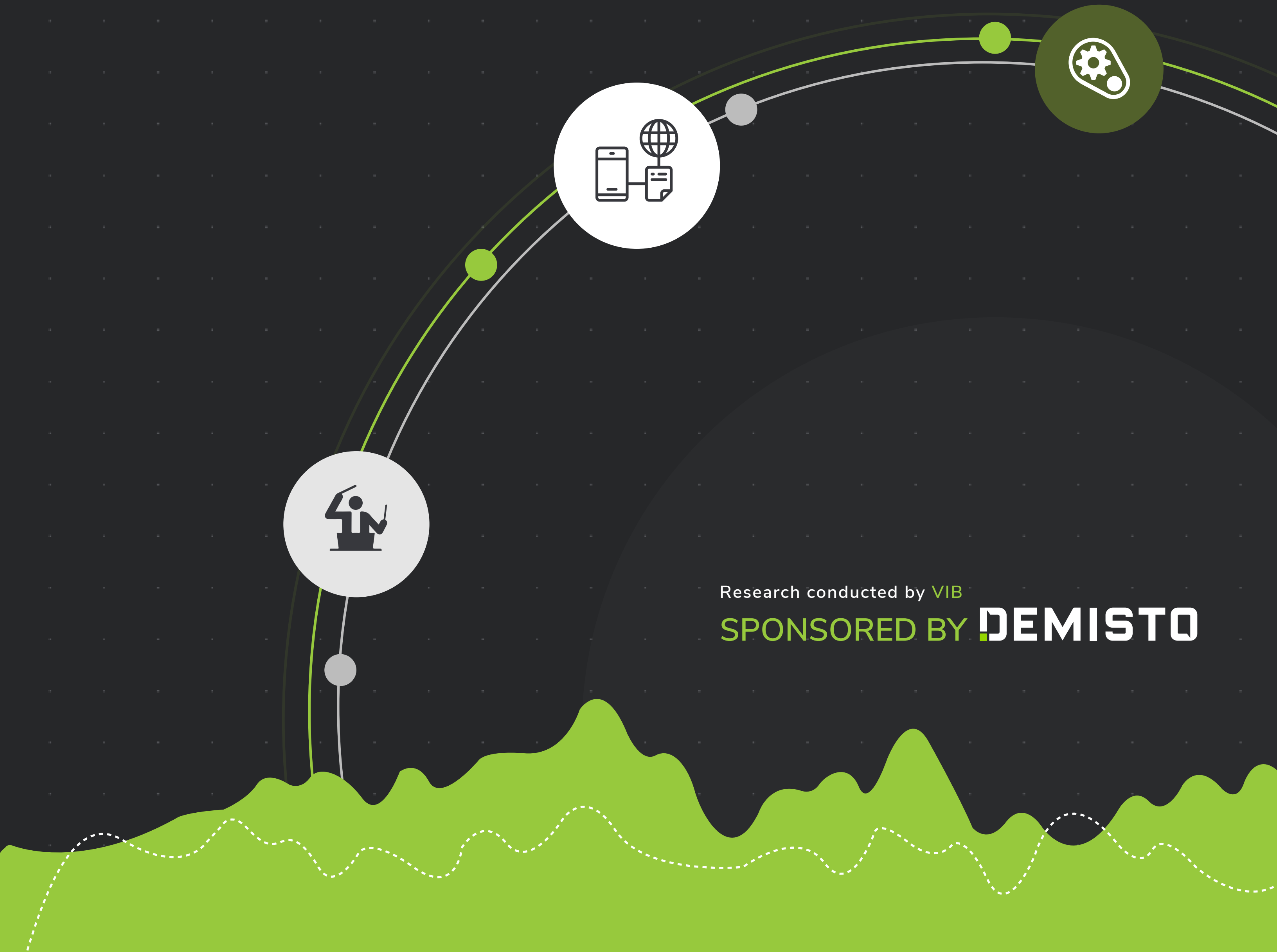
The State of SOAR Report, 2018

The second annual state of incident response report



Research conducted by VIB

SPONSORED BY DEMISTO

TABLE OF CONTENTS

Executive Summary

Today's business landscape is a delicate balancing act between technological advancement and security. Workplace changes and technical innovations have made it easier to do business and live our lives, but securing these manifold developments is a mammoth task that falls upon already overworked security teams.

There is already a wealth of research that highlights the unending growth in security alerts, a widening security skills gap, and the ensuing fatigue that is heaped upon understaffed security teams. Demisto conducted a large study to delve deeper into these issues, their manifestations, and possible solutions. Our results yielded fascinating insights into the state of cybersecurity in businesses of all sizes.

Shift to SOAR

For this second annual report, we decided to shift our focus from incident response to SOAR (Security Orchestration, Automation, and Response) as we believe SOAR to be a more all-encompassing lens through which to view the security posture of a business. We will present a brief overview of SOAR and its drivers before discussing our research findings.

Alerts Continue to Rise

Research found that security teams are facing over 174,000 alerts per week on average and are able to review only around 12,000 of them. The chief sources for this alert fatigue were a proliferation of security tools (46% of respondents stated that their security tools generated too many alerts) and a shortage of experienced analysts (79% of respondents highlighted 'not enough people' as a key SOC challenge). A direct outcome of rising alert volumes was felt in high MTTR (Mean Time to Respond), with research finding that it took an average of 4.35 days to resolve an incident.

Personnel Challenge

Organizations continue to face challenges in hiring, training, and retaining security personnel. Our research found that it took an average of 8 months to train new security analysts; despite this, a quarter of employees were likely to end up leaving within 2 years. In this scenario, SOAR tools should aim to both fill personnel gaps and make existing analysts' jobs easier and more fruitful.

Piecemeal Processes and Measurement

A direct consequence of rising alerts and scarce resources is that security teams are too busy responding to incidents to find time for strategic process measurement and improvement. Close to 42% of respondents cited that they didn't have a system in place to measure IR metrics. Over 50% of respondents stated that they either did not have process playbooks in place or that the playbooks were rarely updated after initial implementation.

Willingness to Automate

One of the key findings from our research was an increase in the number of respondents who indicated a strong ‘readiness to automate’. Besides the growing market validation of automation, this increase in willingness is likely connected to the fact that all four major security challenges revealed by research participants were related to human capital shortages.

It’s Threat Hunting Time

Research respondents saw SOAR helping with both proactive and reactive spheres of their day-to-day operations. Around 62% of respondents cited threat hunting as an expected benefit of SOAR (specifically automation). SOAR tools have a unique capability combination: they’re able to ingest threat data from multiple sources, and they’re able to execute automated playbooks that rapidly check for these threats across user environments. When executed correctly, threat hunting and SOAR work hand in glove.

Multi-faceted SOAR Value

The survey found that respondents understood the value of SOAR and estimated that it could help across a range of issues. The major expected benefits of SOAR were in reducing false positives, prioritizing incidents after risk determination, coordinating actions across security tools, and automating repeatable response actions.

1. Understanding SOAR

To understand the reason for our shift from incident response to SOAR as a focal point, it is important to understand what SOAR is and how it encompasses incident response. Incident response focuses primarily on addressing issues after they have been identified. However, an incident's lifecycle involves many more stages: aggregation, enrichment, correlation, and investigation being some of them. SOAR, unlike incident response, addresses all these stages and more. Here's a brief description of the building blocks that make up SOAR.

- **Orchestration** refers to the act of integrating disparate technologies, usually through workflows, so that they can function together. This means using security specific and non-security specific technologies simultaneously in a way that eases coordination.
- **Automation** refers to the process of machines executing tasks hitherto performed by humans. In the context of SOAR, automation is ideally seen as human enhancement and not human replacement. Automation of repeatable, low-level tasks acts in concert with human decision-making for overall acceleration of incident investigations.
- **Incident management and response** is still a crucial element in SOAR. Fundamentally, SOAR seeks to foster a comprehensive, end-to-end understanding of incidents by security teams, resulting in better, more informed response.
- **Dashboards and reports** form a critical part of SOAR. One of the ways to achieve unified response is by providing data visualizations where incidents can be easily seen, correlated, triaged, documented, and measured.

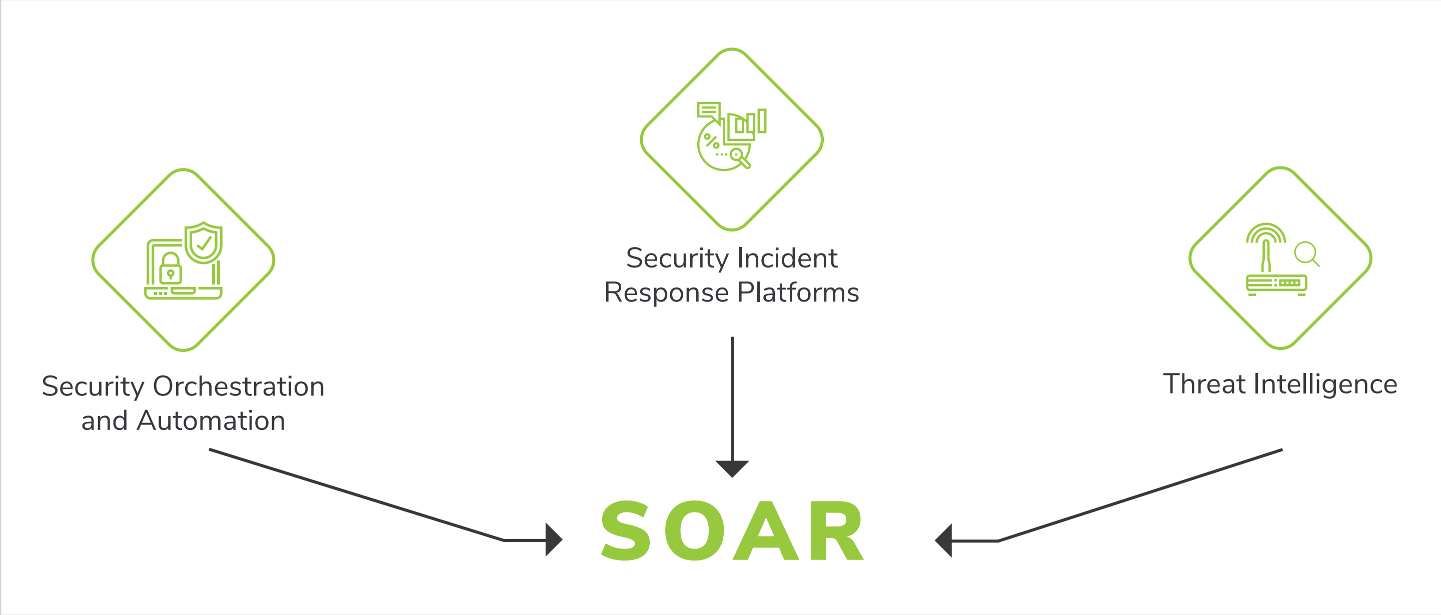

Security Incident Response Platforms
Security Orchestration and Automation
Threat Intelligence
SOAR

Figure 1

2. SOAR Drivers

The development of SOAR as a cybersecurity practice has been driven chiefly by the shortcomings of conventional tactics:

- **Staff Shortage:** There continues to be a sizable demand-supply gap in terms of security personnel. To meet this challenge, organizations are searching for fields where automation and standardization can help their existing employees work better and faster.
- **Unattended Alerts:** The sheer volume of alerts far outpaces the security team's capacity to examine them. Consequently, serious threats can be left unaddressed because security teams are too busy wading through the sea of events on their screens.
- **A Paucity of Proactivity:** Since security teams are so busy dealing with day-to-day alert prioritization and response, they don't have time to proactively hunt for threats in their environment before it's too late. This inability to read early warning signs results in a vicious cycle that leads to even more alerts being generated, usually after it's too late.
- **Lack of Central Context:** The process of determining if an alert constitutes a serious threat requires cross-referencing multiple data sources for complete context. While a large number of security tools provide unique threat insights, teams find it tough to collate and correlate intelligence at a central location, leading to variance in investigation quality.

3. Security Challenges

To better understand how cybersecurity shortcomings are affecting businesses in the real world, we asked several questions in our study. These questions helped us understand two things. Firstly, it helped us verify whether our survey recipients felt the same challenges as those expounded by general research. Secondly, it helped us understand the priority and magnitude of each issue.

