Improving the Effectiveness of the Security Operations Center

Sponsored by Devo Technology

Independently conducted by Ponemon Institute LLC

Publication Date: June 2019

Improving the Effectiveness of the Security Operations Center

Presented by Ponemon Institute, June 2019

Part 1. Executive summary

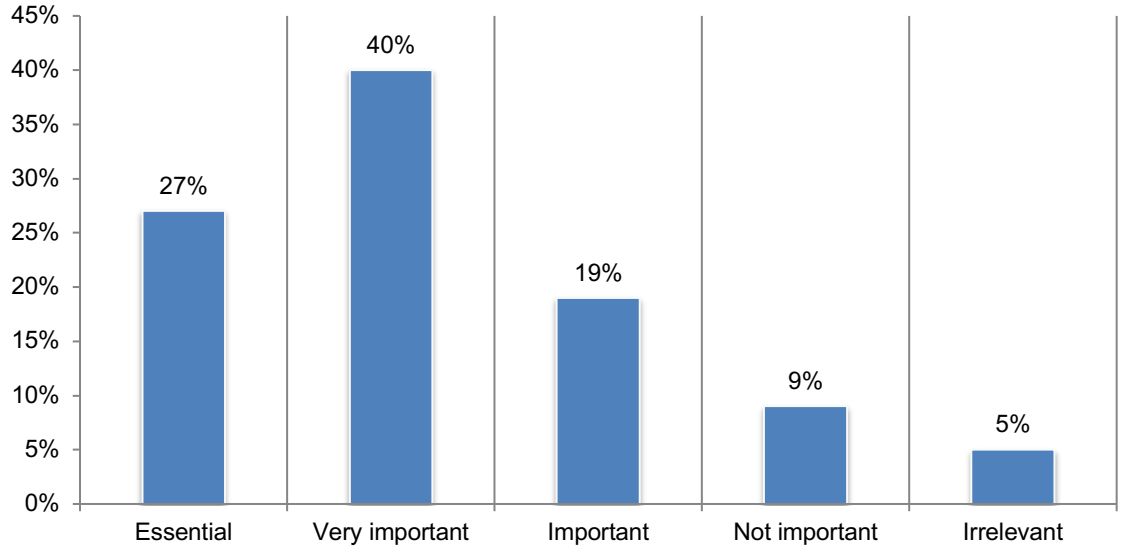
Security Operations Centers (SOC) are an increasingly important part of organizations' efforts to keep ahead of the latest cybersecurity threats. However, for a variety of reasons revealed in this research, organizations are frustrated with their SOC's lack of effectiveness in detecting attacks.

A SOC is defined as a team of expert individuals and the facility in which they work to prevent, detect, analyze and respond to cybersecurity incidents. Critical to the SOC's success is support from the organization's senior leaders, investment in technologies, and the ability to hire and retain a highly skilled and motivated team. The purpose of this research is to understand the barriers and challenges to having an effective SOC and what steps can be taken improve its performance.

Sponsored by Devo Technology, Ponemon Institute surveyed 554 IT and IT security practitioners in organizations that have a SOC and are knowledgeable about cybersecurity practices in their organizations. Their primary tasks are implementing technologies, patching vulnerabilities, investigating threats and assessing risks.

While respondents consider the SOC as essential or important, as shown in Figure 1, most respondents rate their SOC's effectiveness as low and almost half say it is not fully aligned with business needs. Problems such as a lack of visibility into the network and IT infrastructure, a lack of confidence in the ability to find threats and workplace stress on the SOC team are diminishing its effectiveness.

Figure 1. How important is your organization's SOC to its overall cybersecurity strategy?



The following findings reveal why organizations have SOC frustration

- The visibility problem: The top barrier to SOC success, according to 65 percent of respondents, is the lack of visibility into the IT security infrastructure and the top reason for SOC ineffectiveness, according to 69 percent, is lack of visibility into network traffic.

- The threat hunting problem: Threat hunting teams have a difficult time identifying threats because they have too many IOCs to track, too much internal traffic to compare against

IOCs, lack of internal resources and expertise and too many false positives. More than half of respondents (53 percent) rate their SOC's ability to gather evidence, investigate and find the source of threats as ineffective. The primary reasons are limited visibility into the network traffic, lack of timely remediation, complexity and too many false positives.

- The interoperability problem: SOCs do not have high interoperability with the organization's security intelligence tools. Other challenges are the inability to have incident response services that can be deployed quickly and include attack mitigation and forensic investigation services.

