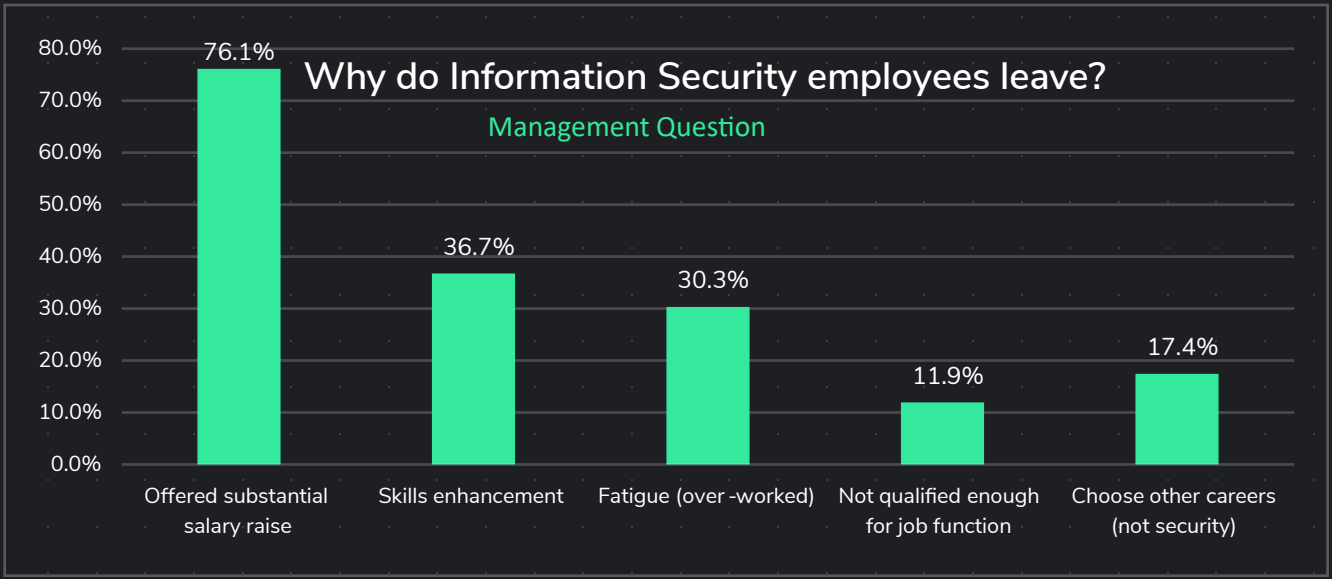
When asked about their involvement with incident response, **31.8 percent** of respondents stated that their duties were dedicated to the SOC or IR. However, **62.9 percent** reported that they had some responsibility for incident response or the security operations center, or that they had oversight of IR and/or the SOC.



TALENT ATTRITION: WHY EMPLOYEES LEAVE

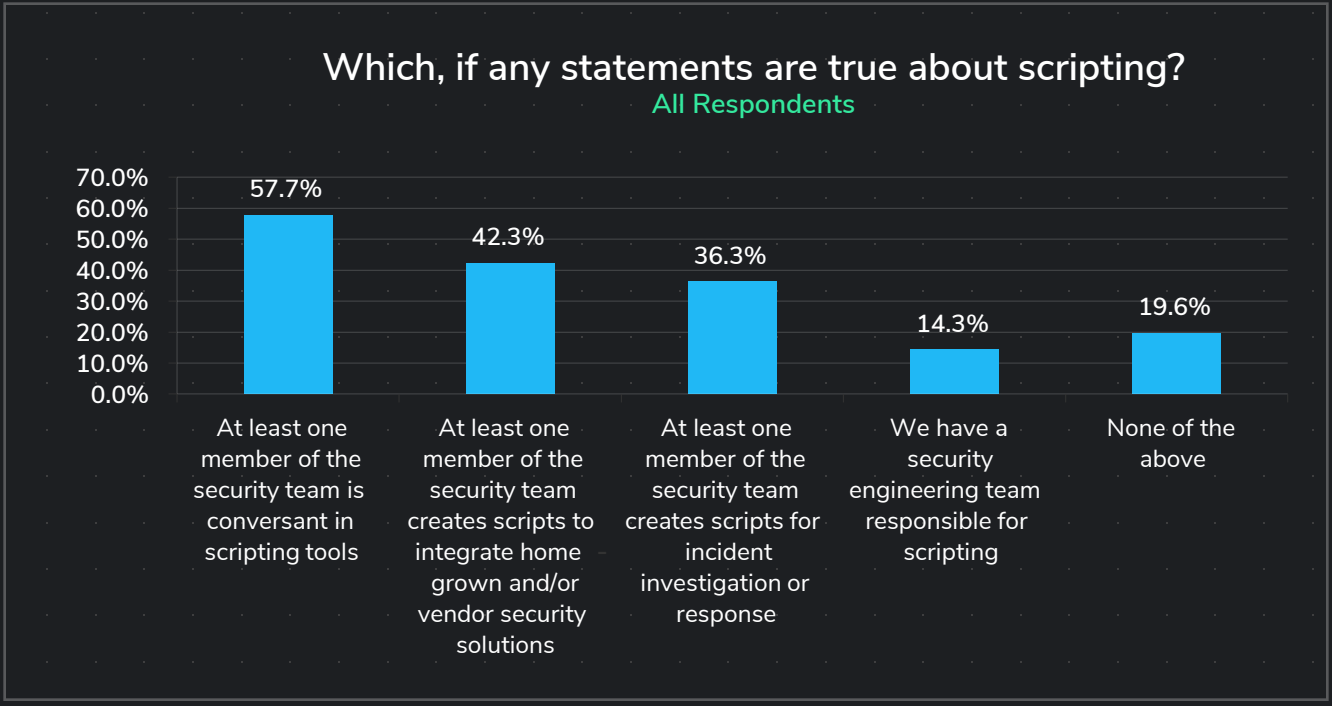
Management believes that employees leave because of Money. In reality they leave because of Fatigue.

When respondents who indicated they were in management were asked about the reasons that employees left their organizations, **76.1 percent** stated that their information security staff left to accept an offer that represented a substantial increase in salary. Approximately **36.7 reported** that the employees made a change to accept a position that would enhance their skills, and **30.3 percent** left due to fatigue caused by too much work. All three of these statistics point to the fact that managers think that retention can be expensive and that money plays an important role in increasing the retention rate significantly.



However, when security analysts were asked the same question, they indicated that the top reason why they leave is Fatigue.

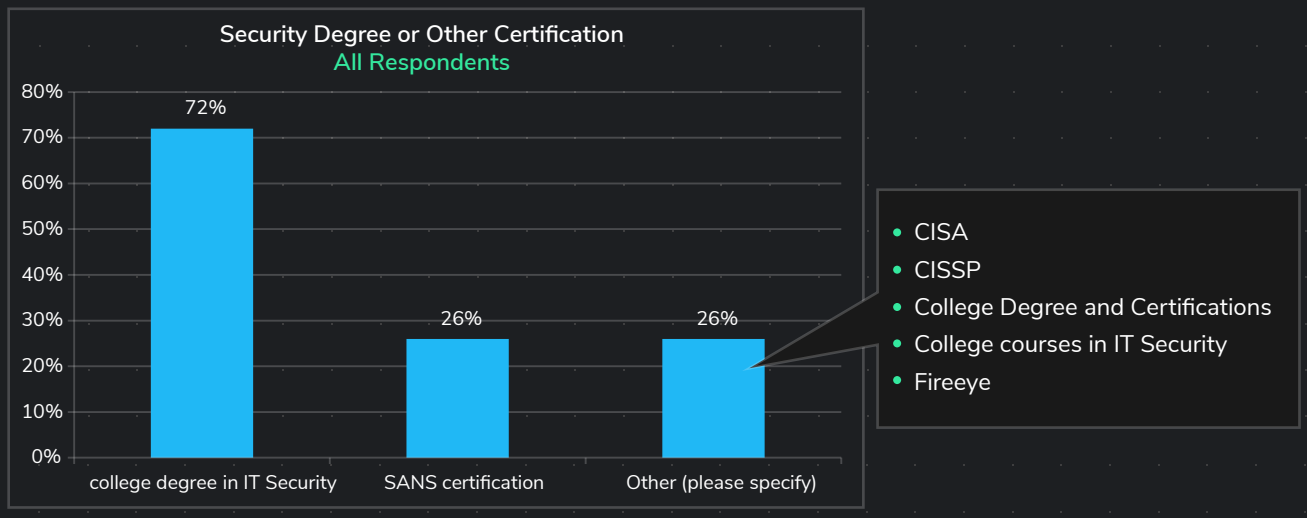
IR SKILLS: SCRIPTING CAPABILITIES



Scripting capabilities appear to need some improvement, according to the survey. More than **40 percent** reported that they had no security team member conversant in the scripting tools used.