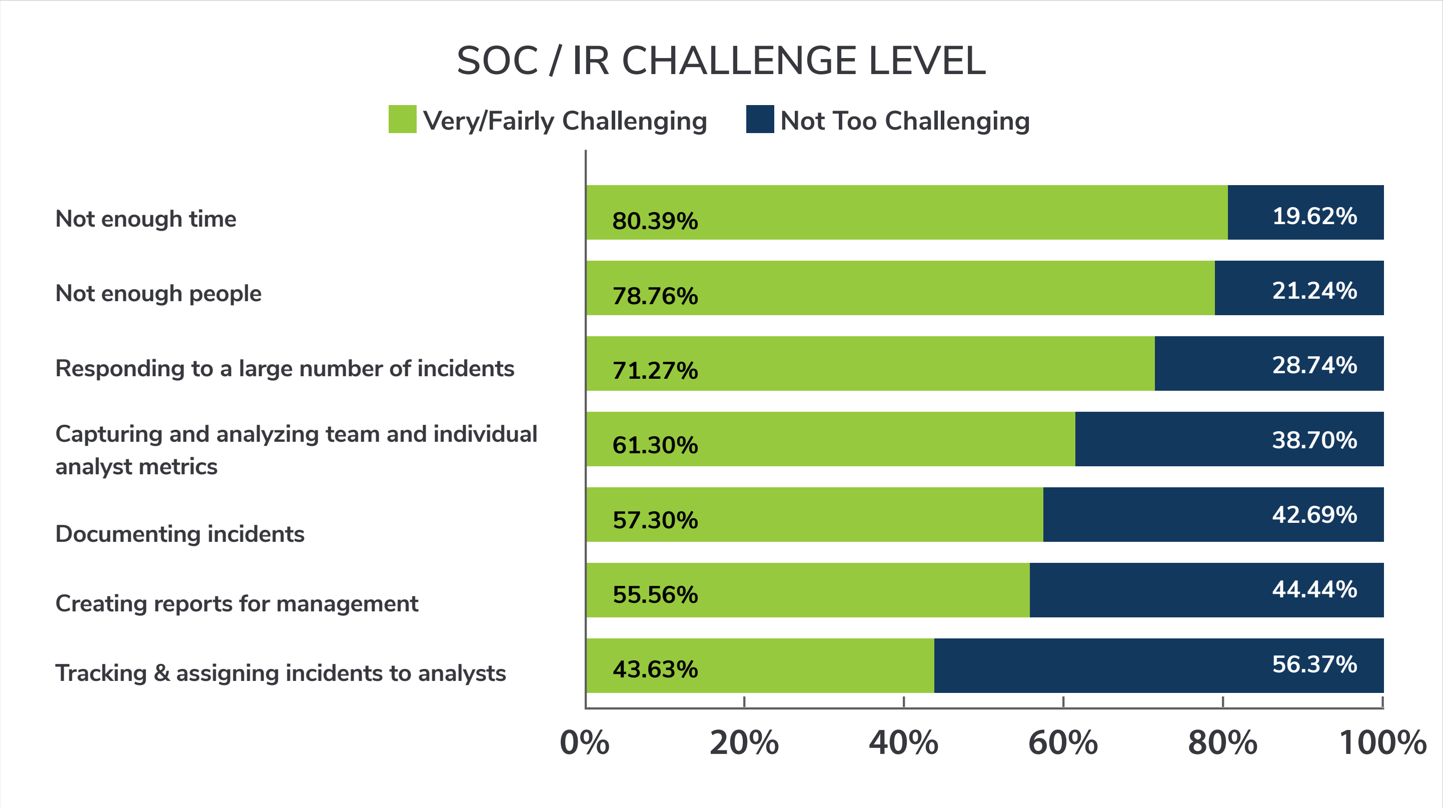


Figure 2

The pattern that stands out starkly from these results is that the **security skills gap continues to be a challenge**. Improving processes and results, coordinating among multiple products, improving team collaboration, and avoiding effort duplication ranked highly among organizational security challenges, with the human capital crunch being a common underlying thread.

While these results were insightful in isolation, we also asked recipients to provide subjective comments and additional information that allowed us to better understand their specific challenges.

We were able to identify a unique agreement among respondents as they further explained their issues with staffing. We got comments from businesses worried about "fewer people doing more work" and analysts having "a lot of other responsibilities and finding it difficult to devote enough time to properly documenting incidents, resolutions, etc."

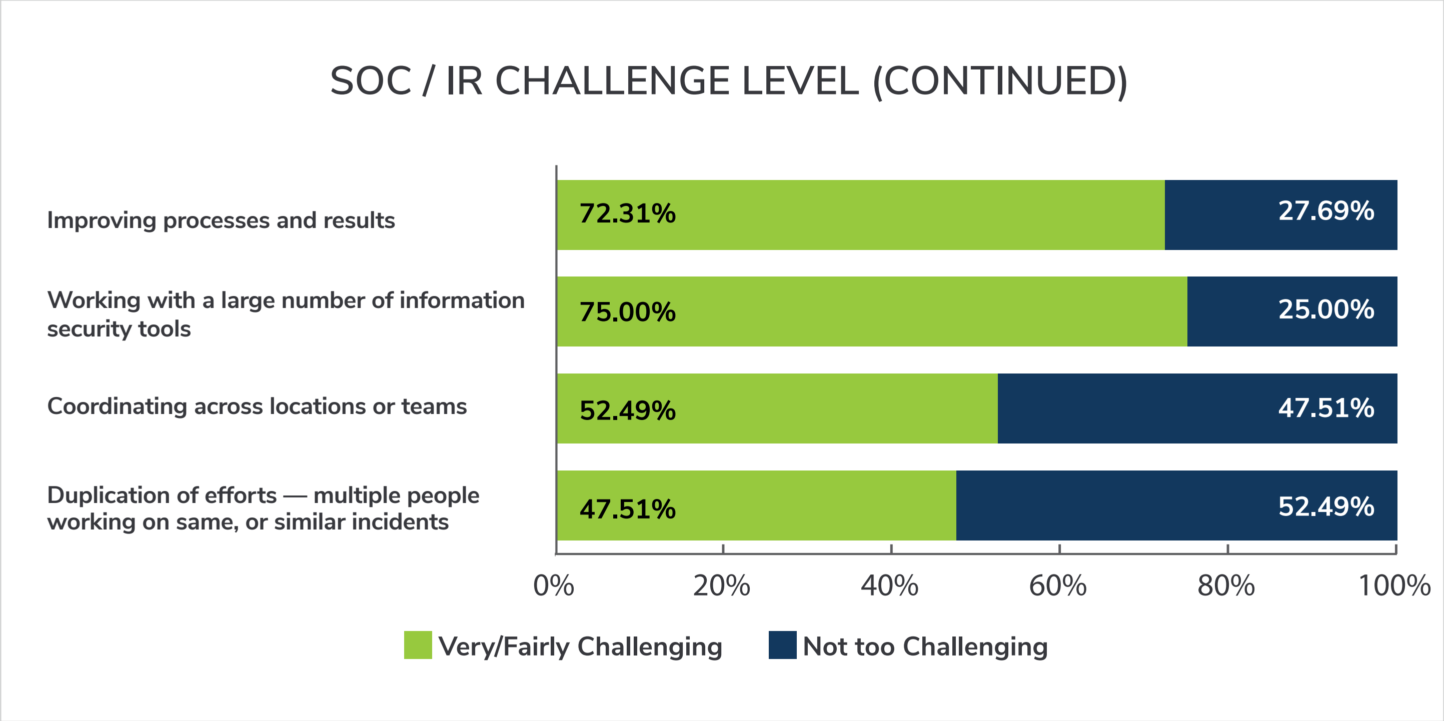


Figure 3

Respondents also opened up about how these issues could be resolved. Many emphasized the importance of proper communication, observing how a lack of single-source communication could lead to unnecessary duplication of efforts. They also emphasized the importance of creating and implementing new processes to address these issues.

EMPLOYEE RETENTION

To further explore the issue of employee retention, we asked several questions to help gauge the health of hiring and turnover in information security.

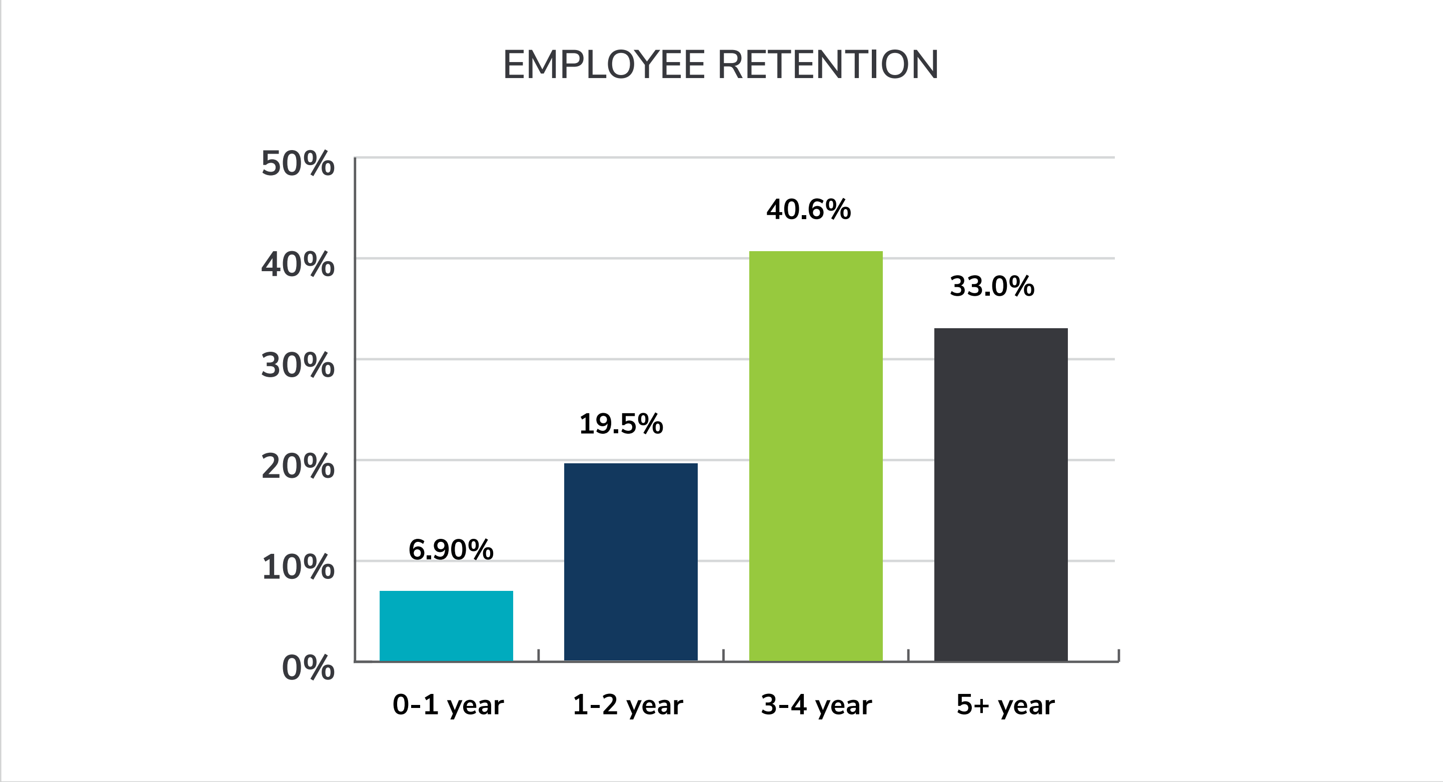


Figure 4

From these results, we can see that 67% of employees leave in 3-4 years and **a quarter of employees leave within two years**. With the notoriously steep learning curves and training routines that define a security analyst's onboarding, this retention rate is a concerning figure.

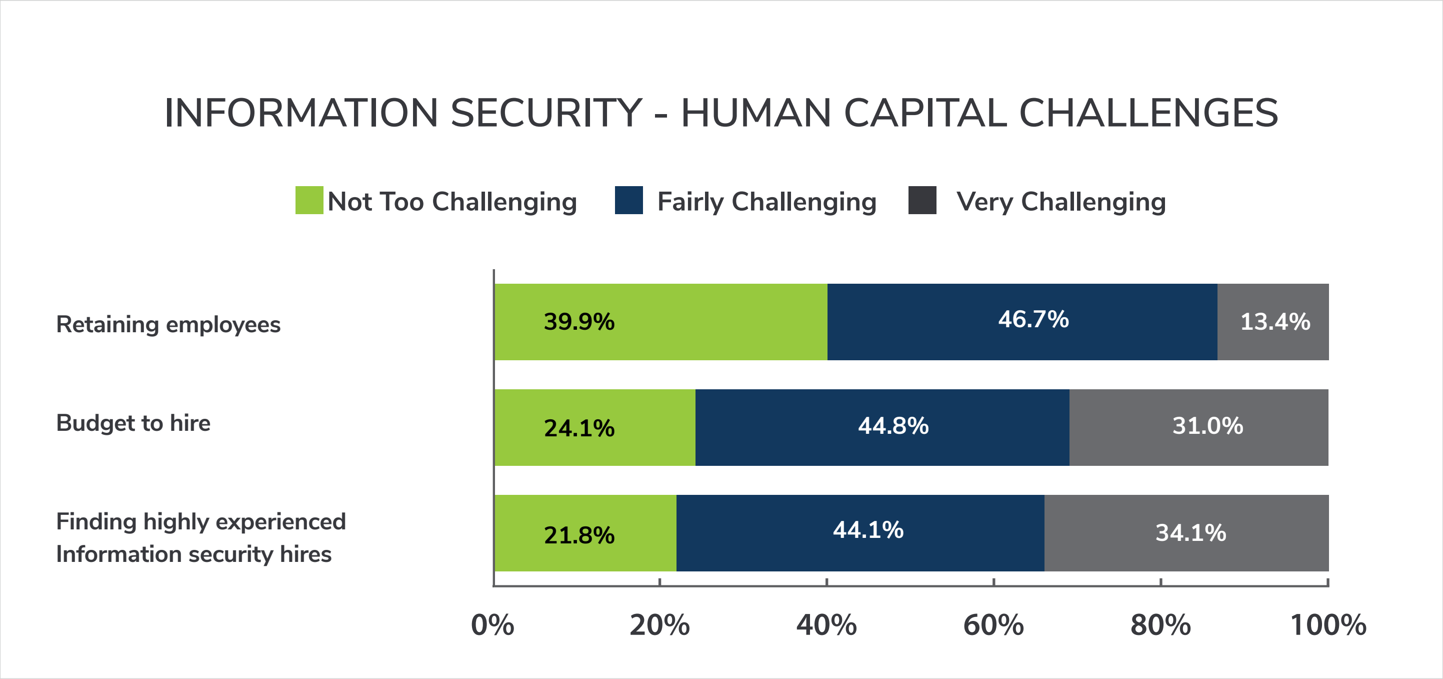


Figure 5

Respondent commentary on the matter provided further insight into the hiring dilemma. It was noted that attracting talent to the public sector was often a difficult challenge. Many professed an inability to find qualified candidates given the large discrepancy in what candidates list on their resume as a skill versus what they know.

Lastly, there seemed to be a broad agreement on the fact that money/budget was now a secondary issue after time. Time was by far the most limiting factor facing many of the businesses we interviewed.

ATTRITION

While interviewing employees, we wanted to find out what was causing the high rate of attrition within information security.