- The alignment problem: SOCs are not aligned or only partially aligned with business needs, which makes it difficult to gain senior leadership's support and commitment to providing adequate funding for investments in technologies and staffing. Further, the SOC budget is inadequate to support the necessary staffing, resources, and investment in technologies. On average, less than one-third of the IT security budget is used to fund the SOC and only four percent of respondents say more than 50 percent of the cybersecurity budget will be allocated to the SOC.

- The problem of SOC analyst pain: IT security personnel say working in the SOC is painful because of an increasing workload and being on call 24/7/365. The lack of visibility in to the network and IT infrastructure and current threat hunting processes also contribute to the stress of working in the SOC. As a result, 65 percent say these pain factors would have caused them to consider changing careers or leave their job and many respondents say their organizations are losing experienced security analysts to other careers or companies.

- As a result of these problems, the mean time to resolution (MTTR) can be months. Only 22 percent of respondents say resolution can occur within hours or days. Forty-two percent of respondents say the average time to resolve is months or years.

Following are other insights from the research.

- Organizations are shifting to the cloud. Fifty-three percent of respondents say what best defines the IT infrastructure that houses their SOC is mostly cloud (29 percent) or a combination of cloud and on-premises. Forty-seven percent of respondents say it is on-premise.

- The majority of respondents (51 percent) say their companies invest in threat intelligence feeds. Of these organizations, 54 percent of respondents say the threat intelligence feeds combine open source and paid feeds. Sixty percent of respondents in organizations that invest in threat intelligence feeds develop custom feeds based on a technology profile. Twenty-eight percent of respondents say their organizations do not develop custom feeds.

- The exploits most commonly identified by the SOC are malware attacks, exploits of existing or known vulnerabilities, spear phishing and malicious insiders.

- Monitored or managed firewalls and intrusion prevention systems and intrusion detection systems are most often deployed within the SOC environment. Other services include managed vulnerability scanning of networks, servers, databases or applications and monitored or managed multifunction firewalls or unified threat management (UTM) technology.

- Organizations outsource based on their size and maturity level. Smaller organizations tend to outsource because of the inability to have an expert in-house SOC team and the necessary technologies. Further, these organizations outsource to improve the efficiencies and cost-effectiveness of their cybersecurity strategy. As size and maturity increases, outsourcing the SOC decreases.

Part 2. Key findings

In this section, we provide a deeper dive into the findings of the research. The complete audited findings are presented in the Appendix of the report. We have organized the research into the following topics.

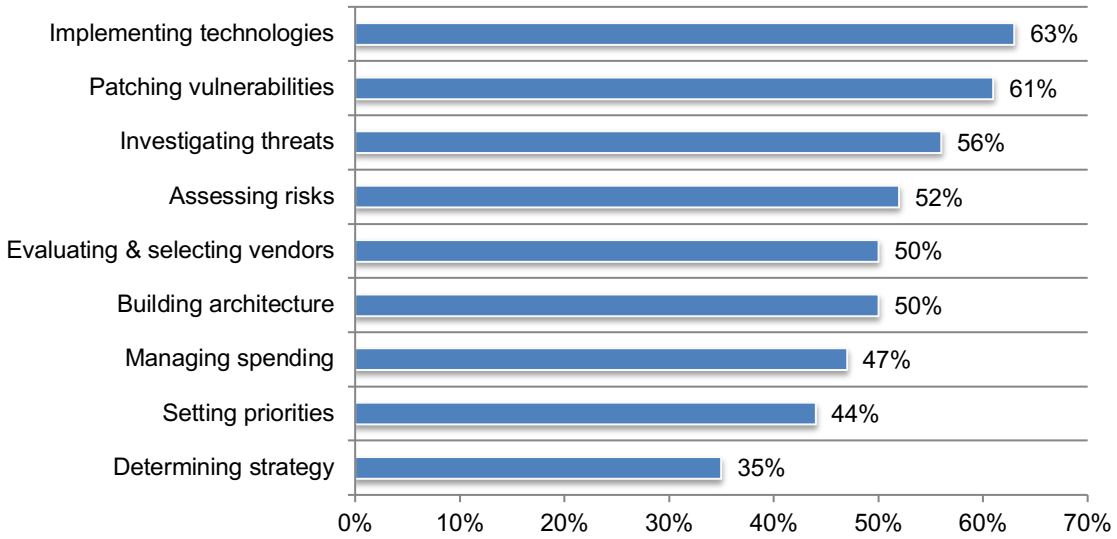
- The anatomy of today's SOC
- The SOC frustration factors
- The problem of SOC team burnout and alert fatigue
- Why organizations outsource SOC responsibility
- Special section: Why organizations do not have a SOC
- Conclusion and recommendations

The anatomy of today's SOC

Cybersecurity best practices are always evolving along with the latest attack techniques. The state of the SOC has evolved in kind, and while there are often business challenges or silos that can appear to hinder progress, organizations are continually adding services to support and improve their security postures.