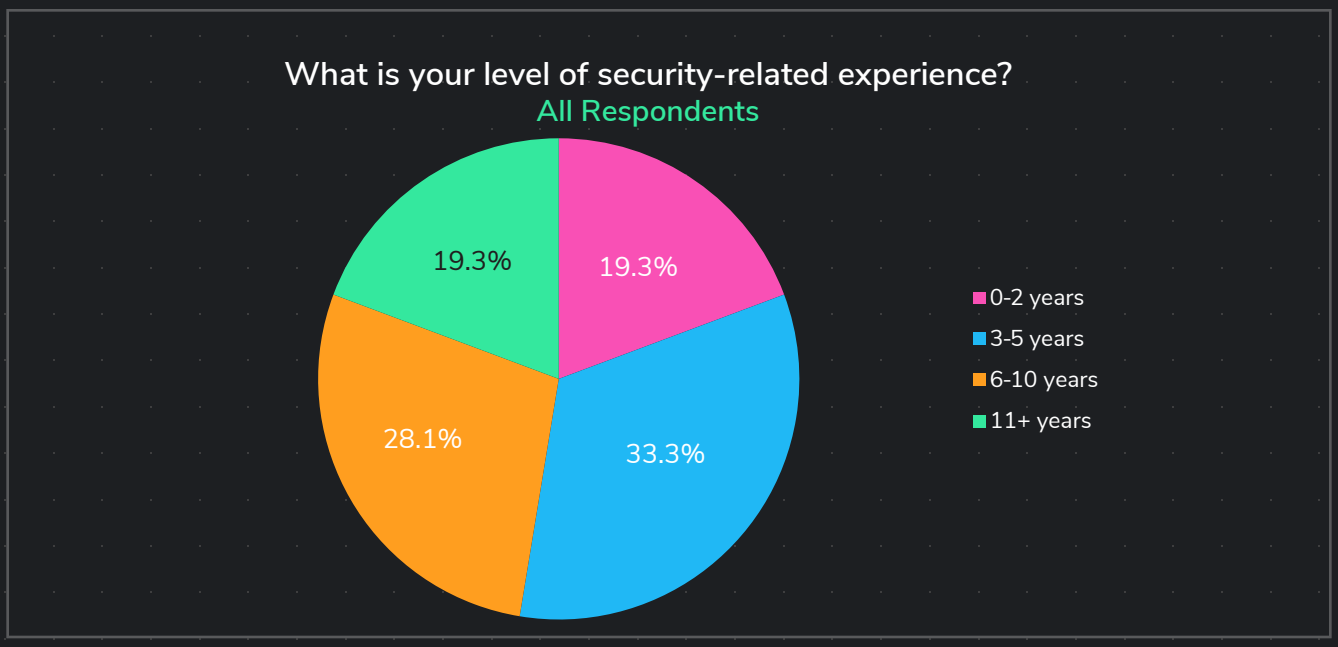
Slightly more than 42 percent stated that there was at least one team member who could create scripts to integrate vendor or home-grown security solutions, and 36.3 percent reported that at least one team member could create scripts for incident response or investigation. Approximately 14.3 percent stated that they had a security engineering team handling scripting responsibilities. However, 19.6 percent chose “none of the above” as their response. One respondent stated that all analysts were required to have scripting skills, while another respondent reported that scripting was handled by a third-party provider.

EDUCATION: SECURITY DEGREE OR OTHER CERTIFICATION

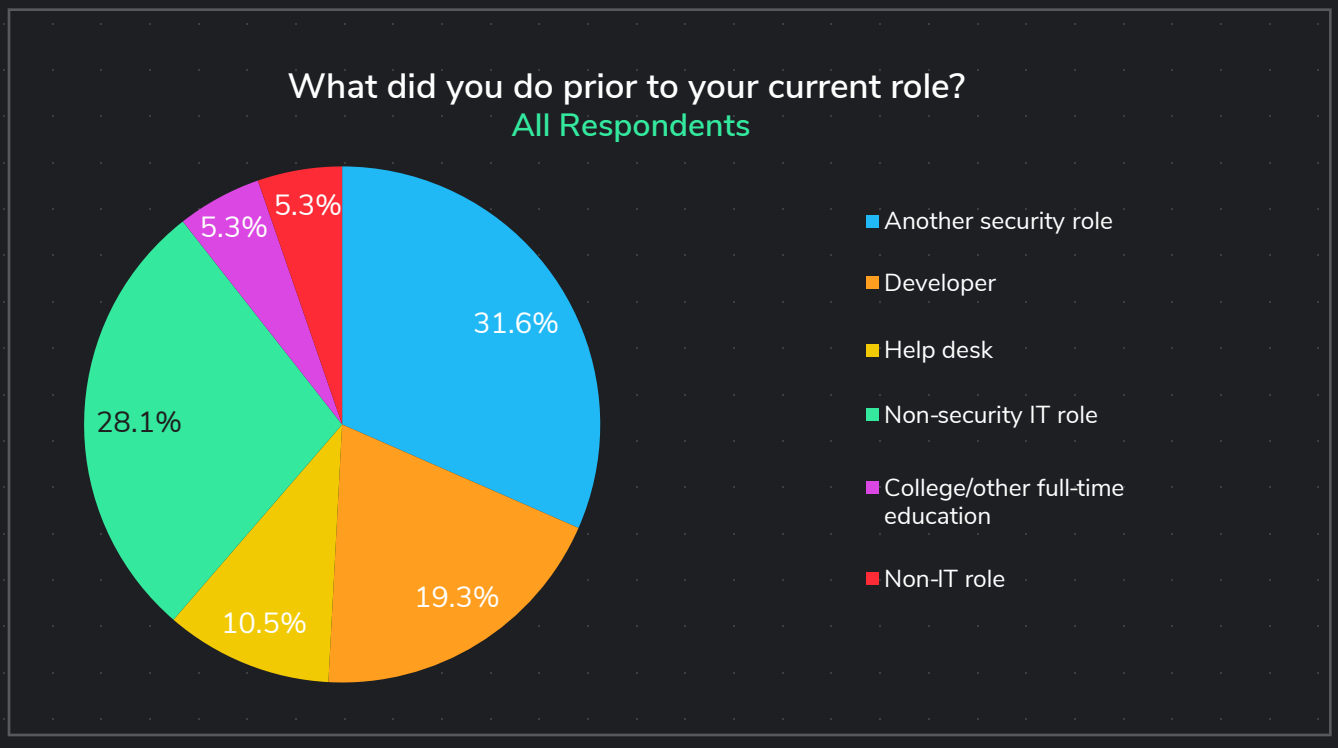


Cybersecurity team members appear to be increasingly well-educated. Approximately 72 percent of respondents stated that they had a college degree in IT security, and 26 percent reported that they held SANS certifications. Approximately 26 percent chose “Other” to report education and certifications. Among this category, some of the responses were college-level courses in IT security, unspecified engineering degrees, MBAs, CISA, CISSP, Fire Eye certified, CS and MIT.

SECURITY RELATED EXPERIENCE



The survey found that respondents had varying levels of security-related experience and represented a mix of relatively new workers and seasoned professionals. The same number — **19.3 percent** — reported having more than 11 years of experience as reported having less than 2 years of experience. Approximately **33 percent** had between 3 and 5 years of security-related experience, while **28.1 percent** had between 6 and 10 years.