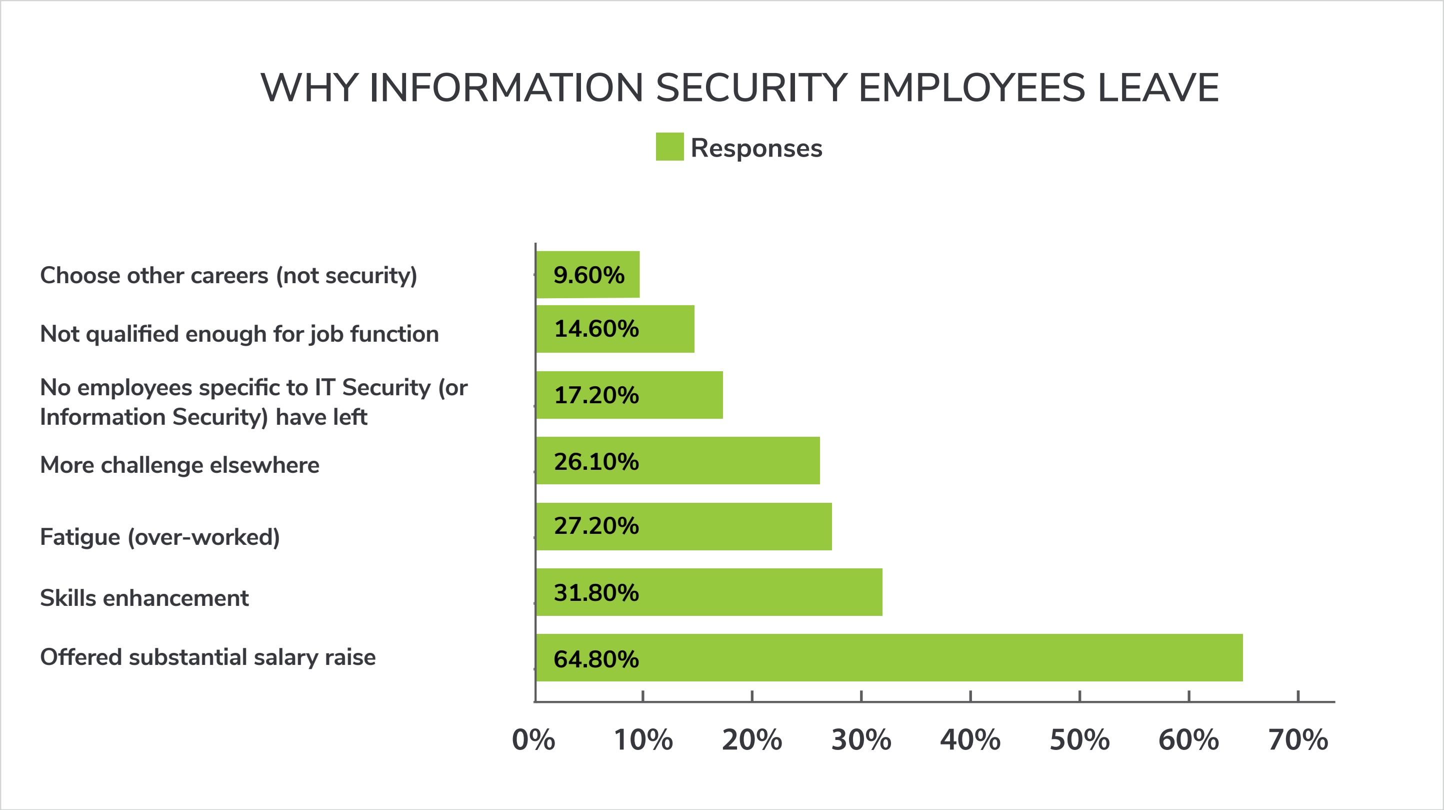


Figure 6

Unsurprisingly, a substantial salary raise was far and away the number one reason for employee departure. This is congruent with the security skills gap: if there's a dearth of new security personnel on the market and it takes time to train security teams, companies will try to outdo each other in terms of remuneration to prize away experienced security analysts.

To delve further into this information, we asked employees a more generalized question about what was important to them in their field.

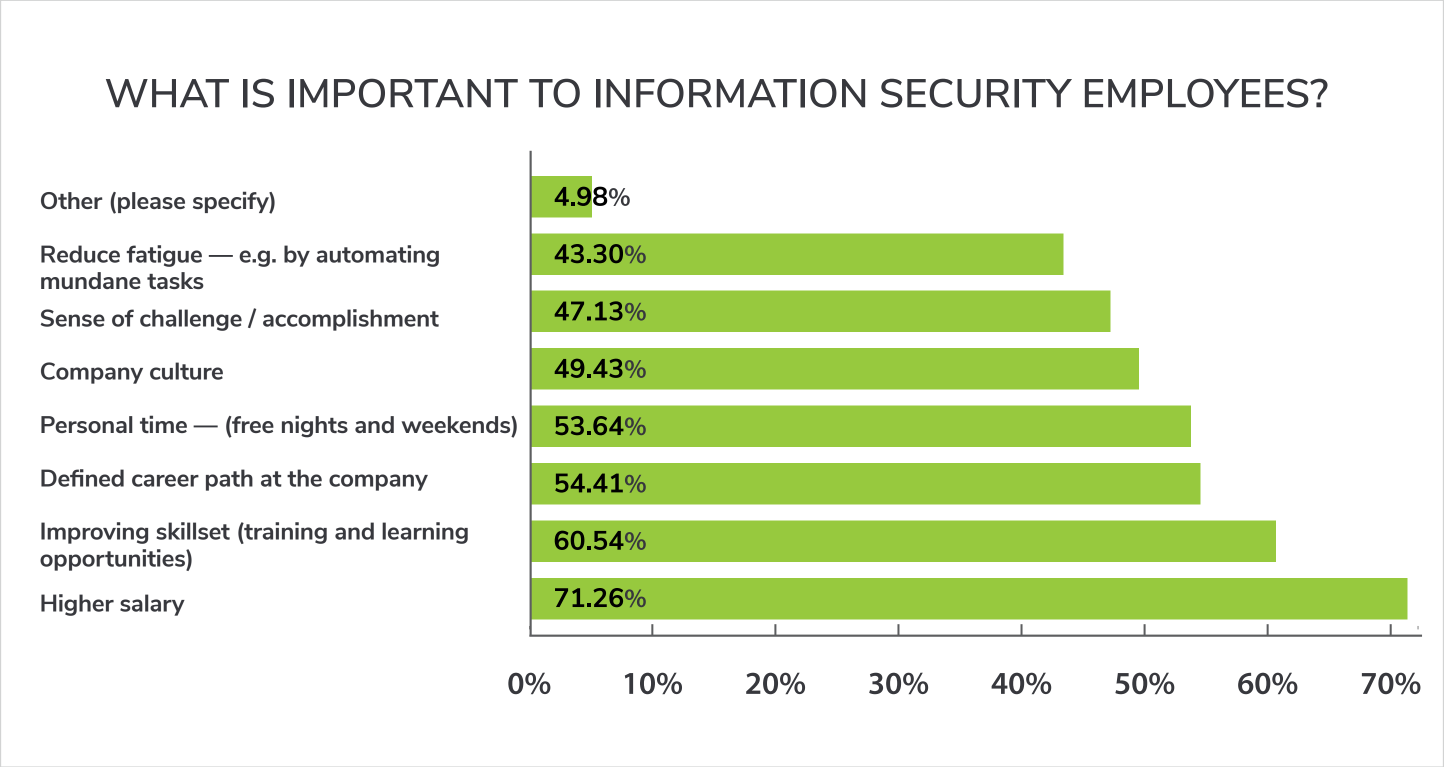


Figure 7

Respondent data made it clear that salary was the chief driving factor. Taking this information in concert with other security challenges, it's understandable that overworked security analysts – who are in demand and have irreplaceable knowledge – expect to be compensated for their skills and efforts.

Looking beyond the monetary reasons, respondents also cited a desire for work-life balance and skills improvement as desirable aspects they looked for in a job opportunity and employer.

HIRING + TRAINING

Turning back to employers, we wanted to ascertain how long it took for them to acquire and train a new employee and better understand the time/cost concerns associated with high attrition rates.

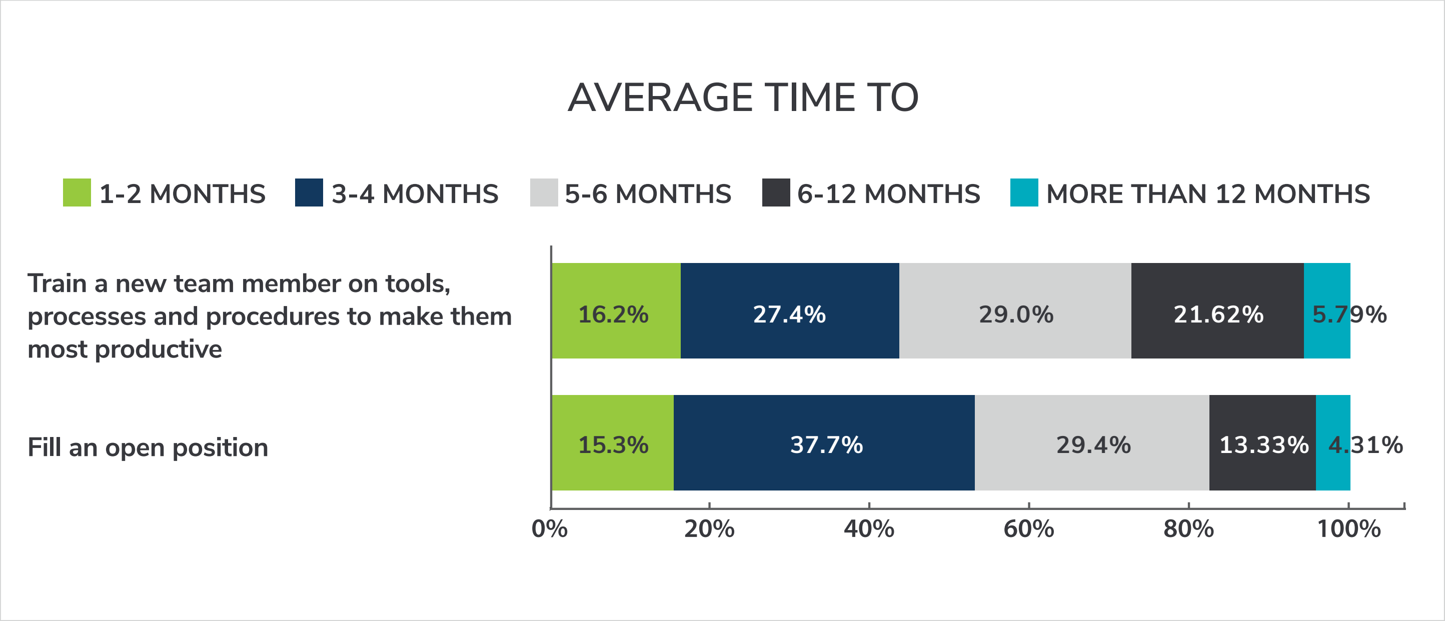


Figure 8

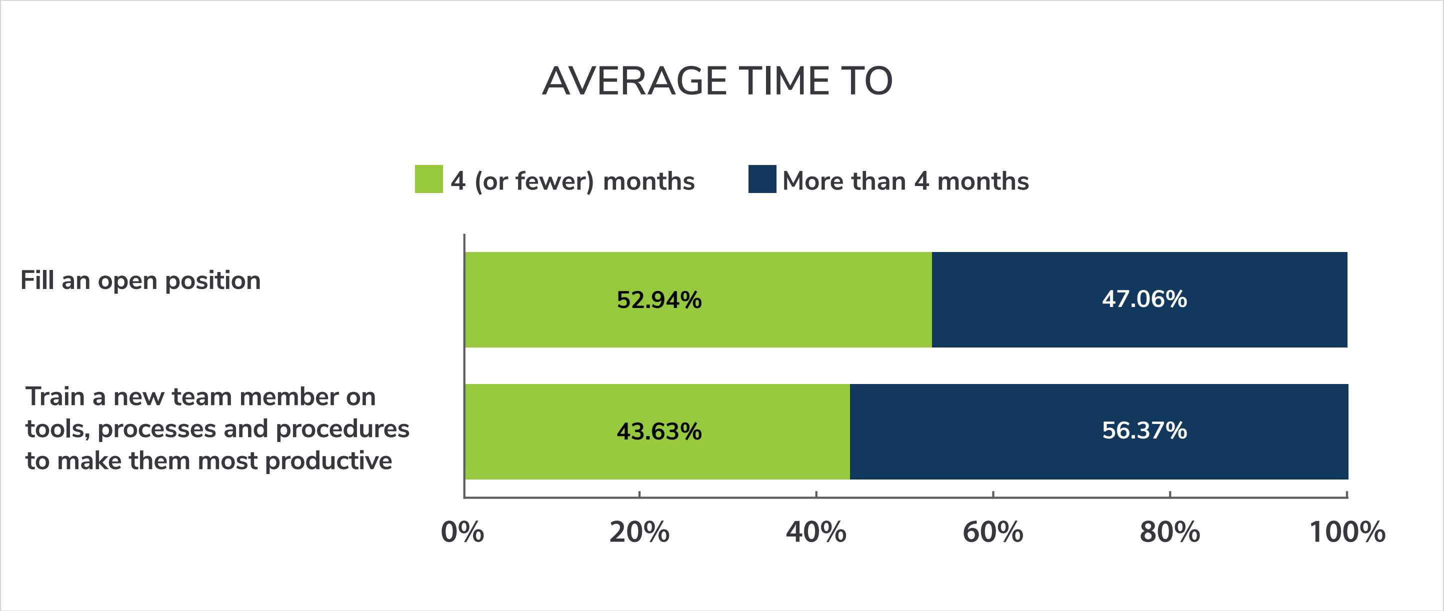


Figure 9

Almost half of our respondents said that **it takes more than 8 months to properly train a new team member**. When this figure is contrasted with low employee retention rates, it paints a picture of lost investment and time without requisite return.

Additional comments indicated a lack of employee experience in corporate culture which inhibited the training procedure, invariably extending it beyond conventionally 'normal' limits. As previously stated in this report, employers also expressed deep concerns when it came to employee experience, citing a discrepancy in 'on-paper' experience versus 'actual experience'.

4. The State of Security Orchestration

Security orchestration – the process of interweaving security tools, teams, and processes together for coordinated incident response – seeks to solve user pain points including product proliferation, unstructured processes, and swivel-chair investigations.

We asked respondents for their thoughts on orchestration drivers and security tool challenges to verify, validate, and evolve industry perception on their pain points and how orchestration can help bridge the gap.