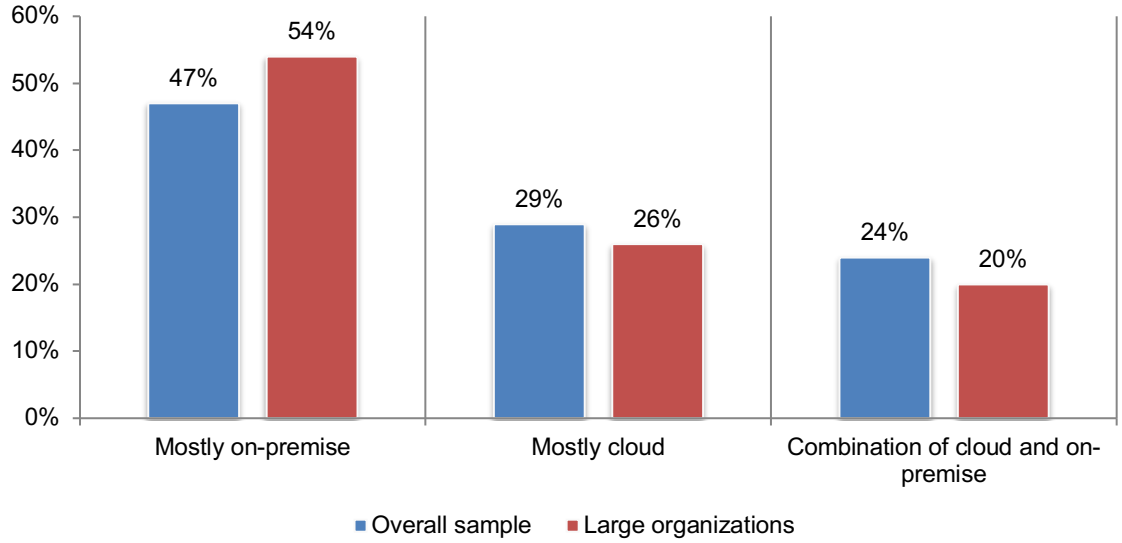
Respondents' primary tasks are Implementing technologies, patching vulnerabilities and investigating threats. Figure 2 presents nine cybersecurity activities. As shown, the focus of most respondents is to implement technologies (63 percent), patch vulnerabilities (61 percent) and investigate threats (56 percent). They are less involved in setting priorities and determining strategy.

Figure 2. Which of the following best describes your cybersecurity role?
More than on response permitted



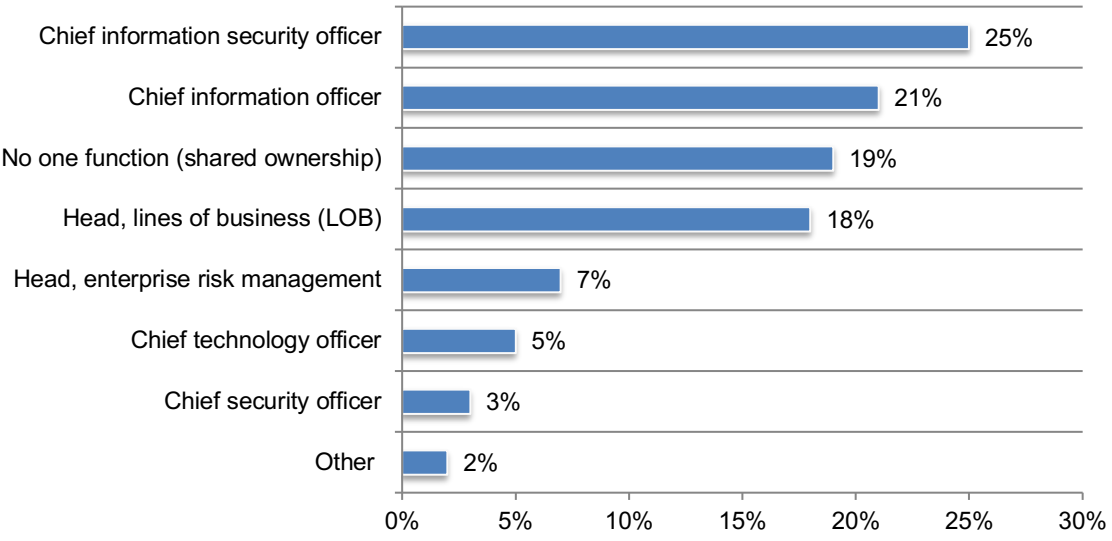
Organizations are moving to the cloud. As part of the research, we did an analysis of organizations with a headcount of more than 10,000 (large organizations). In Figure 3, we compare the differences between the overall sample of respondents and respondents in large organizations. As shown, 53 percent of respondents in the overall sample define the IT infrastructure that houses the SOC as mostly cloud (29 percent) or a combination of cloud and on-premise. Fifty-four percent of respondents in the large organizations say it is mostly on-premise.