When asked about their prior experience, **31.6 percent** stated that they had held a different security role, **28.1 percent** had performed a non-security IT function, **19.3 percent** were developers, and **10.5 percent** had previously held a position at a help desk. Approximately **5 percent** were hired immediately after completing college or other full-time educational pursuits, and the same number came to IR from a role not associated with IT.

4. STATE OF INCIDENT RESPONSE PROCESSES

The survey indicated that many organizations are struggling with all three elements of incident response – people, processes and technology – but when it came to processes, some companies are struggling more than others. Although the terms procedure and process are often used interchangeably, there is an important difference. An incident response process encompasses a collection of procedures that are focused on the identification and investigation of, and response to, potential security incidents in a manner that will minimize the impact to the organization and help expedite recovery from the incident. In concise terms, procedures are the tactics used, but the process is the complete life cycle of the incident. From the survey, it can be inferred that there is still some confusion about the terms and a lingering tendency to view incident response as a security or IT process rather than a business process aimed at helping the company achieve its goals, including retaining loyal customers, increasing profitability and growing its market share.

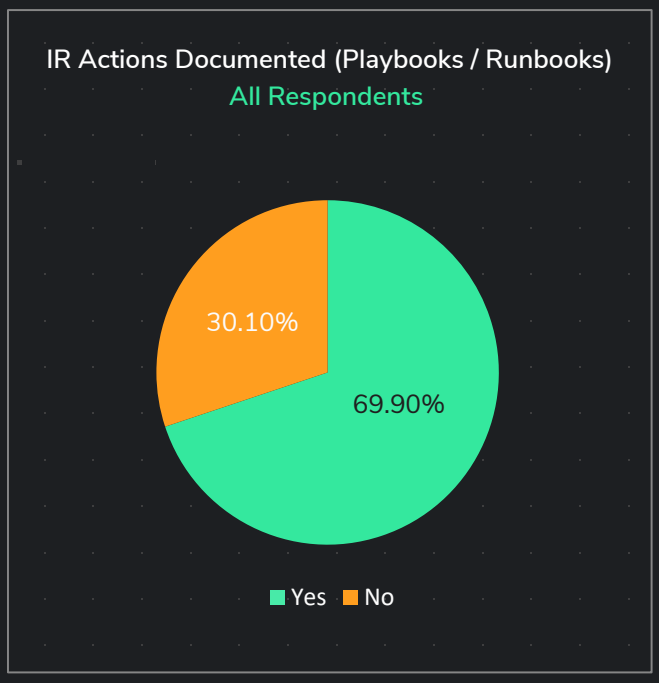
PROCESS DEFINITION: ARE PROCESSES WELL DEFINED?

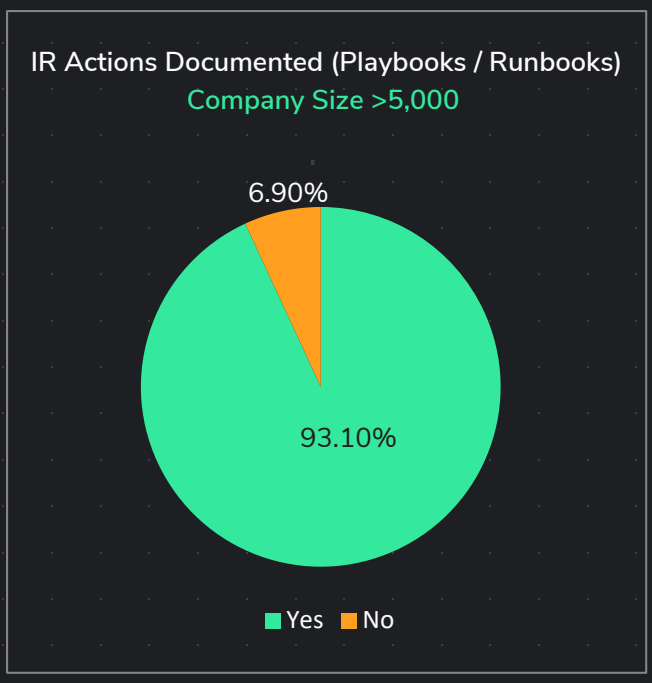
An organization's incident response process may include checklists, runbooks, playbooks or other documentation that detail the actions that should be taken from the time that an anomalous behavior is detected until the forensic investigation has been completed. The process for responding to a phishing attack, however, can be dramatically different from the process for responding to a ransomware attack.

PROCESS DOCUMENTATION: INCIDENT RESPONSE PLAYBOOK/RUNBOOK/PROCESSES

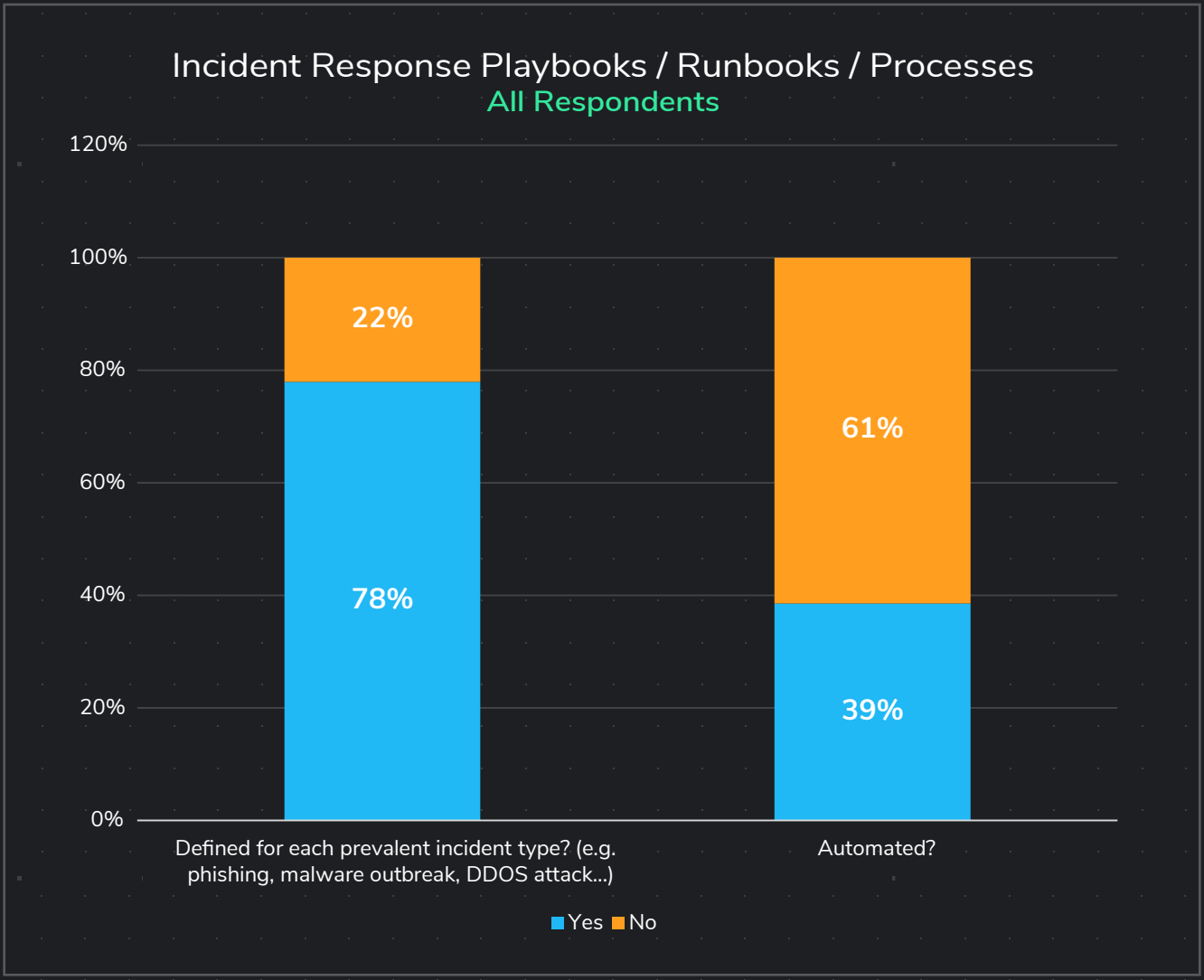
> *Documentation still needs work and does not include everything - still working on it.*
>
> - Anonymous Survey Respondent

When asked whether their organizations have runbooks, playbooks or other documents for incident response actions, **69.9 percent** replied affirmatively. Just more than **30 percent** responded that they did not have their incident response actions documented. When considering the data for respondents that belong to companies with more than **5,000 employees**, a whopping **93.1 percent** have their processes well documented, indicating that bigger companies are much more organized.