ORCHESTRATION DRIVERS

To figure out which security tasks were the most mundane and distracting for information security staff, we asked them to select options from the list below:

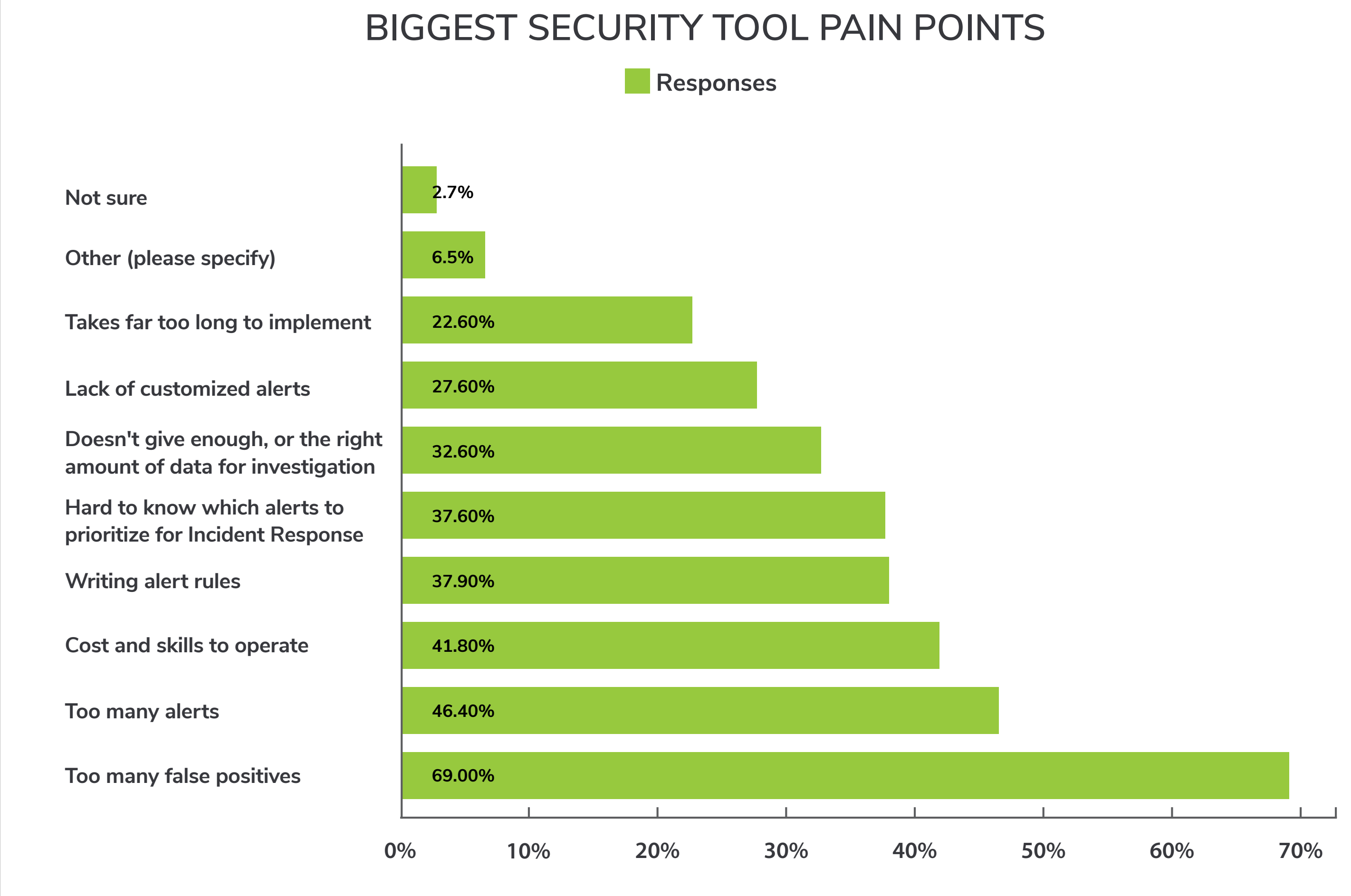


Figure 10

The results show most respondents concerned with the **high number of false positives**, followed by a concern with alert volume in general. This insight is concurrent with the 'tool sensitivity' debate that's gripping the security industry. If security tools are not sensitive enough, real and dangerous alerts can slip through the cracks and cause organizational havoc. To err on the side of caution, security tools are instead 'too sensitive' and spin up a multitude of alerts, enveloping security teams in false positives.

SOAR tools can mitigate this challenge through branching workflows that execute differing actions based on alert malice and seriousness, ensuring that security teams only investigate high-priority alerts and aren't mired in false positives.

STATE OF SECURITY TOOLS

In addition to gauging which pressing issues were affecting security teams, we also wanted to know how many security tools an analyst needed to learn for effective security operations and incident response.

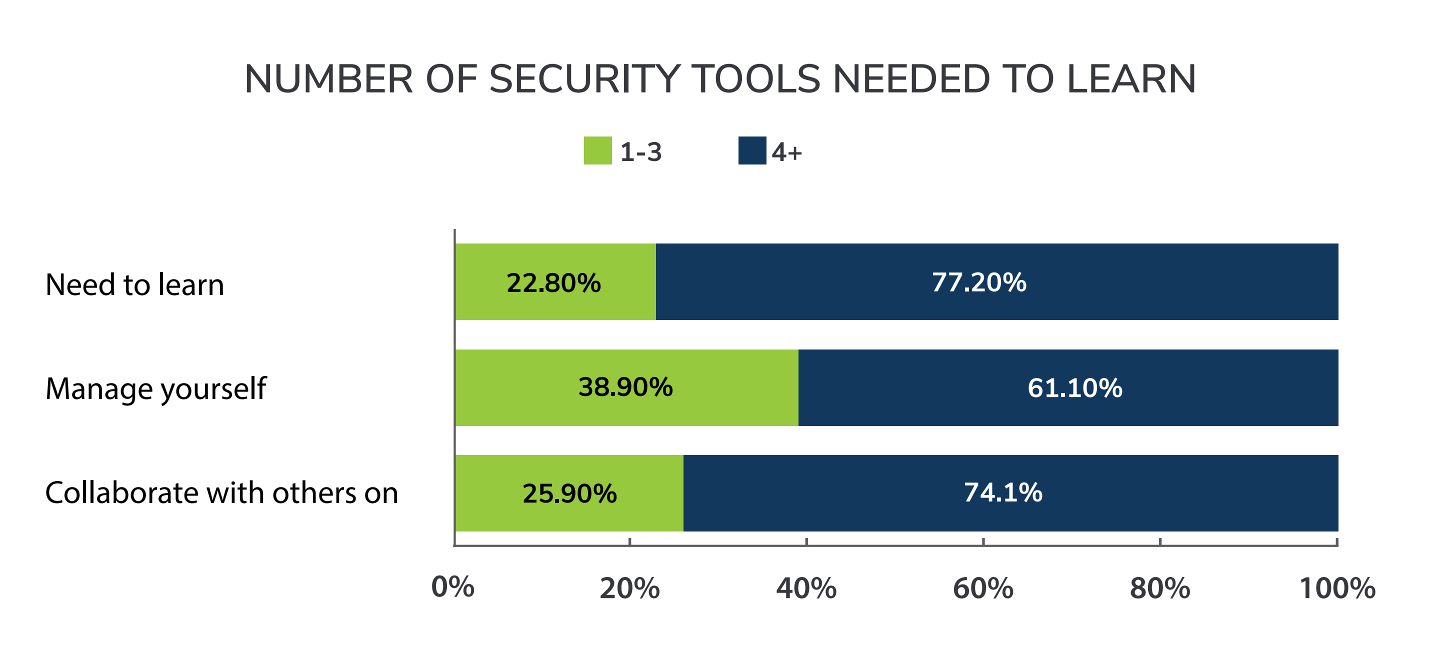


Figure 11

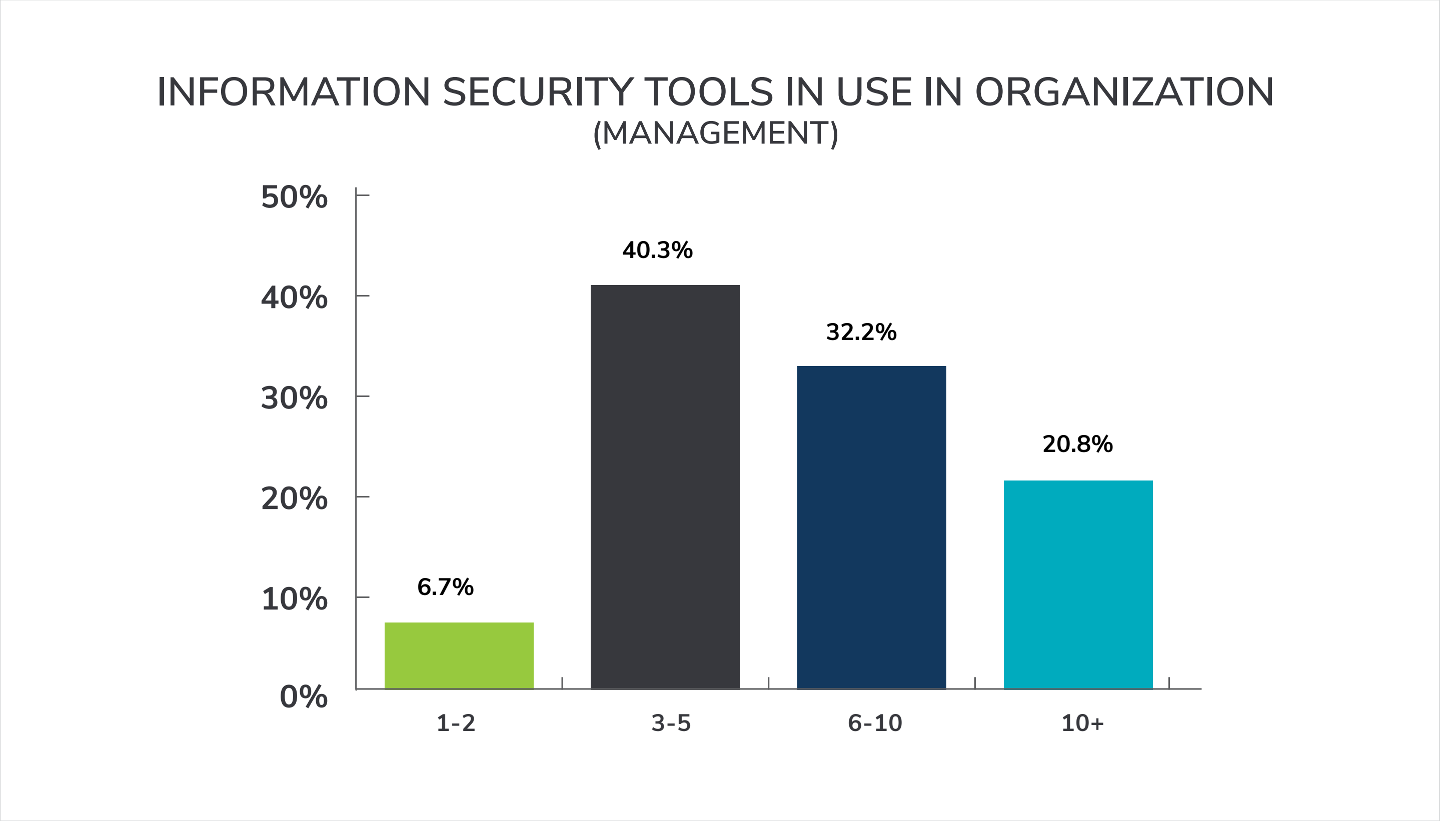


Figure 12

As we can see, there are plenty of tools to learn and many of these tools need to be personally managed. This result helps us contextualize the high training times needed for security analysts discussed earlier in this report. But with the number of tools constantly on the rise, high training times and attrition rates truly spell out the gravity of the human capital challenge facing the industry today.

5. The State of Security Automation

Automation has been one of the practices at the forefront of security innovation for a while. The two governing criteria while deciding upon candidates for automation are

1. How long the task takes, and
2. How often the task must be performed.

We sought to refine these initial thoughts and asked our respondents about incident loads, processes, and perceived automation benefits.

AUTOMATION DRIVERS

An important goal of our study was to find and validate linkages between high incident loads, high response teams, and the desire for automation. Thus, we asked respondents to give us a 'best guess' estimate on how many incidents they examined per week.

Tell us on average (whole numbers)

Answer Choices	Average Number
Number of alerts you review per week	12023.95
Number of alerts that occur per week in total	174956.36
Number of days to resolve an alert	4.34
Most weeks spent on a single alert in the last 2 years	5.99

Figure 13

These results indicate that information security staff are overwhelmed by the tasks at hand. The average number of alerts they review in on a weekly basis is roughly 12,024. This sobering statistic coupled with the fact that it **takes more than 4 days to resolve an alert** makes it clear that there's a vicious cycle in effect. Alert volume leads to increased MTTR which in turn leads to even more alert volume.

ARE SECURITY PROCESSES WELL DEFINED?

For automation to be successful, the tasks which the automation system takes over must be properly defined, preferably with sequential workflows. Defined processes are also important as a knowledge repository that security teams can both feed into and learn from.

To understand the extent to which processes were defined, we asked respondents about the tasks they felt would benefit most from automation.