Figure 3. What best defines the IT infrastructure that houses your SOC?



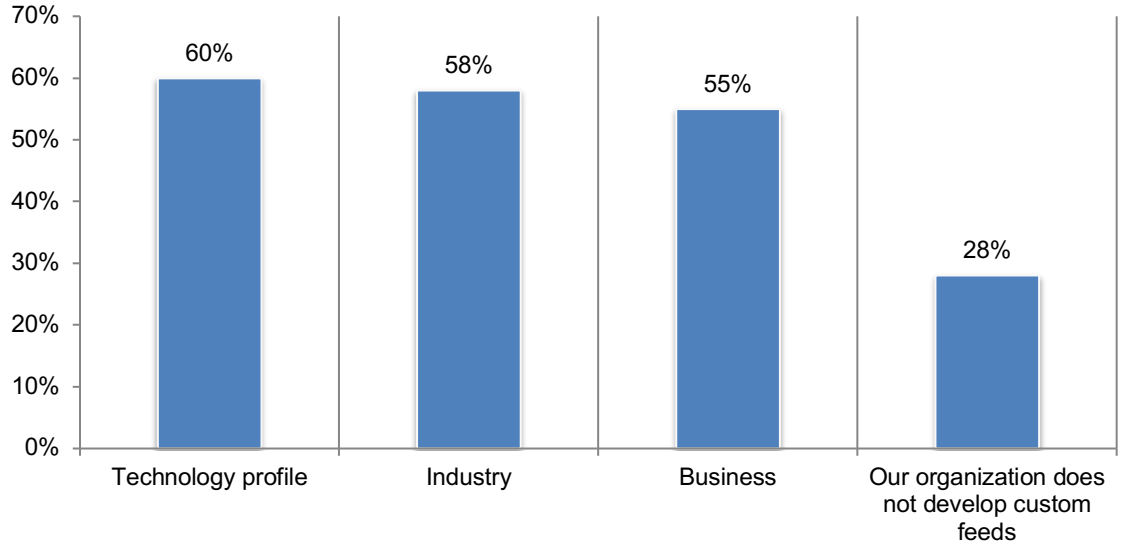
Security leads the SOC team. According to Figure 4, the CISO and CIO most often lead SOC operations in most organizations represented in this research. However,19 percent of respondents say no one function has clear authority and accountability for the SOC. In these organizations, it can be more difficult to make decisions that could lead to improvements in the SOC.

Figure 4. Who leads your organization's SOC team?