Numerous respondents elaborated on their answers, mentioning that they had no formal process, the process covered only the early response efforts with the balance handled “on the fly,” the process covered only some of the potential incidents, or that they simply lacked the time to put processes in place. Approximately 22 percent of the respondents who stated that they had documented actions for incident response admitted that they did not have documented processes for each of the most common types of incidents.

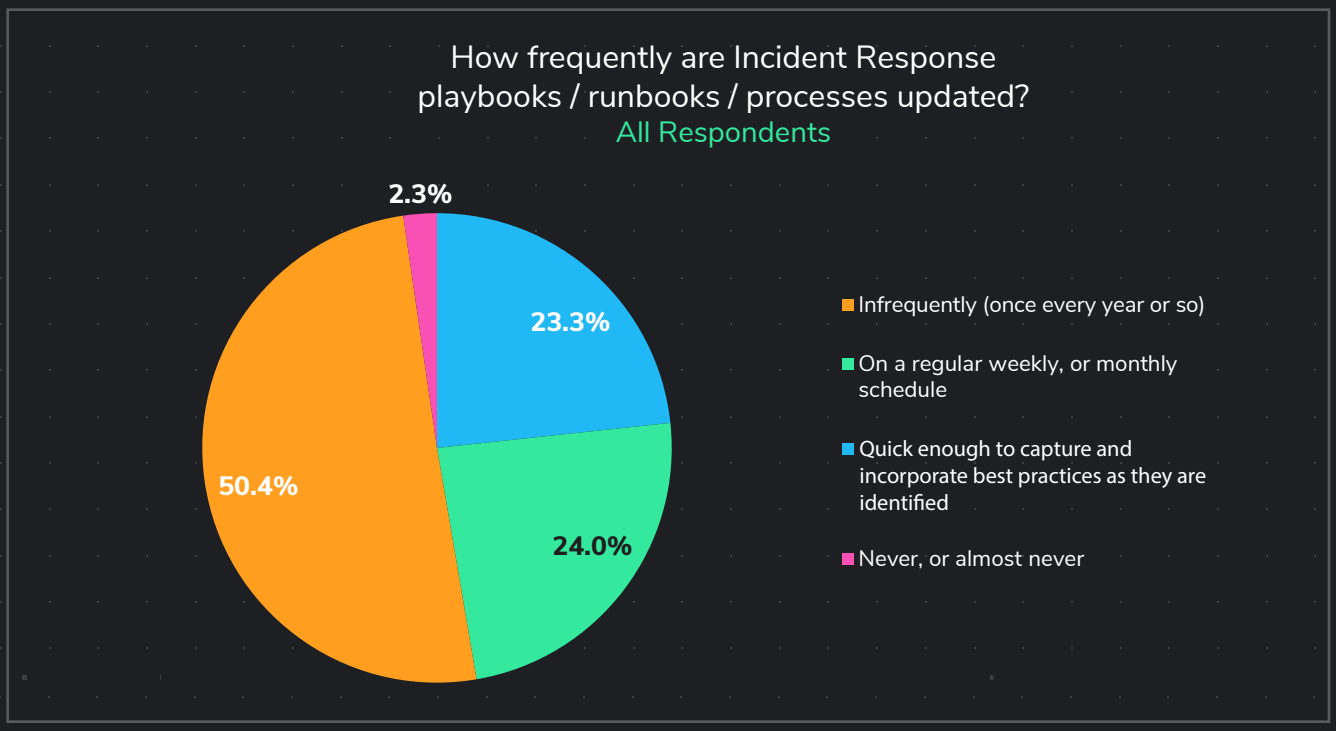


PROCESS UPDATE FREQUENCY: INCIDENT RESPONSE PLAYBOOK/RUNBOOK/PROCESSES

Almost half of respondents are in continual fire-fighting mode making it seemingly impossible for these respondents to keep pace in a rapidly evolving threat environment.

The threat environment is constantly — and rapidly — evolving. Attackers have become increasingly organized, skilled and persistent. New vulnerabilities are being uncovered on almost a daily basis. Innovative ways to circumvent an organization's cybersecurity defenses are creating havoc among government agencies, large companies and relatively small retailers.

Responding to threats requires cybersecurity professionals to maintain constant vigilance, which includes updating response processes and procedures frequently. Admittedly, this can be difficult; almost half of the people responding to the survey stated that they were in constant fire-fighting mode. However, the new normal for an incident response platform will be the ability to update quickly enough to allow best practices to be captured and incorporated as soon as they are identified.

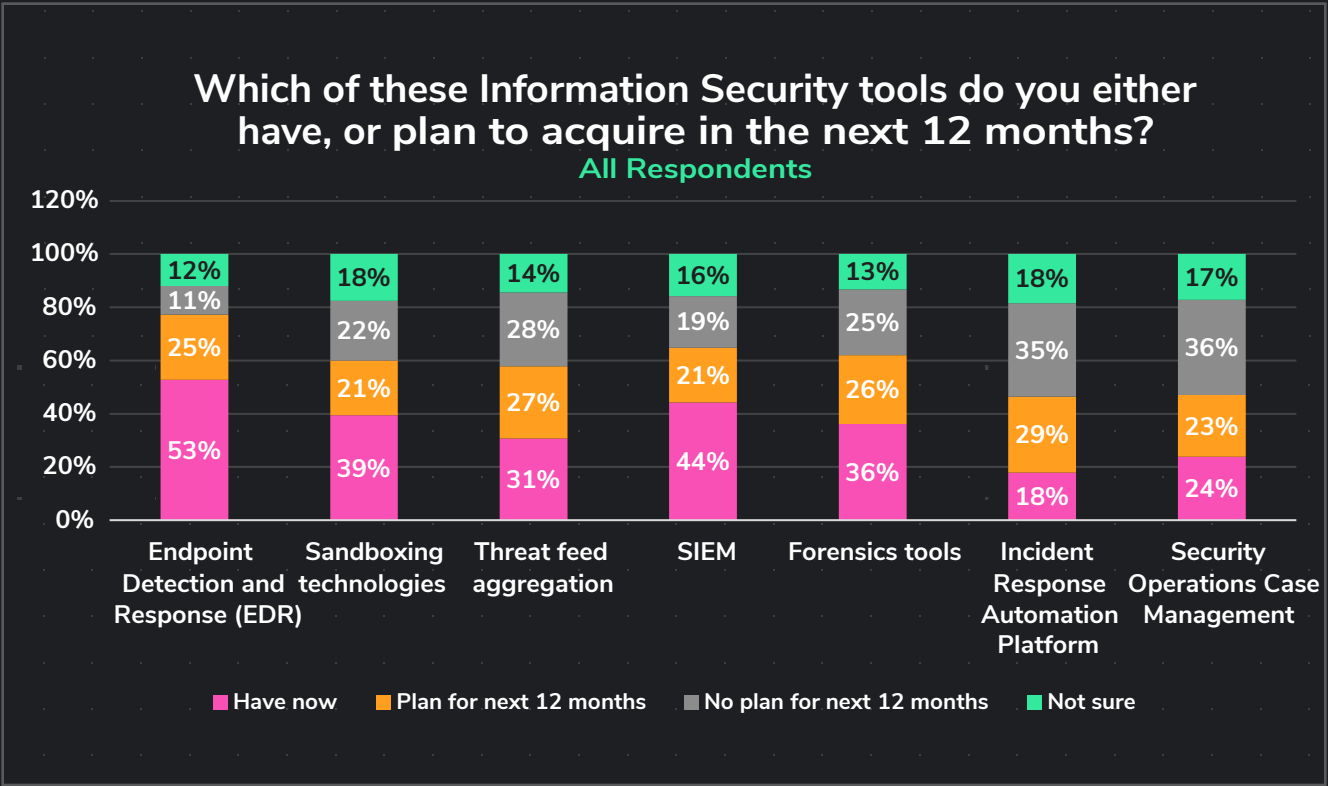


Alarmingly, few respondents indicated that they are performing updates as frequently as they should. In fact, **50.4 percent** responded that updates are performed only once every year or so. A mere **23.3 percent** stated that updates were performed frequently enough to capture and incorporate best practices. Approximately **24 percent** stated that updates were performed on a regular monthly or weekly schedule, but in the rapidly evolving attack environment that exists today, even weekly might not be often enough.