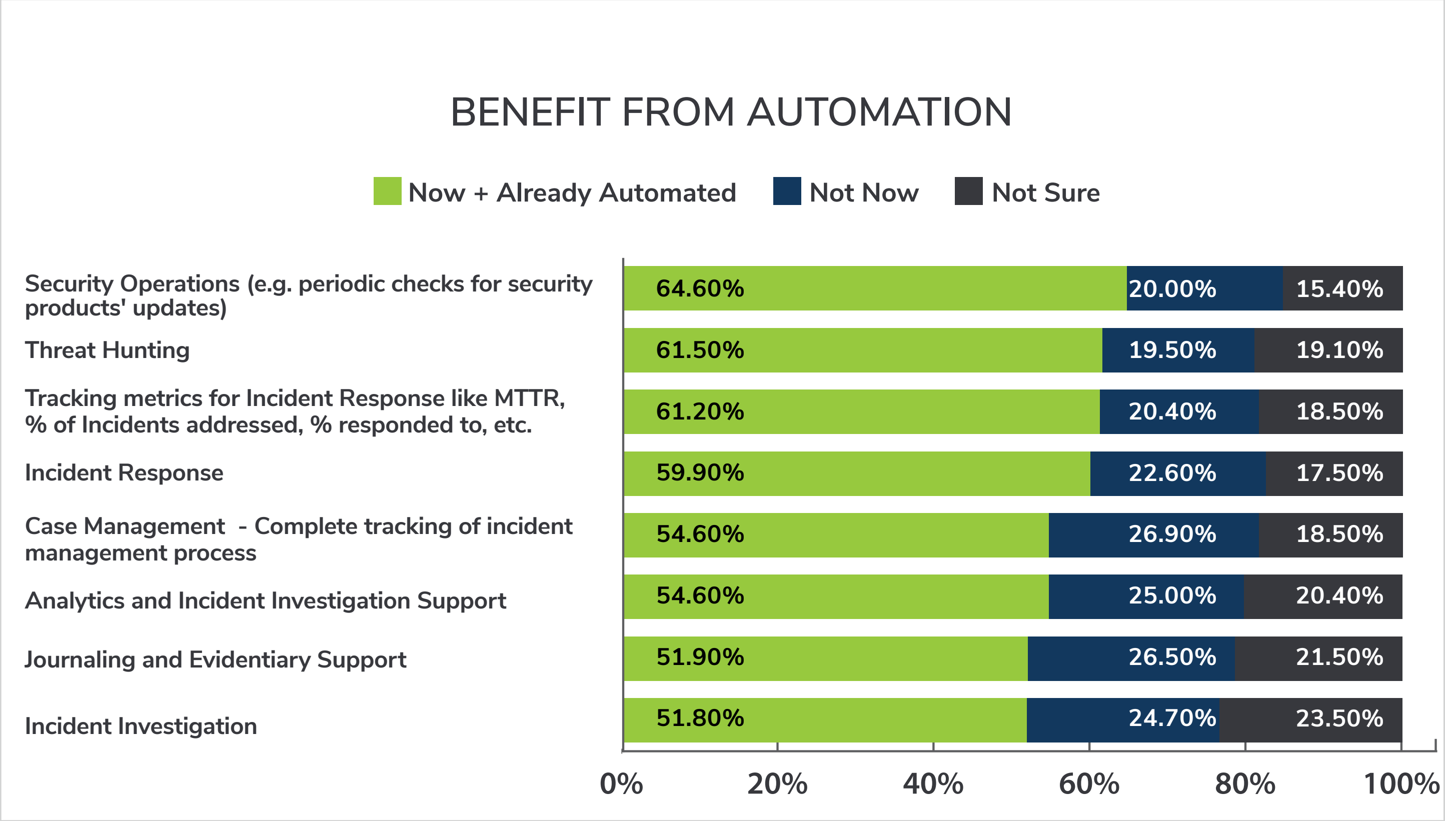


Figure 14

Results show a robust automation base (and a willingness to automate further) on both the proactive and reactive front. Proactively, security operations and threat hunting ranked high on the 'automation candidates' list, highlighting security teams' desire for automation to assist them in identifying incipient threats and vulnerabilities. Reactively, incident response, tracking IR metrics, and case management were felt as good candidates for partial or full automation.

PROCESS DOCUMENTATION: INCIDENT RESPONSE PLAYBOOK/RUNBOOK/PROCESSES

In addition to understanding what tasks should be automated, we also wanted clarity over documentation processes and whether they varied across security departments. The process of automation implies a degree of uniformity, and the presence of disparate documentation sources would make it that much more difficult to kickstart structured automation in a security department.

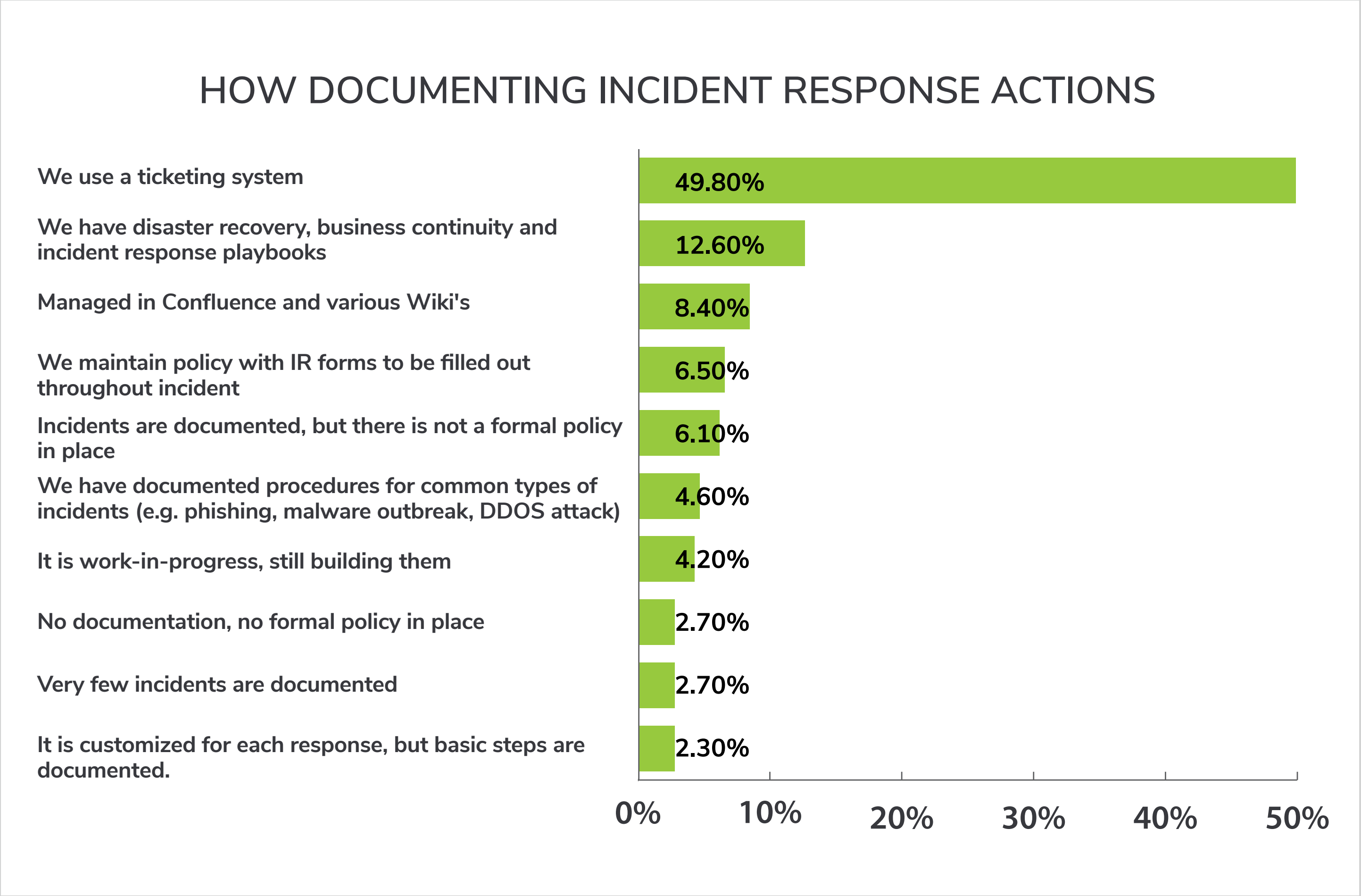


Figure 15

Our results show conclusive unanimity in this regard. Ticketing was by far the most popular documentation process followed by our respondents. Since ticketing systems often span across teams (IT, security, support, and so on), it makes sense for central documentation to occur on these platforms. A SOAR platform that integrates robustly with existing ticketing tools while providing its own ‘security documentation center’ would be a good start for automation and process definition.

However, an overreliance on ticketing platforms for security operations has its own problems, which we will cover later in the report.

PROCESS UPDATE FREQUENCY: INCIDENT RESPONSE PLAYBOOK/RUNBOOK/PROCESSES

One relatively overlooked side effect of the alert fatigue and day-to-day firefighting that security teams face is the stagnancy of security processes. When analysts are strapped for time, they find it difficult to capture the gaps in current processes and update them on an ongoing basis.

We wanted to see if this hypothesis rang true with our respondent base and asked them about the frequency with which they updated their incident response processes.

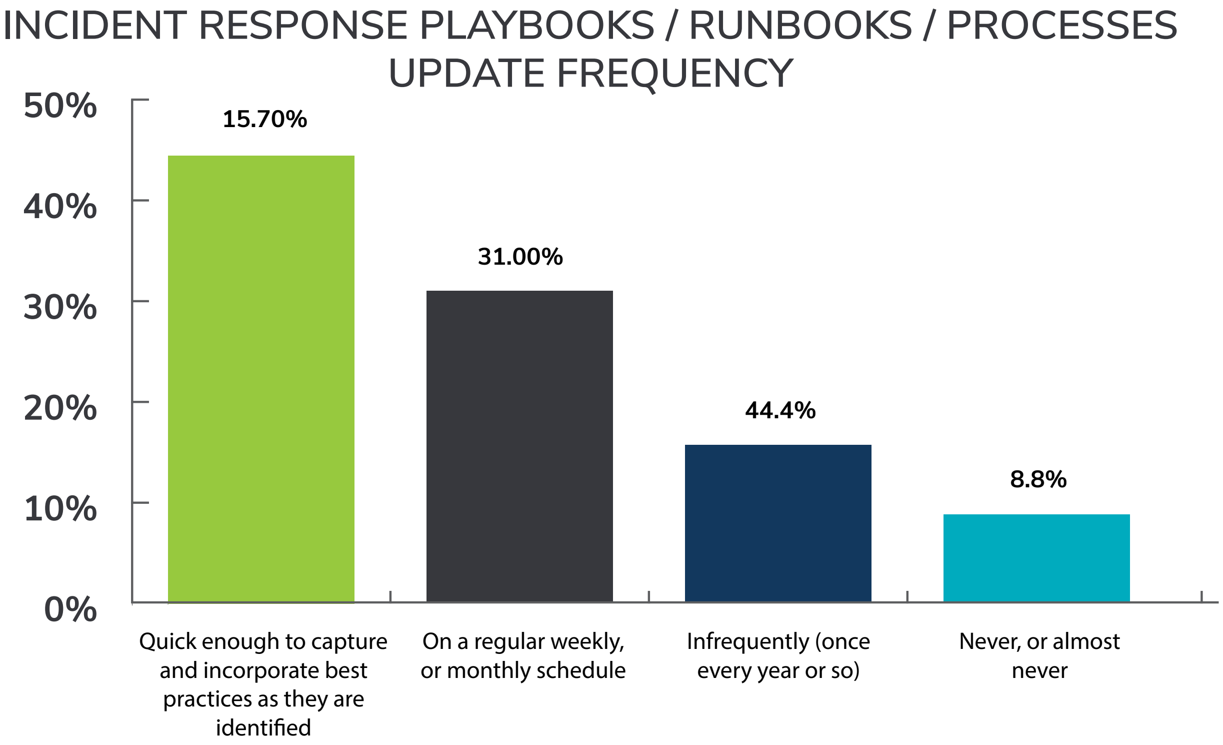


Figure 16

Results show that over **50% of respondents either didn't update IR processes at all or updated them infrequently**. SOAR platforms will not only improve process speed through automation, but also enable the iterative improvement of processes through proper metric capturing and visibility of process gaps and potential improvements.

6. The State of Incident Management

Currently, incident management is done almost exclusively by people. While it's important for teams to retain control over incident management, this task becomes tougher with a wider geographical dispersion of teams. To verify the extent of personnel dispersal, we asked respondents whether their IR function was in-house/outsourced and centrally located/distributed.

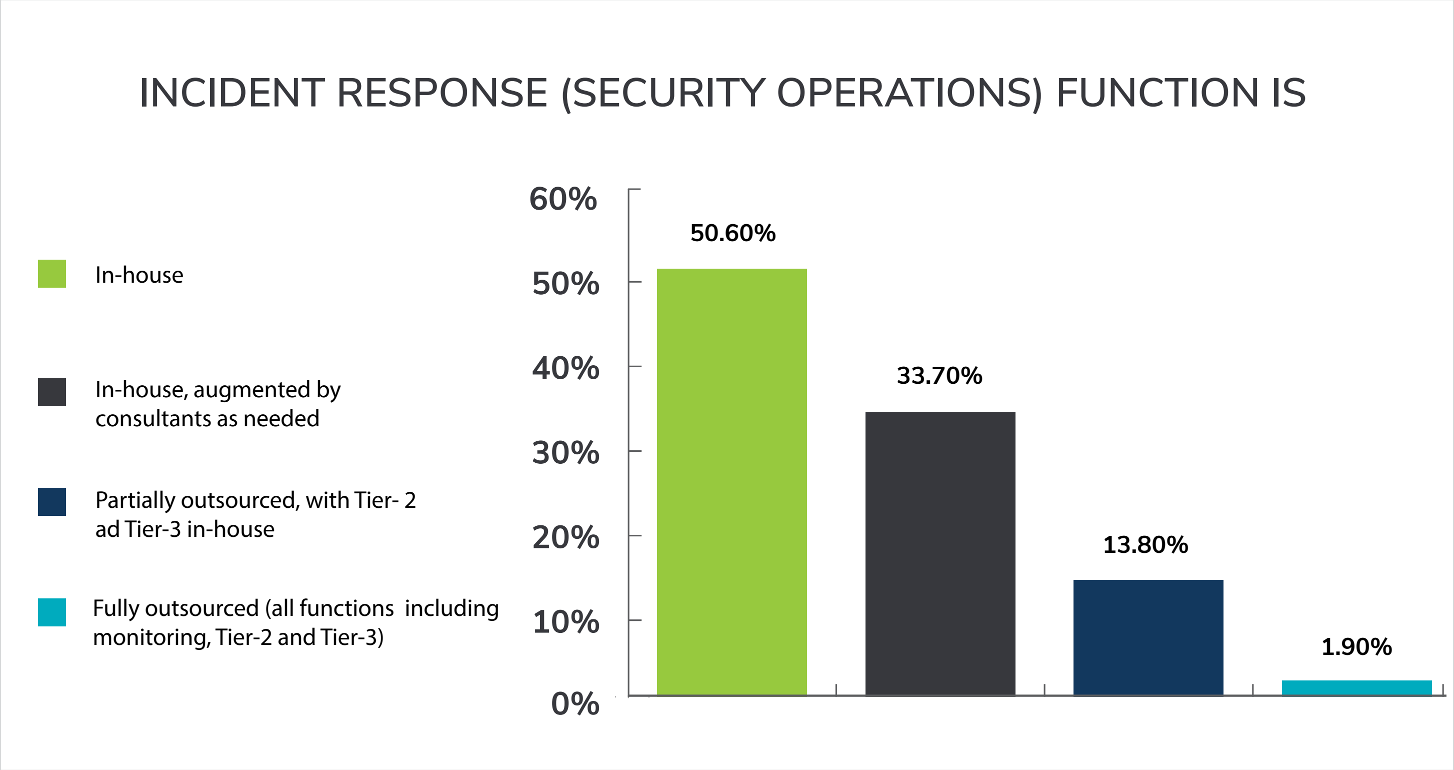


Figure 17

Although 84% of respondents stated that their IR functions were largely in-house, those in-house teams seem to be widely dispersed both nationally and internationally. Around 68% of respondents had security teams either dispersed across locations in one country or observing a Follow-the-Sun model across multiple countries.

Whether it's due to scale, labor pressures, or the need for customer proximity, security teams are dispersed. This dispersal makes it much harder to conduct unified incident management.

In the following sections, we will go through various components of incident management and discuss what our research insights project for these practices.

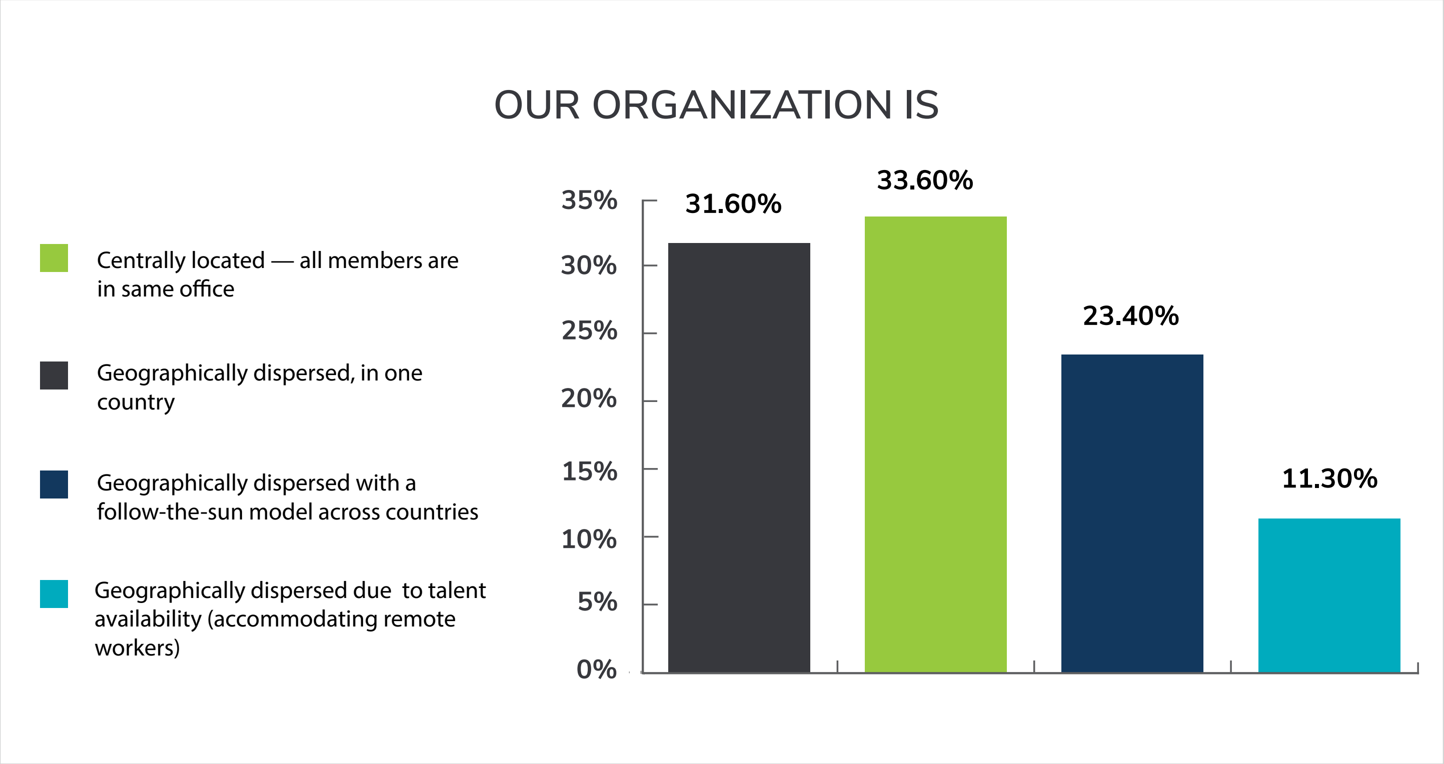


Figure 18

ALERT PROCESSING AND TRIAGE

Research results conclusively convey the trouble security teams have with processing and contextualizing alerts. From simple alert volume and resolution stats (Figure 13) to false positive concerns (Figure 10), the state of today's threat landscape has resulted in a proliferation of alerts that are tough to prioritize in a timely manner.

JOURNALING AND EVIDENTIARY SUPPORT

From the insights we have in the report so far, we can infer that security teams are dispersed and use a variety of security tools to conduct incident response. This presents a problem during evidence collection and post-incident documentation. Consider the following cases:

- An attack campaign manifests over a long period of time and records of what took place are lost or only faintly remembered by a few people.
- There are multiple security analysts working on the same incident.
- Incidents involve multiple teams. For instance, if an incident involves a data breach of personal information, regulatory mandates require that breach notifications are sent out to affected individuals.

None of the above cases can be resolved successfully at scale using the current incident management setup that organizations possess.

CASE MANAGEMENT AND WORKFLOW

Our research shows two main challenges with existing case management and workflows.

Firstly, over 50% of our respondents stated that they rarely updated processes (Figure 16), highlighting a lack of both analyst time and process intelligence to make updates happen.

Secondly, most respondents use ticketing platforms to document incident response actions (Figure 15). Since ticketing platforms are designed to be 'static' and capture moment-in-time comments and flows, it prevents the dynamic, fast workflow changes that are necessary in the face of sophisticated attacks.

In our view, SOAR platforms should be capable of both integrating with third-party ticketing tools, as well as providing their own, more modular and flexible case management that's better suited to security use cases.

MANAGEMENT OF THREAT INTELLIGENCE

Threat intelligence tools form a vital cog in the wheel of incident response and security operations. Our research found a healthy mix of respondents using open-source and commercially available tools. With each TIP providing a unique slice and perspective on threat data, it becomes critical to have an action hub that can aggregate data from different third-party sources for central visibility and informed response.

SOAR tools are uniquely placed to leverage multiple threat intelligence platforms (both open-source and commercially available), aggregate indicator reputation, and provide security teams with the means to drive threat data to action.

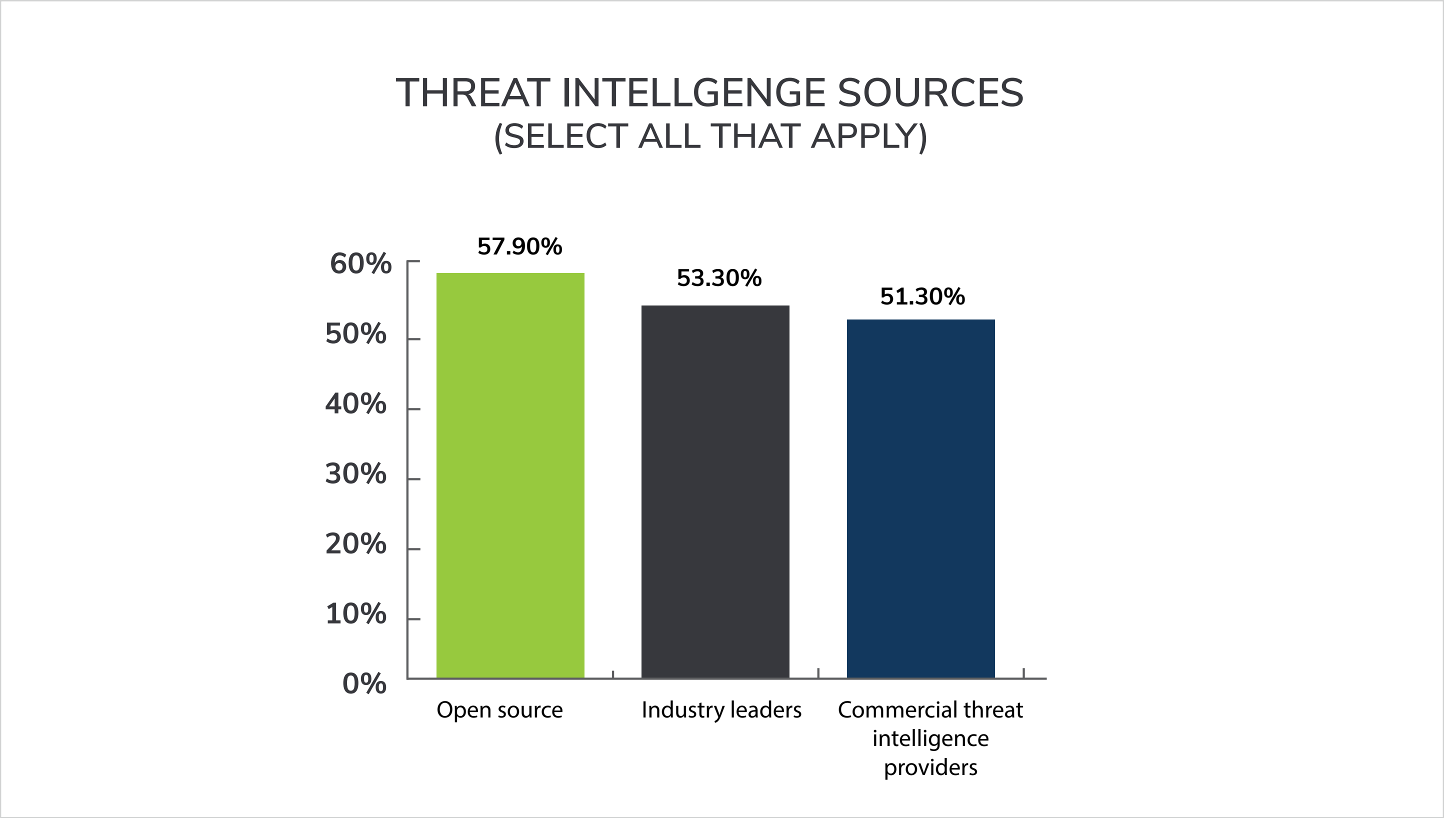

THREAT INTELLGENGE SOURCES
(SELECT ALL THAT APPLY)
60%
50%
40%
30%
20%
10%
0%
57.90%
53.30%
51.30%
Open source
Industry leaders
Commercial threat intelligence providers

Figure 19

7. The State of SOAR Budgets and Measurement

To get a better grasp of SOAR's acceptance among its potential user base, we aimed to find out more information about the measurement of security metrics as well as any budgetary exclusivity assigned to SOAR tools by executives.

SOC METRICS: MEASURING RESULTS

Measuring security results is the cornerstone upon which future improvements are actioned. With this in mind, we asked respondents what metrics they usually measured during incident response.

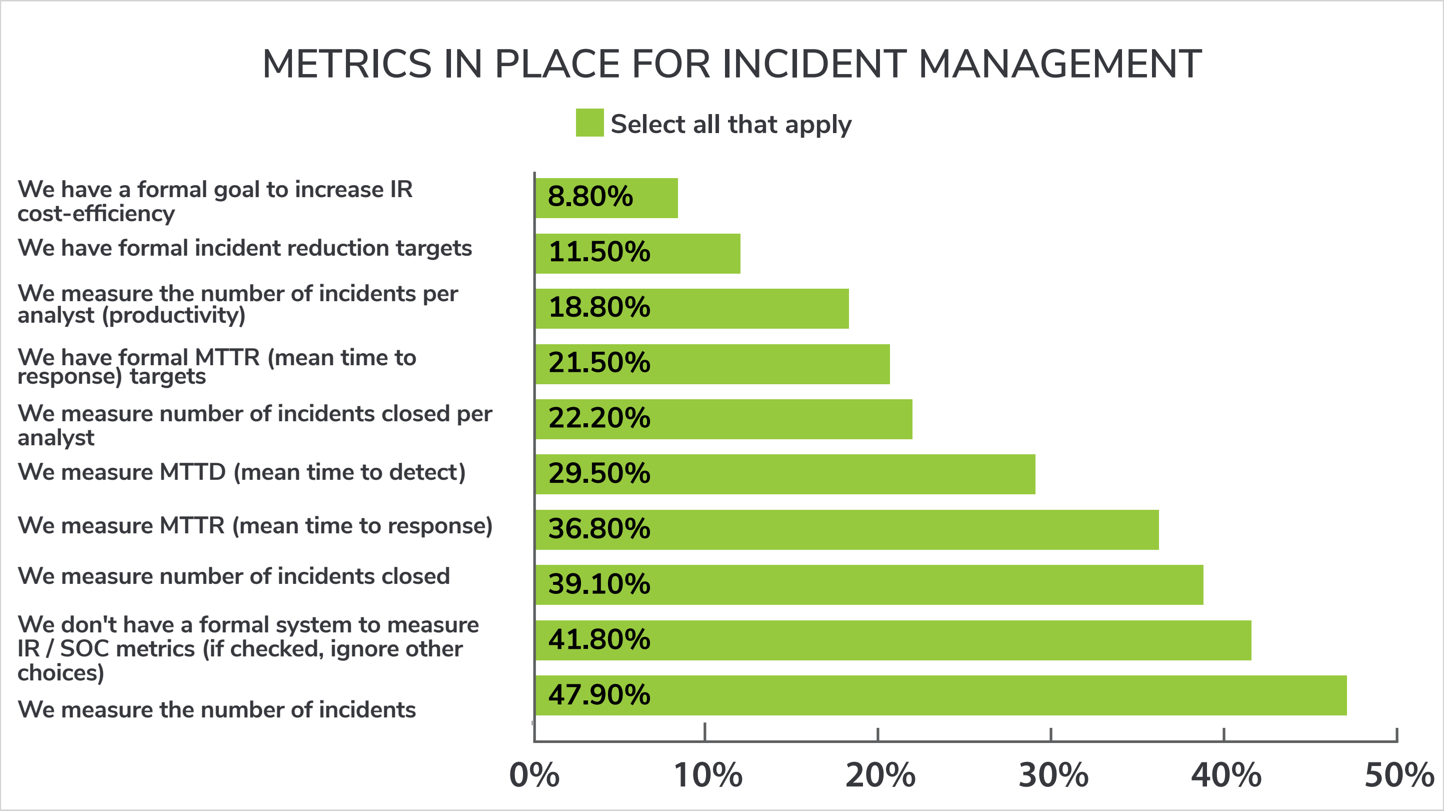


Figure 20

Results show either a lack of formal measurement or rudimentary measurement of incident metrics. Around 48% of respondents stated that they measured the number of incidents, which is a good start but not an ideal end state for SOC efficiency measurement.