5. THE STATE OF INCIDENT RESPONSE TOOLS

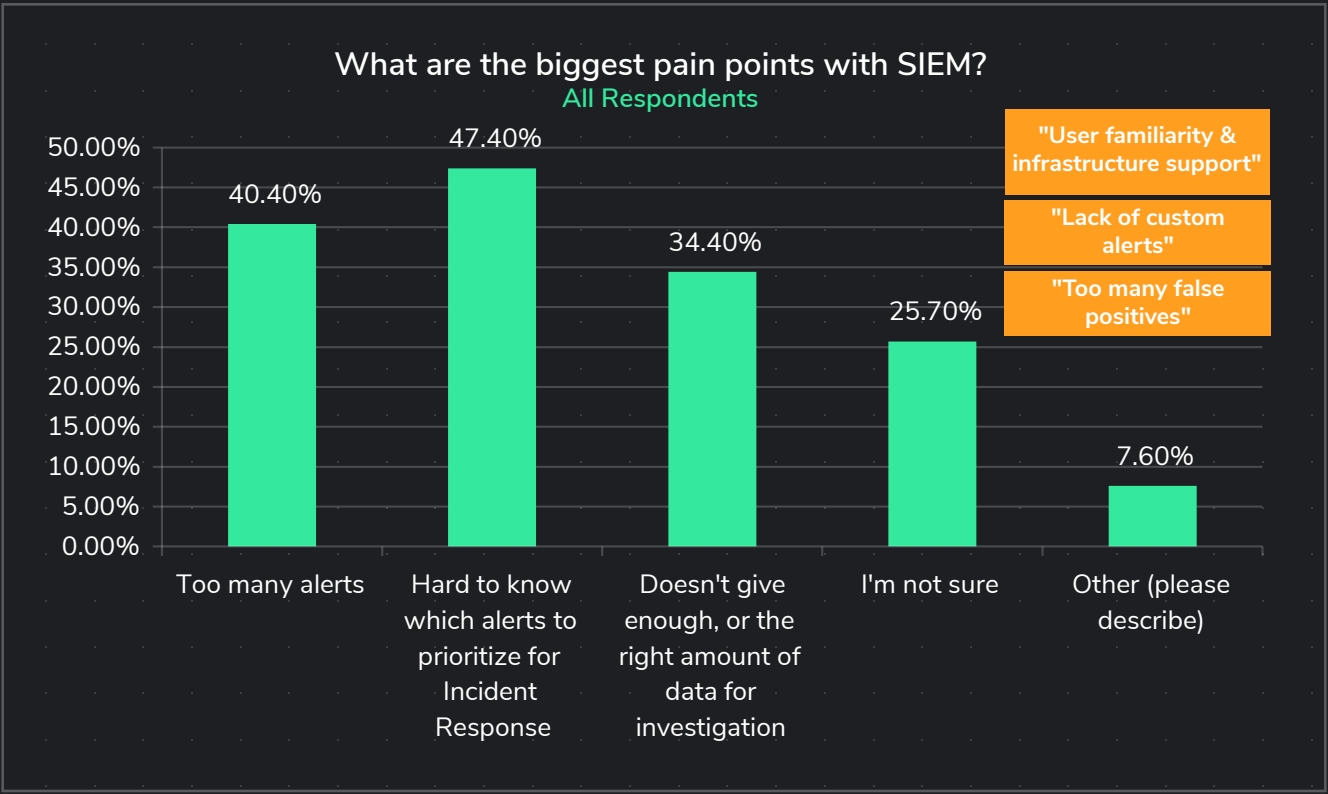
A security information and event manager, or SIEM, is the foundation of an incident response toolbox. SIEM tools are capable of collecting, correlating and analyzing a variety of data, including logs, flows, and alerts, as well as user contexts and vulnerabilities. However, without an appropriate process, SIEM technology is of little or no help. One area in which SIEM shines is the incident response process — but only if the correct tools are used.

TOOLS THEY HAVE NOW OR PLAN TO ACQUIRE



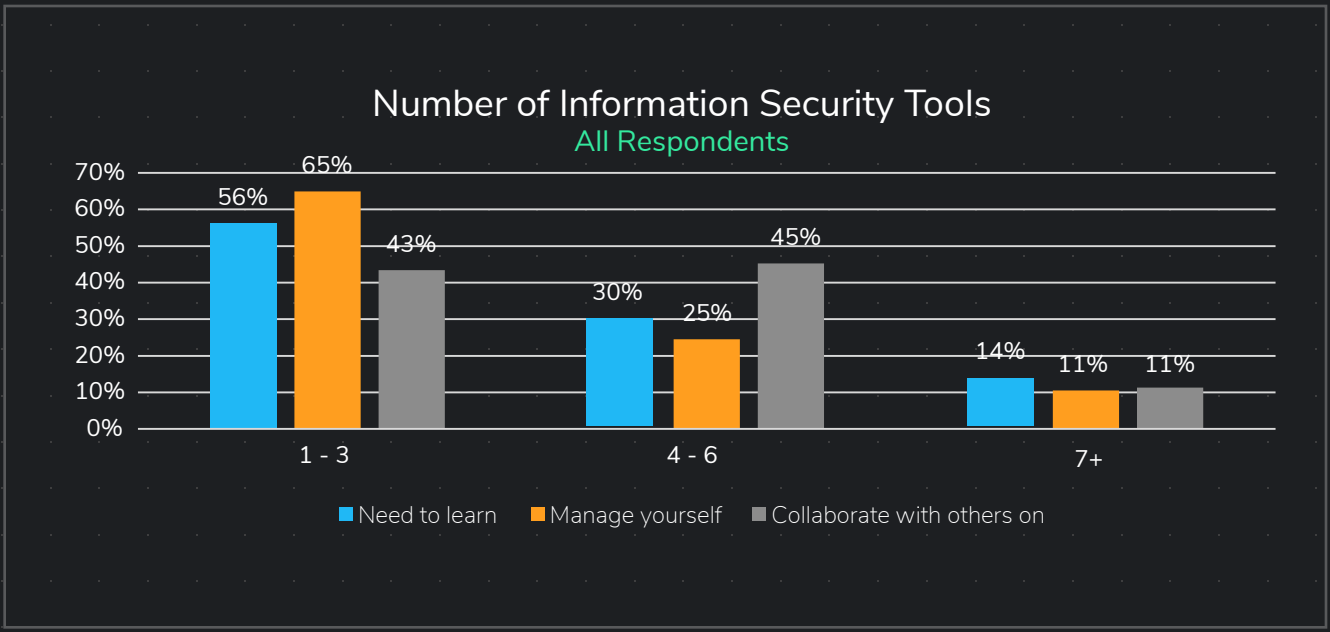
The survey asked respondents to identify security tools that they either had or planned to acquire within the next year. Incident Response Automation Platform was the most popular; 28.9 percent planned to acquire within one year. Threat feed aggregation ranked second, with 27.1 percent planning to acquire within the next 12 months. Forensic tools ranked third with 26 percent planning to acquire within 12 months. EDR, Security Operations Case Management, Sandboxing technologies and threat feed integration were also highly rated with 25 percent, 23 percent, 21 percent and 21 percent planning to acquire within 12 months respectively.