Close to **42% of respondents cited that they didn't have a formal system to measure security metrics at all**; this fact, when coupled with increasing alert volume, leads to a dangerous 'double whammy'. Not only are teams inundated with alerts, but they're also unable to verify the accuracy and efficacy of their response to those alerts.

SOC BUDGET: WHAT ARE THEY SPENDING ON

Usually, a security industry or segment being assigned its own budget line is a strong indicator of maturity. We wanted to find out if SOAR tools had their own budgetary allotments and, if not, what other security concerns they had to compete with.

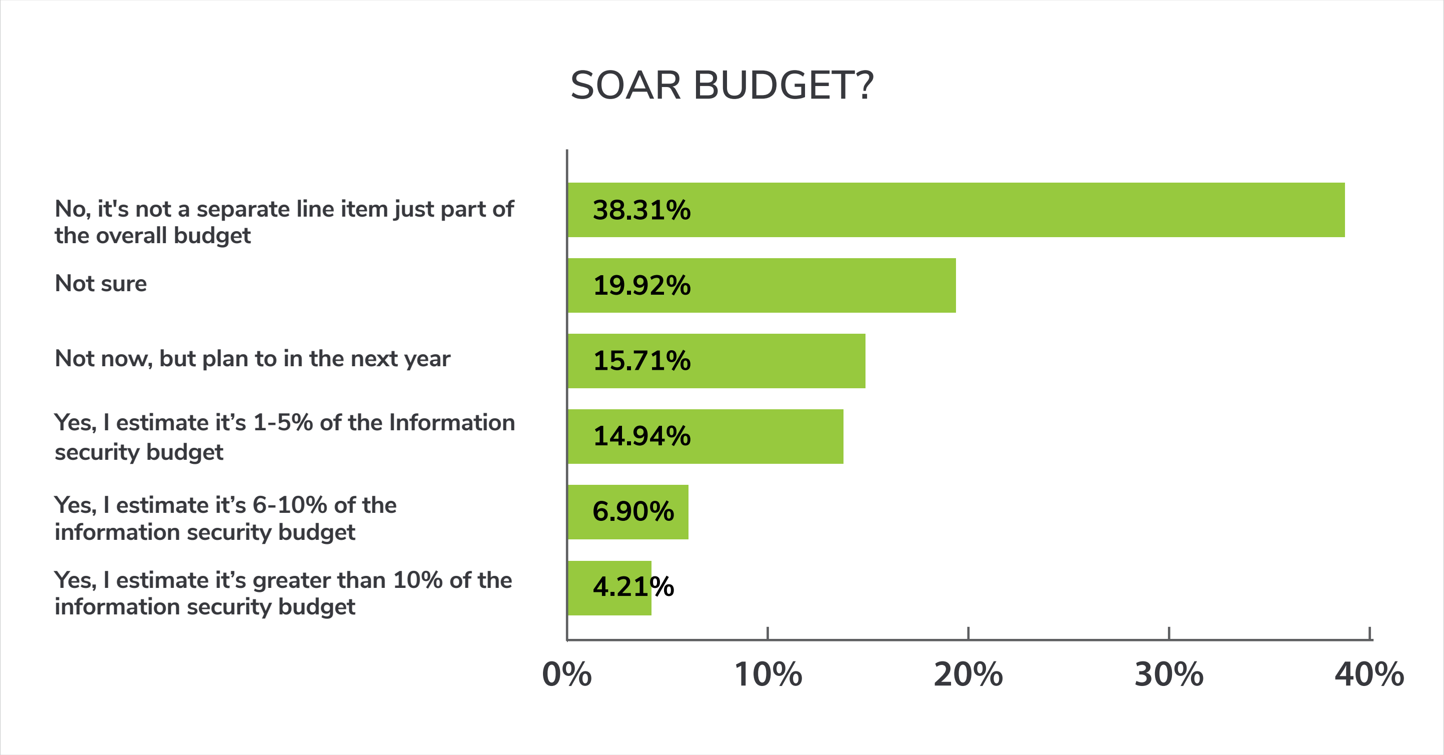


Figure 21

Results show that the SOAR space is not mature enough to demand its own budget line, but it's growing at an appreciable pace. Around 38% of respondents stated that, while SOAR tools didn't have a dedicated budget, they were a part of the overall security budget. A further 15% of respondents projected to including SOAR tools in their budgets the following year.

A sign of SOAR's emergent nature is highlighted by around 20% of our responders being unsure about where to include SOAR in their budgets. A growing acknowledgement of SOAR in security budgets will come with increased awareness and continued verifiable benefits in existing SOAR deployments.

8. SOAR Benefits

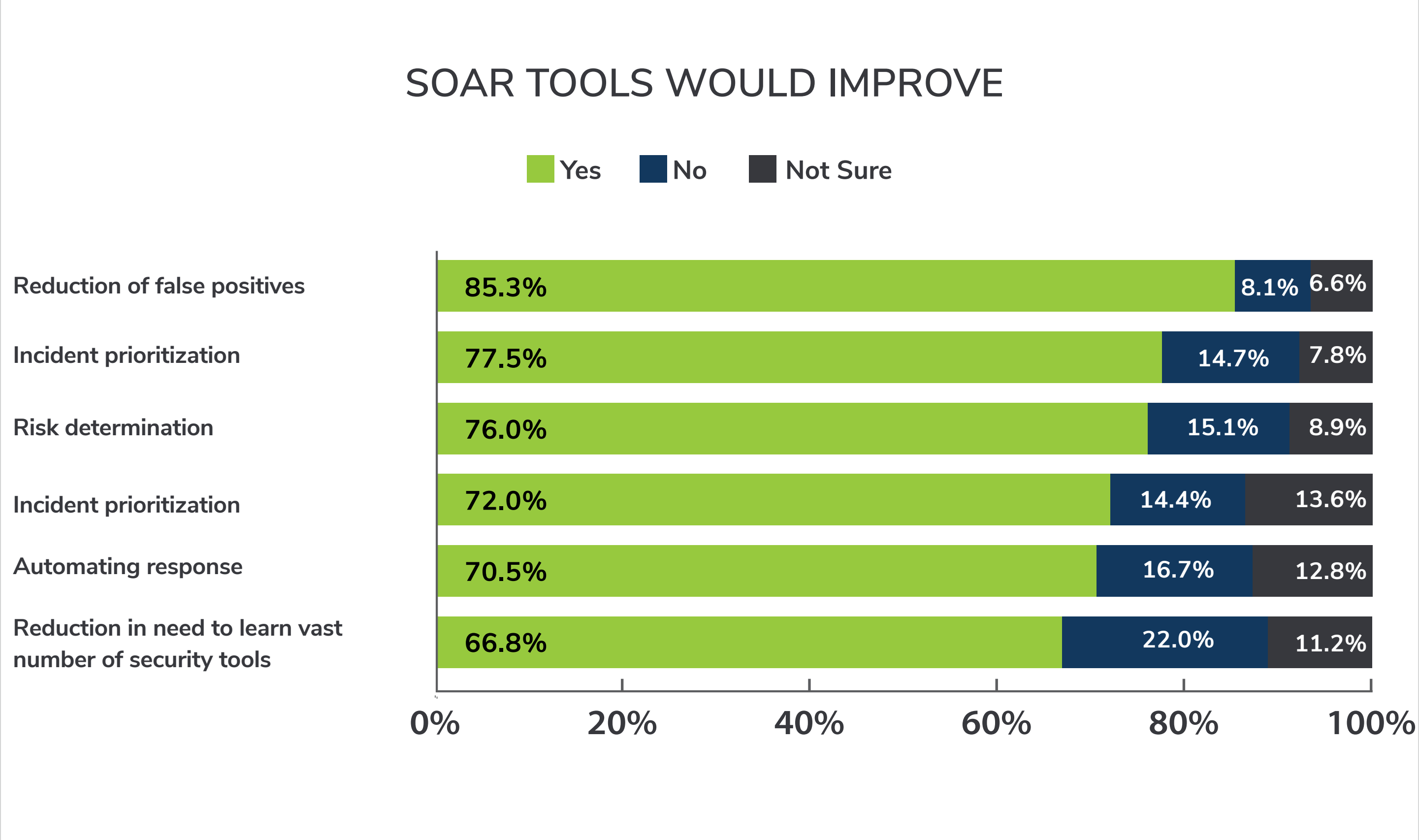


Figure 22

When asked about challenges that SOAR tools could help solve, respondents addressed applications in multiple fields.

- **Alert triage:** Respondents cited 'reduction of false positives', 'identification and classification of threats', 'risk determination', and 'incident prioritization' as major areas where SOAR tools could help. SOAR tools that ingest alerts from multiple sources and automate enrichment and triage rules across products will help alleviate the 'context chaos' currently engulfing security teams.
- **Faster response:** Around 70% of respondents stated that SOAR tools would be beneficial in 'automating response'. For simpler use cases, security teams can use SOAR playbooks to automate repeatable steps and achieve quick resolution. For complex use cases, playbooks can include manual checks and balances that give the analysts final control.
- **Tool coordination:** Around 69% of respondents cited a 'reduction in need to learn vast number of security tools' as a benefit of SOAR deployment. While learning more tools is always helpful for personal development, SOAR platforms can prevent the necessity to manually perform 'basic' but important tasks hundreds of times per day.

9. A Look Into the Future

SOAR APPLICATIONS

As SOAR tools continue to gain market acceptance, their functionalities and use cases will grow. Currently, based on our industry knowledge and research results, we posit the following applications of SOAR tools:

- **Proactive threat hunting:** Since threat hunting usually requires analysts to rapidly coordinate among multiple security tools, it presents a great opportunity for orchestration with immediate impact. SOAR tools can enable security teams to ingest third-party threat feeds and automate 'search and destroy' workflows that scan for potential vulnerabilities across environments.
- **Standardize and iterate incident processes:** It's vital for security teams to minimize 'quality variance' in incident management and response. SOAR workflows are a great first step in this direction, allowing for partial/full codification of best-practice processes and guaranteeing that security analysts don't have to start from scratch each time they encounter a specific incident. With deployment maturity, SOAR tools will also allow teams to quickly iterate upon these processes by spotting gaps and areas for improvement.
- **Improve investigation quality:** Multiple data points in this report suggest that security teams struggle with gathering incident context and leveraging full visibility of data at their disposal. SOAR tools can help improve investigation quality by enabling faster resolution of false positives, prioritizing incidents and risk through correlated information from multiple tools, and freeing up analyst time by obviating the need to learn the detailed vernacular of many security products.
- **Accelerate and scale incident response:** SOAR offers coordinated automation to an industry that is currently beset by important but repeatable, high-quantity tasks. SOAR tools allow SOCs to rely on automation for the grunt-work and leverage rich, correlated information for decision-making and investigation.
- **Security operations and maintenance:** In addition to automating repetitive response tasks, SOAR tools can also help security teams simplify system checks, maintenance, upgrades, and general security operations. These practices rely on workflows as much (if not more) than response does, and standardized, automated execution will increase accuracy and better plug gaps that leave systems vulnerable.

MAIN DISRUPTOR: MACHINE LEARNING

As with any industry, the growing maturity of SOAR tools will result in a baseline of features that all major solutions in the space will be expected to provide. With clear product differentiators expected to diminish with time, machine learning will emerge as a critical facet through which end users can separate out the leading SOAR products from the rest.

Considering the results of this report and existing industry knowledge, we posit that machine learning sits at the intersection of solving many problems faced by security teams today. Robust machine learning algorithms, if fed with relevant data, can:

- **Simplify workflows:** Machine learning can keep SOAR playbooks/workflows on a path of constant improvement by suggesting ways to shorten task block and identifying manual playbooks that are prime candidates for automation.
- **Increase responder productivity:** Historical readings of incident resolution times can enable machine learning to match effective analysts with specific incident types and guide those analysts with best-practice action sets to resolve incidents that have been seen in the past.
- **Improve campaign visibility:** Machine learning algorithms applied to incident and indicator data can provide analysts with actionable context such as related incidents within an attack campaign, duplicate incidents across user environments, and indicator reputation scores aggregated across multiple third-party tools.
- **Provide organic training and upskilling:** Senior analysts are currently too busy to train/onboard junior analysts effectively, which results in the possibility of mistakes on the job and sub-optimal IR quality at the outset. Machine learning, coupled with SOAR workflows, can provide an effective conduit for ‘on-the-job’ learning. Junior analysts will be able to view workflows and realize the best-practices that need to be followed for different incident types. Security command and security expert suggestions can also help them better chart out response routines and find help during difficult investigations.