DEEPER DIVE INTO SIEM AND PAIN POINTS



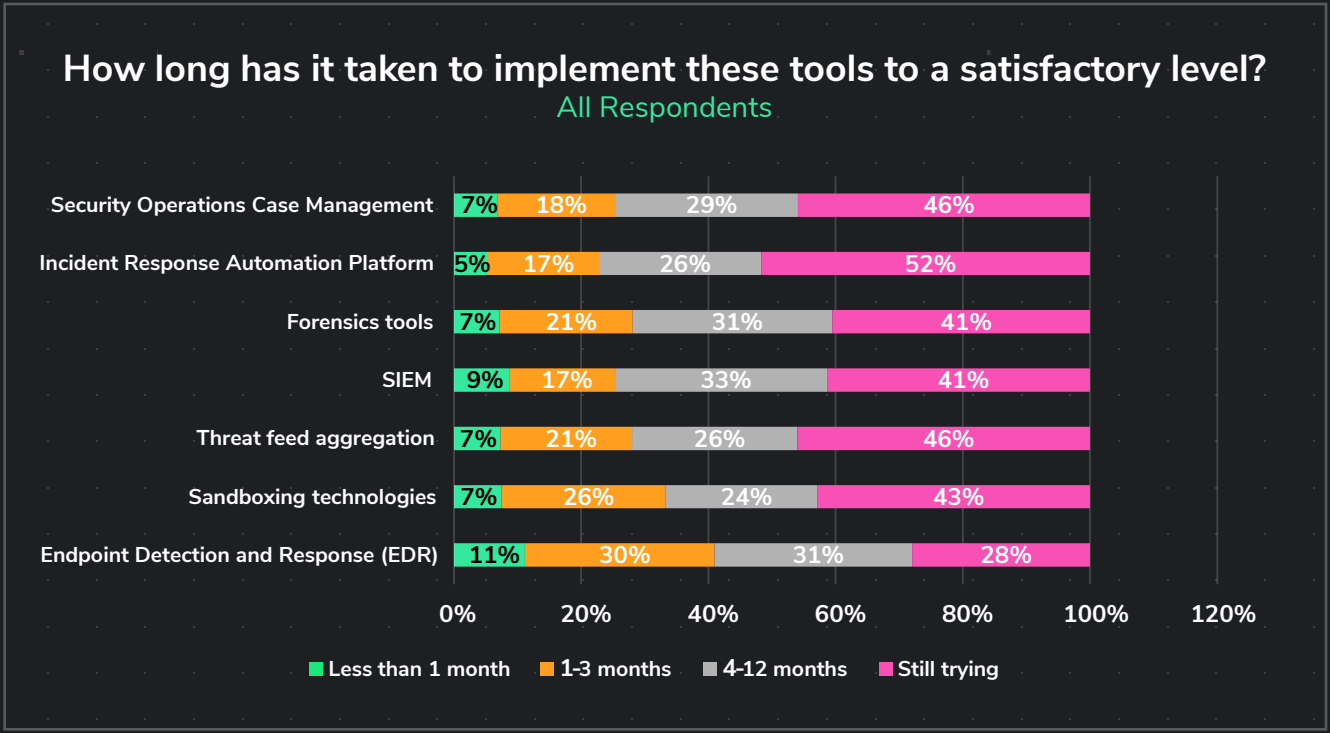
Participants who were already using SIEM were asked to describe their biggest pain points. Approximately **47 percent** felt that it was difficult to determine which alerts should be prioritized for incident response, **40.4 percent** believed the biggest problem was too many alerts and **37.4 percent** felt that they did not get the right amount or sufficient data for investigation. Individual respondents commented that there were too many false positives or that the lack of customized alerts was an issue; writing alert rules, user familiarity and infrastructure support, lack of time to work with SIEM, and finding the funds and skilled personnel to operate were also reported as pain points. Interestingly, many of these pain points could be greatly reduced or eliminated by automating incident response.

NUMBER OF INFORMATION SECURITY TOOLS



When asked for the number of security tools that the respondents needed to learn, **14 percent** responded that they needed to learn at least seven, **56 percent** needed to learn between one and three and approximately **30 percent** needed to learn between four and six security tools. Approximately **43 percent** used between one and three security tools to collaborate with others, **11 percent** collaborated with others using more than seven tools and the remainder used between four and six security tools to collaborate with others. Approximately **65 percent** personally managed between one and three security tools, **10.5 percent** personally managed seven or more tools and the balance managed between four and six security tools.

TIME TO IMPLEMENT TOOLS TO SATISFACTORY LEVEL



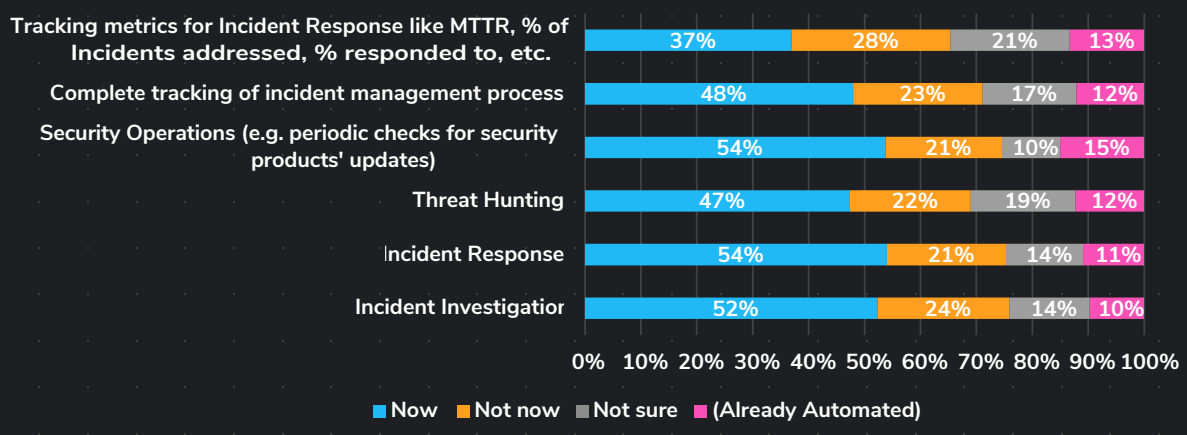
Survey participants were asked to state how long it took for the various tools to be implemented to a satisfactory level, and delivered some disturbing responses. For EDR, 11.2 percent reported that it took less than one month, 29.8 percent reported that it took between one and three months, 31 percent stated that the time was between four months and one year and approximately 28 percent stated that they were "still trying." For sandboxing technologies, only 7.5 percent completed the implementation in less than 30 days, 25.9 percent needed between one and three months, 23.8 percent required between 4 and 12 months and 42.9 percent were still trying to complete the implementation. The results were similar for threat feed aggregation, which had an average time of 3.11 months to implement to a satisfactory level, versus 3.02 months for sandboxing technologies. The longest average time —over 3.2 months — to implement to a satisfactory level was for an incident response automation platform, and more than half of the respondents stated that they were still trying to complete the implementation. Implementation times for security operations case management, SIEM and forensics tools were greater than 3.1 months but less than 3.2 months. Those who reported that they were still trying were asked how long implementation had taken so far; the answers include one year, 15 months and simply, "Years."

6. A LOOK INTO THE FUTURE – WHERE ARE WE HEADED?

The type of attacks, the skills of the attackers and the motives for the attacks have been changing frequently, especially in the past 20 years. It is safe to assume that cyber attacks are here to stay and that they will continue to evolve. Meeting the future challenges will require cybersecurity professionals to evolve as well. One goal for this survey was to gain better insights into how to address future threats by determining today's major pain points.

IR AUTOMATION WILL BE THE MAIN DISRUPTOR

Automation is going to play a critical role in how organizations handle their responses to incidents. However, despite the fact that 54 percent of the respondents believed that automating incident response would provide immediate benefits, only 10.9 percent had already automated this facet. The results were similar when it came to automating incident investigation, threat hunting and tracking the entire incident management process.



Unfortunately, many organizations have automated isolated tasks rather than deploying an incident response platform. They believe that they are "already automated" and fail to recognize what they could gain from an incident response platform, particularly at large companies where automation may consist of a number of disconnected solutions.

Another issue that frequently arises is that management tends to be more enthusiastic about automation than workers. It is a classic dilemma that is often encountered whenever a new solution is proposed, including new software, upgraded systems, and updated procedures. Workers who perceive that the change threatens their job security or happiness can find an extensive range of justifications to undermine efforts to improve efficiency.

Furthermore, they may be wary of the ease of implementation or unaware of how a new solution could benefit them. Therefore, when opting for an automated incident response platform, managers must ensure that they understand the motivations and fears of their staff members.

Yet another issue that can arise is the misconception that automation can resolve all IR issues. Although automation can provide many benefits, it cannot completely close the skills gap or replace humans in the IR process. During an incident response, analysts typically progress through four stages:

1. Preparation
2. Detection and analysis
3. Containment, eradication and recovery
4. Post-incident activities

Automation may help during each stage, but the amount of help provided varies. Therefore, organizations need the ability to perform collaborative, interactive investigations to scale the incident response function effectively within a SOC.

Interactive, collaborative investigations can help narrow the talent gap. However, great benefits can be realized through machine learning. For example, the system can learn to identify the experts in certain types of incidents. The system can learn what actions an expert would take in a particular situation and recommend those actions to a junior analyst. The system can also recommend who junior analysts should contact when an incident within the expert's area of expertise occurs.

OTHER POTENTIAL DISRUPTORS

Automation may be the greatest disruptor that will be seen in the future, but it is not the only potential disruptor. Many of these other potential disruptors may rely on automation, but others may be innovative solutions that are presently unknown. However, based on the data collected during the survey, it is predicted that there are three types of potential disruptors that will change many facets of incident response.

1. Technology that can address the widening skills gap is desperately needed. When asked to rate the pain level for finding talent with highly specialized security skills, **91.1 percent** of the respondents rated the pain level as moderate or high, and approximately **92 percent** rated the pain level as moderate or high when it came to finding candidates who were highly experienced in information security. The demand for cybersecurity talent is only going to increase, worsening the global shortage of qualified candidates.

2. Employee retention is also a major pain point for most organizations. Approximately **54 percent** of the respondents assigned a pain level of moderate or high for employee retention. Since the survey revealed that more than **76 percent** of information security (IS) employees left to accept positions with higher salaries, companies that cannot compete monetarily must find new ways to keep analysts happy. Overwork, fatigue and the opportunity for skills enhancement also figured prominently in the list of reasons why cybersecurity staff members leave.

   Technology that can improve the happiness of the security staff can help address retention issues. Eliminating duplicate efforts, filtering out and responding to false positives through automation, reducing the volume of alerts to which each analyst must respond, and reducing the number of mundane tasks handled can help improve morale and employee satisfaction.

3. Technology that can address ROI can help keep management happy. After all, a company is in business to generate a profit, and when managers lack visibility into the return on cybersecurity investments, they can begin to question every expenditure. Technology that can provide this visibility and improve reporting can help generate support for the SOC from C-suite executives.

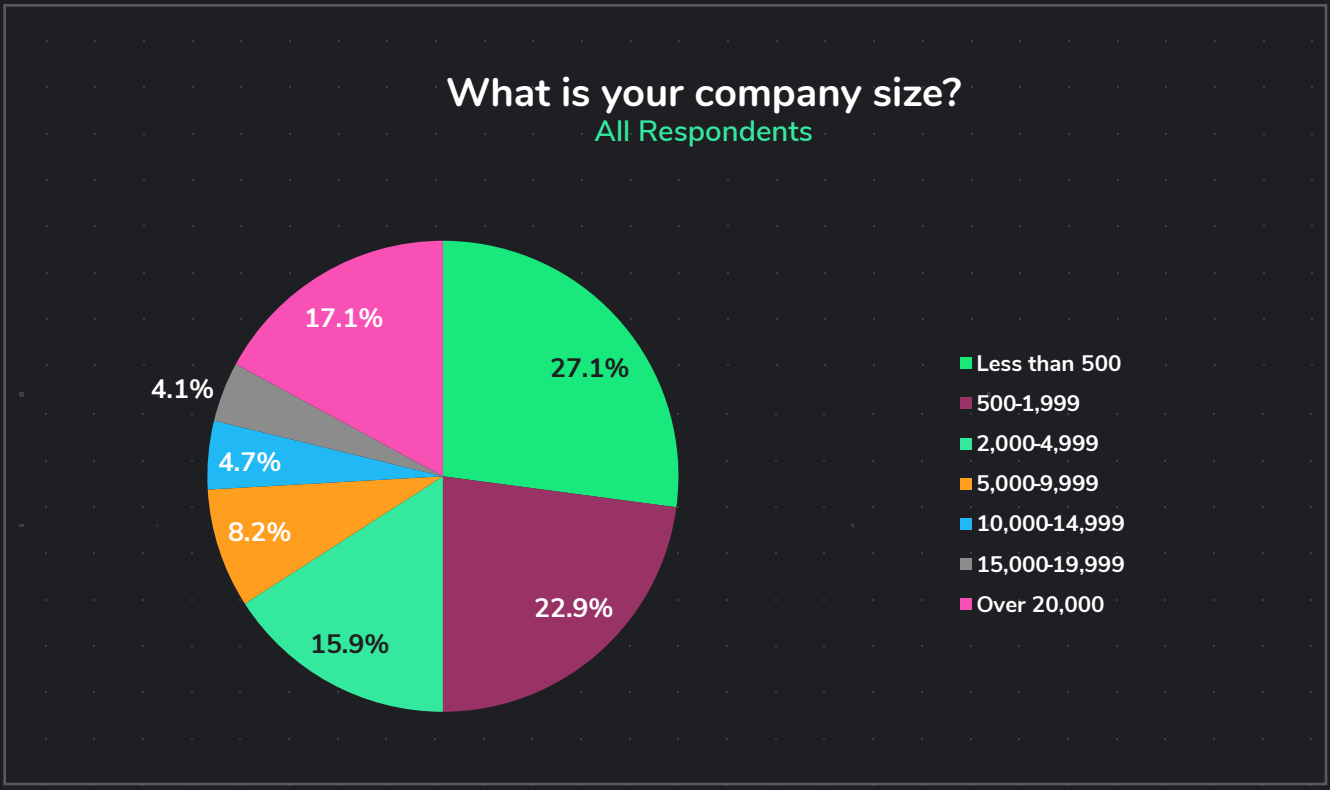
PREPARING FOR DISRUPTORS

Considering the potential disruptors looming on the horizon, security automation is no longer enough. What is needed is a true security orchestration and automation solution. Orchestration allows security professionals to have access to the “big picture.” It is a combination of automation and human analysts that allows the SOC to accomplish more in less time and with fewer resources. Those organizations that embrace security orchestration now will be in a better position to take advantage of the potential disruptors that are sure to come.