10. Who we surveyed

To enumerate the depth and breadth of our study, we wanted to document the broad demographics of our respondents. These details include company size, company location, and job roles.

COMPANY SIZE

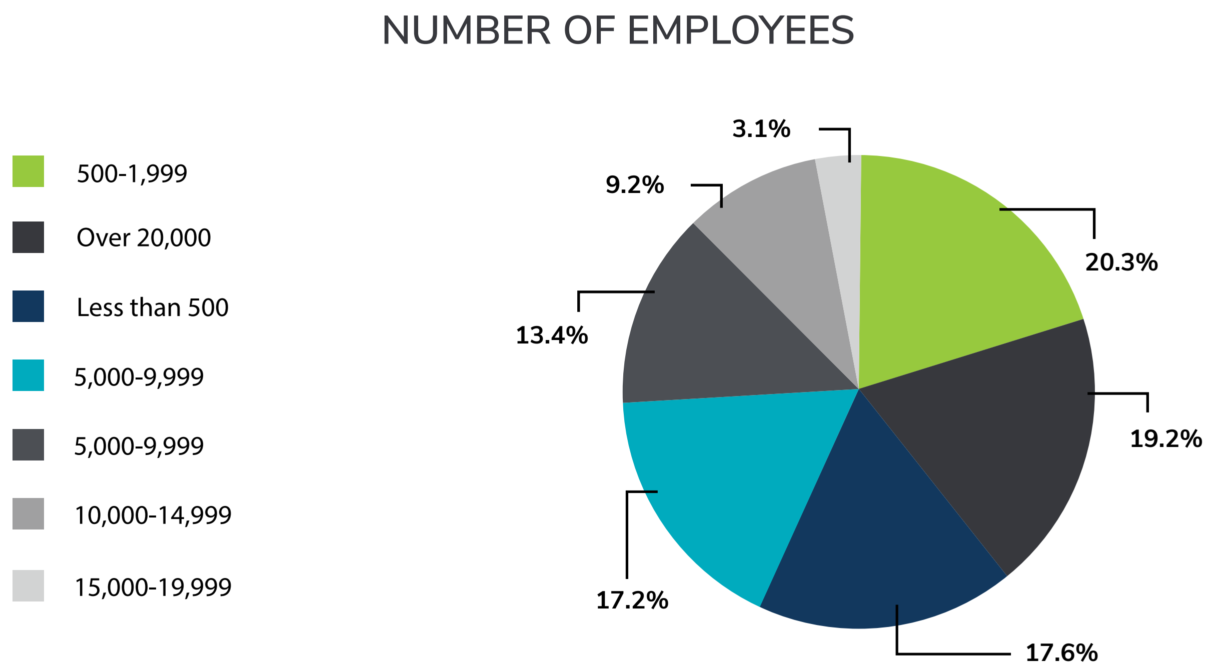


Figure 23

We tried to maintain an appropriate dispersion of businesses sizes to cater results and insights to the widest possible user base. As can be seen from the results, we were able to represent a wide variety of businesses and avoid any biases resulting from niche, insulated samples.

RESPONDENT INFORMATION

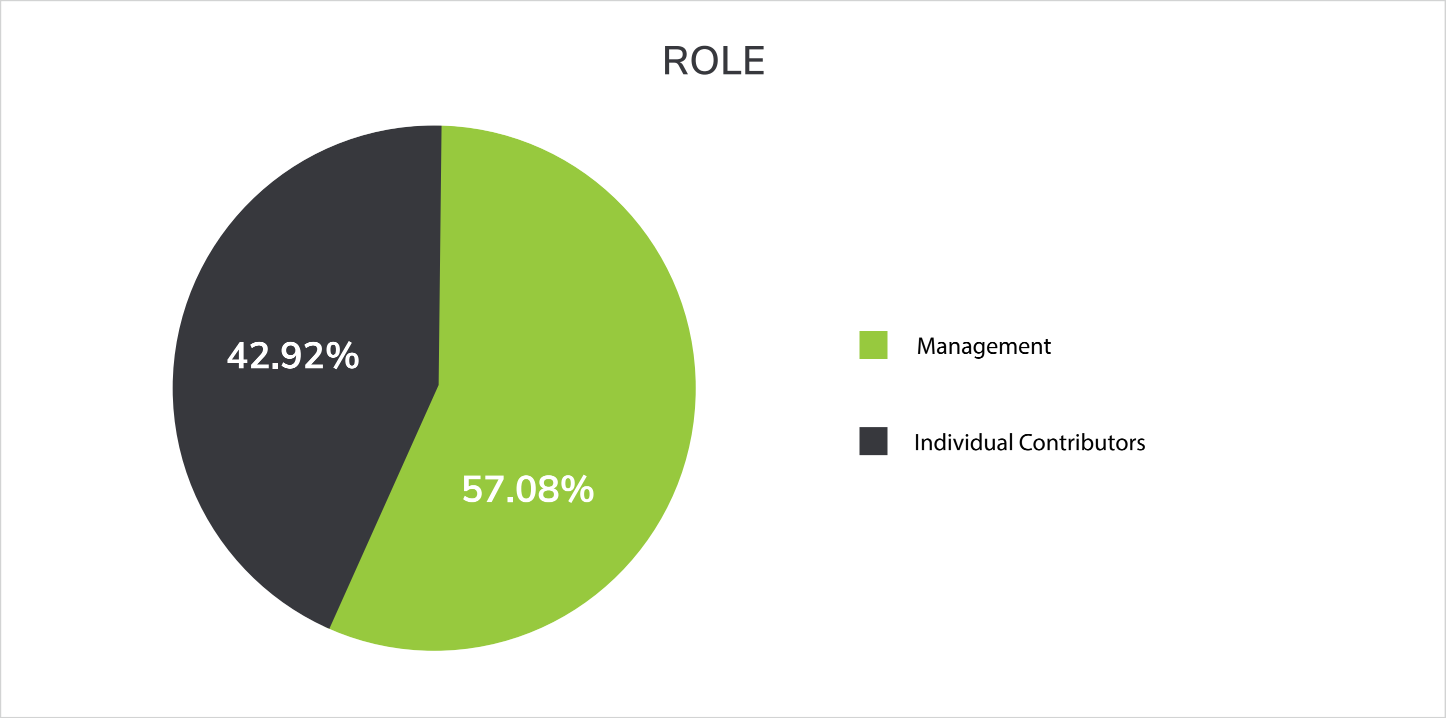


Figure 24

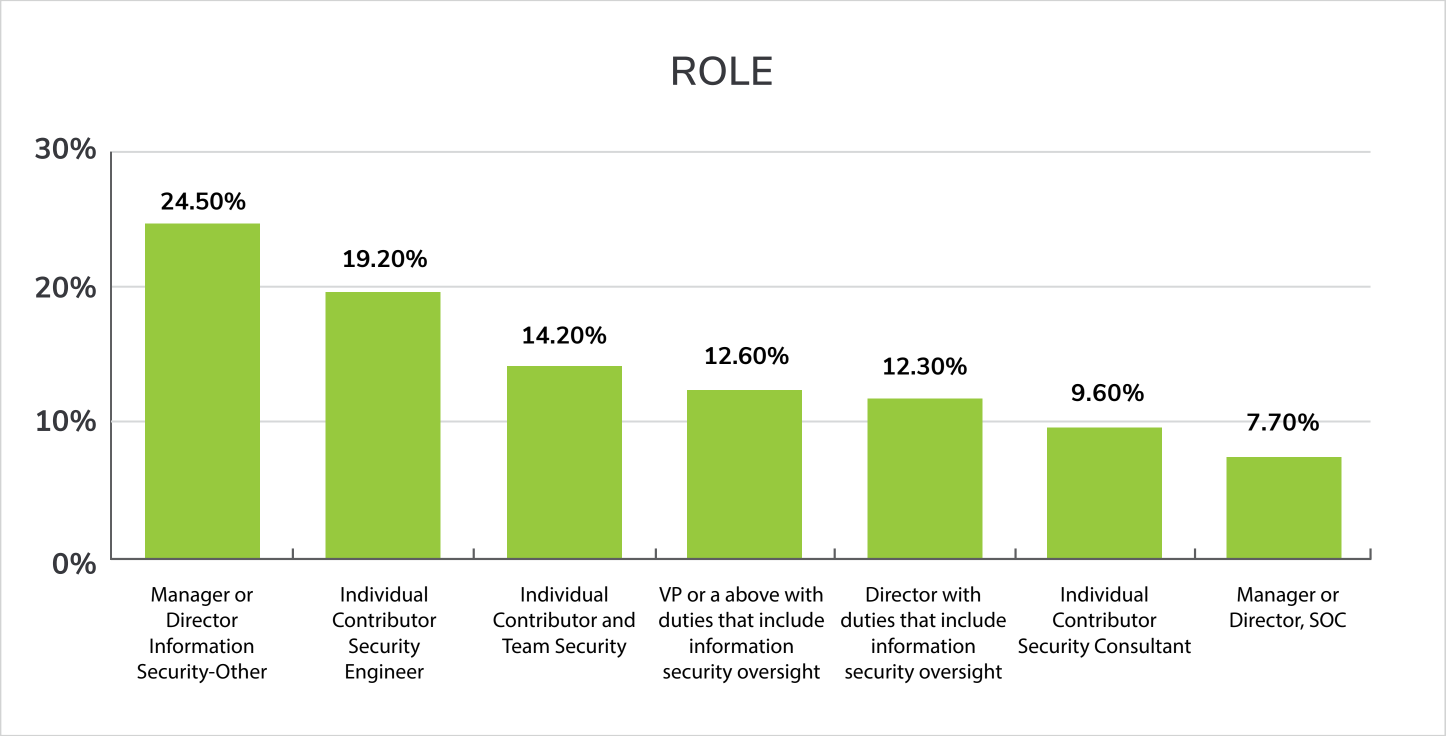


Figure 25

We wanted to get the perspective of both employees and managers and tried to represent the opinions of both sets in this research. Like any industry, cybersecurity is reliant on both the strategic vision of managers and the tactical execution of employees, and the report managed to represent a healthy spread across this aisle.

COMPANY LOCATION

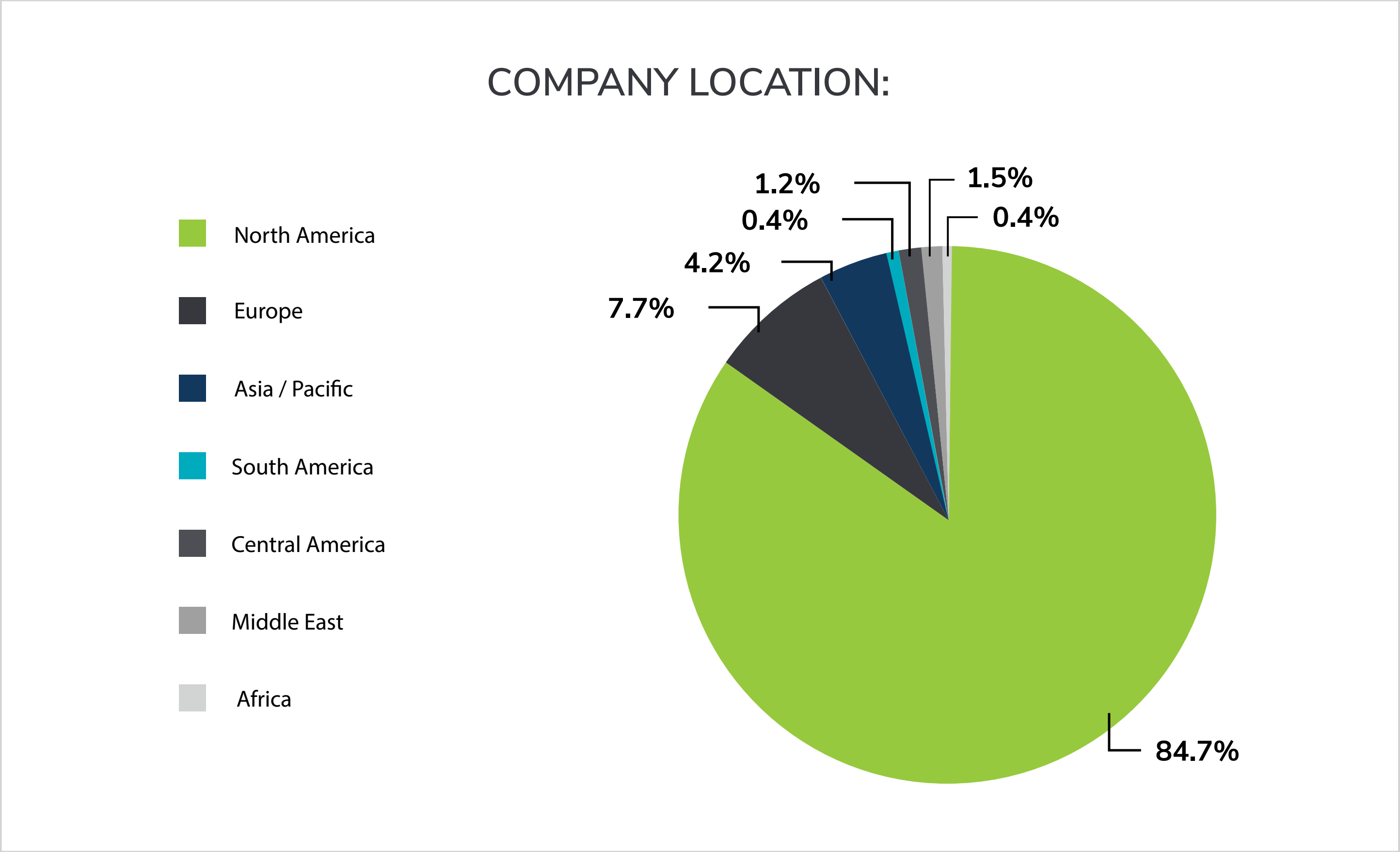


Figure 26

We wanted to have an international respondent spread in our research if possible and avoid any locational biases in responses. Our respondents ended up being mainly from North America. We conceded that responses might be 'localized' as a result, but considering that North America is one of the forerunners in terms of information security, we hope the results and insights from this report provide value to readers across the globe.