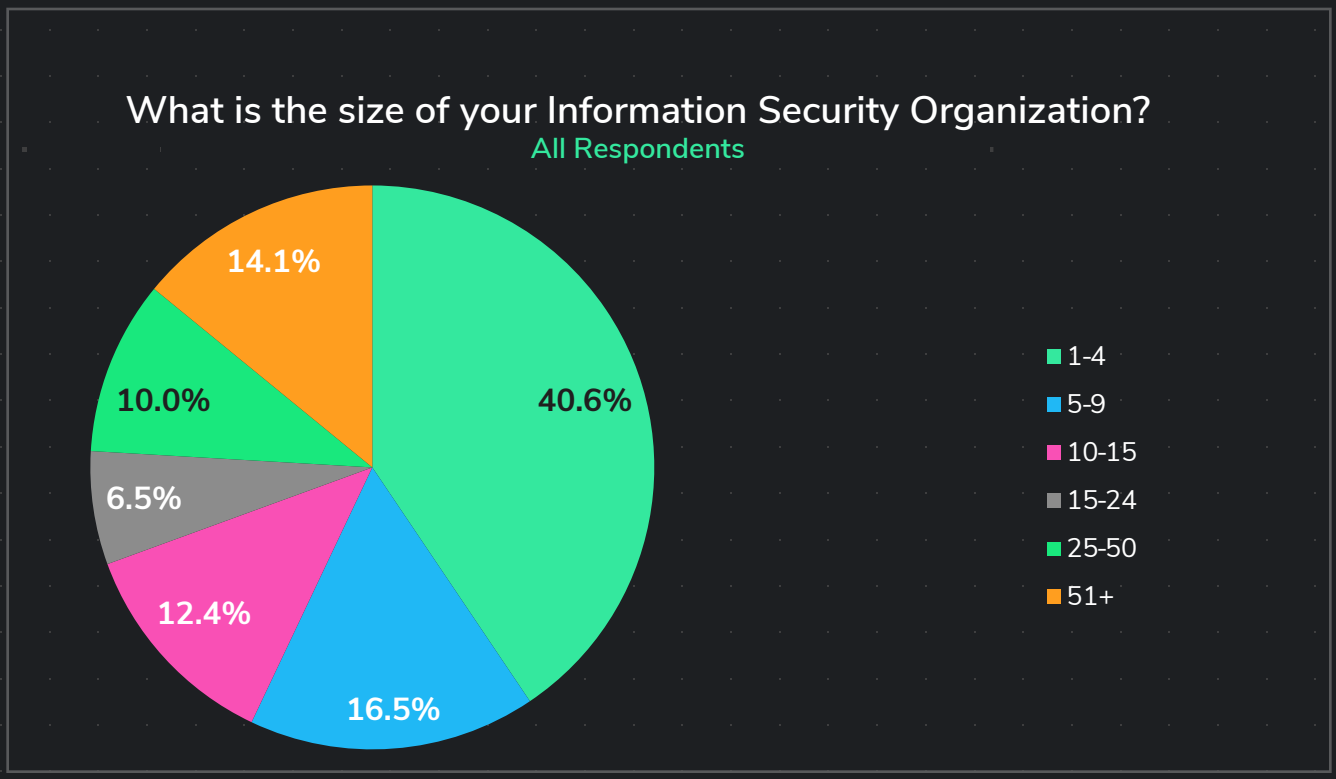
7. WHO WE SURVEYED

To ensure that accurate results from a range of companies were obtained, invitations were issued to qualified respondents who are involved with or are responsible for carrying out the information security and incident response function. Respondent identities were not known to the research firm compiling the responses, nor was any personal or identifiable information collected from respondents.

COMPANY SIZE

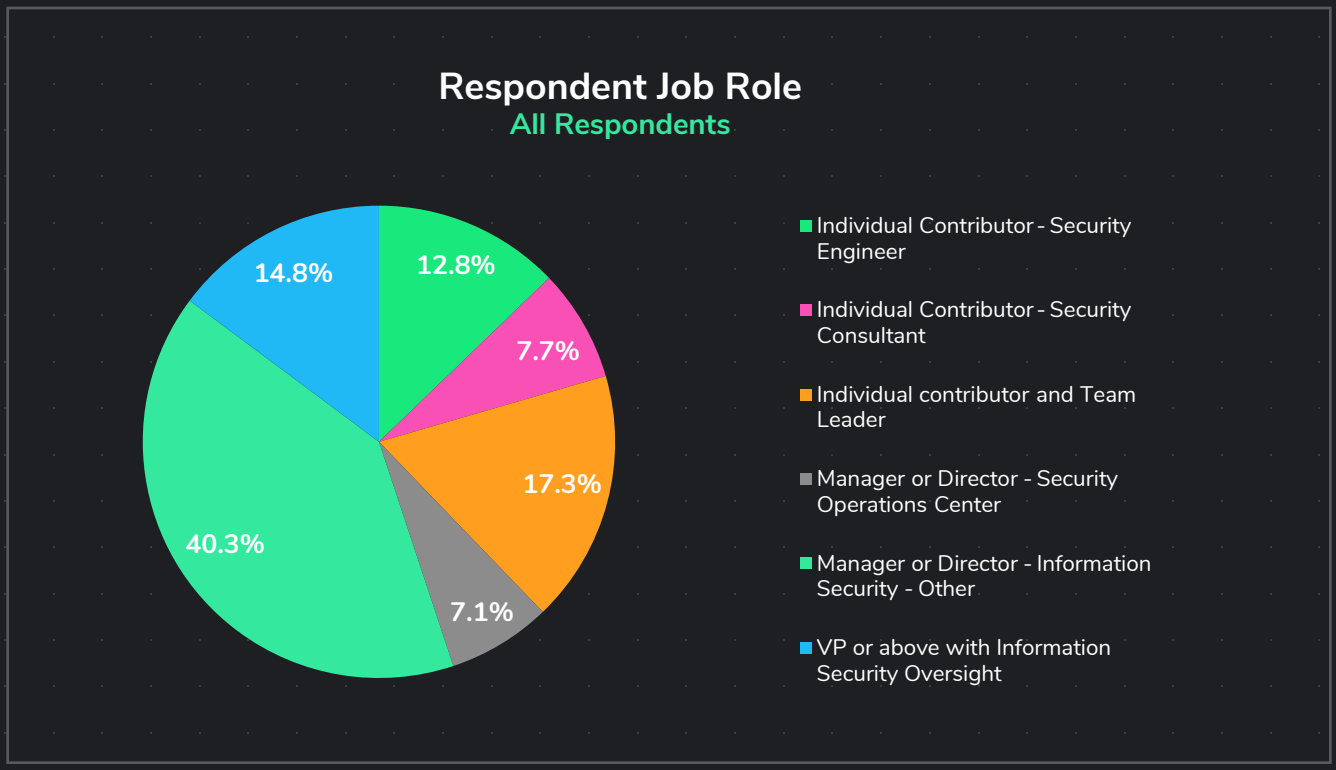


Among all participants, 27.1 percent were from companies with fewer than 500 employees, 22.9 percent were from employees with 500 to 1,999 employees, 15.9 percent were from companies with 2,000 to 4,999 employees, and 22 percent were from companies with 5,000 employees or more. Among companies with more than 5,000 employees, 50 percent had more than 20,000 employees, 12.1 percent had between 15,000 and 19,999 employees, 13.8 percent had between 10,000 and 14,999 employees, and 24.1 percent have between 5,000 and 9,999 employees.



When asked about the size of the IS operations, **40.6 percent** reported between one and four employees, **16.5 percent** stated that there were between five and nine employees and **12.4 percent** reported between **10 and 15 employees**. Approximately **6.5 percent** reported staffing of between **15 and 24 employees**, **10 percent** stated there were **25 to 50 employees** and **14.1 percent** had at least **51 security employees**. Among the respondents having more than **5,000 employees**, **37.9 percent** had more than **50 employees** in their cybersecurity organization.

RESPONDENT INFORMATION



Respondents identified their role in their company's IS organization. Among all respondents, 12.8 percent were individual contributors engaged as security engineers, 7.7 percent were individual security consultants, and 17.3 percent were team leaders. Approximately 7 percent were the manager or director of a security operations center, 40.3 percent were the manager or director of another IS department, and 14.8 percent were at least a vice-president having IS oversight. Among companies having more than 5,000 employees, 41 percent were individual contributors; the balance was managers or executives.

ABOUT VIB - THE RESEARCH COMPANY

Virtual Intelligence Briefing (ViB) conducted the overall research. ViB is an interactive on-line news community focused on emerging technologies. ViB's community is comprised of more than 1.2M IT practitioners and decision makers who share their opinions by engaging in sophisticated surveys across a range of IT solution areas. For its community, ViB stimulates conversations around emerging technologies. For technology marketers, ViB provides a wide range of marketing and sales enablement services including surveys for content generation and market intelligence, and demand generation, newsletter and email list services. For more information visit vibriefing.news.