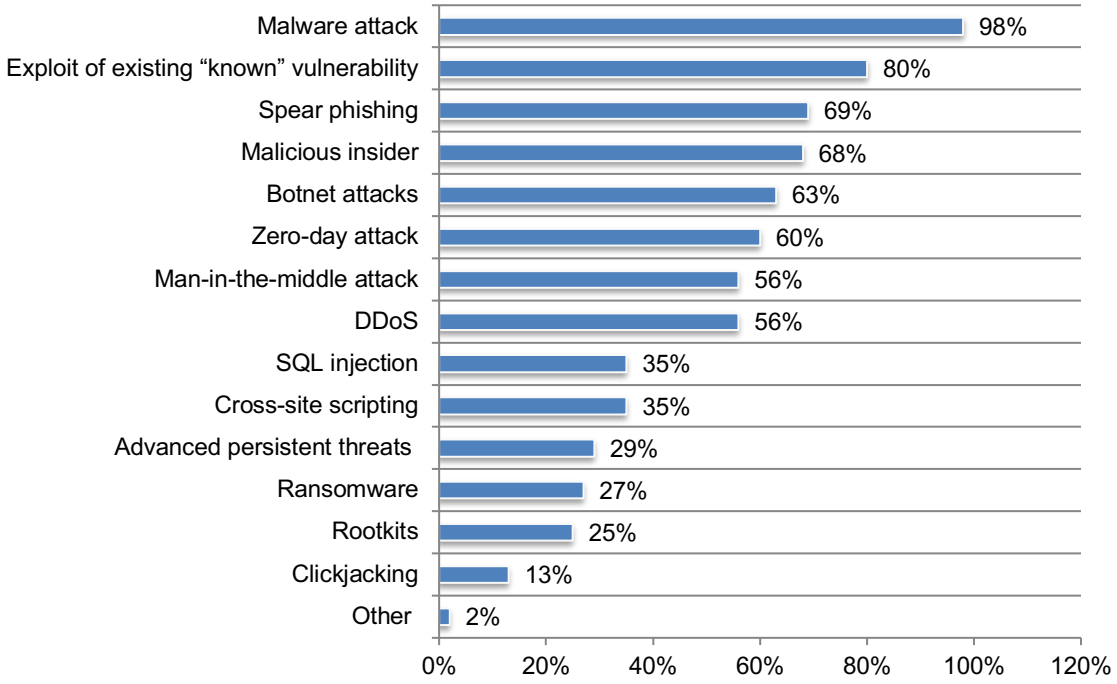
The majority of respondents say their companies invest in threat intelligence feeds. Fifty-one percent of respondents say their organizations invest in threat intelligence feeds and of these organizations, 54 percent of respondents say the threat intelligence feeds combine open source and paid feeds. According to Figure 5, 60 percent of respondents in organizations that invest in threat intelligence feeds develop internal custom feeds based on a technology profile. Twenty-eight percent of respondents say their organizations do not develop custom feeds.

Figure 5. Does your organization develop custom threat intelligence feeds?
The



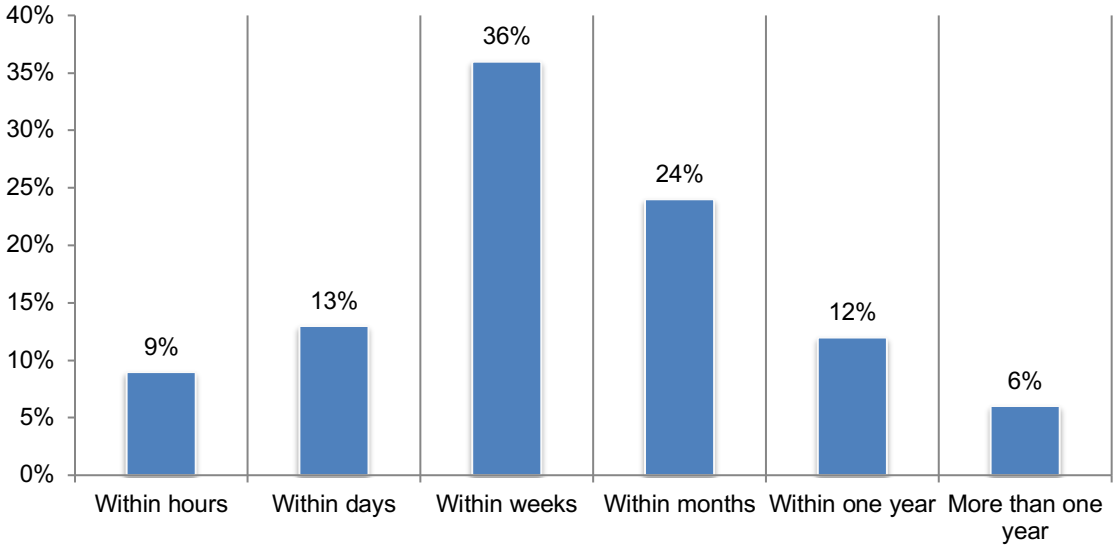
The exploits most commonly identified by the SOC are malware attacks. Figure 6 presents a list of security exploits identified by SOCs. As shown the most common are malware attacks, exploits of existing or known vulnerabilities, spear phishing and malicious insiders.

Figure 6. The exploits or compromises the SOC has identified over the past 12 months
More than one response permitted



The mean time to resolution (MTTR) can be months. Respondents were asked to estimate the time it takes to resolve a security incident. As shown in Figure 7, only 22 percent of respondents say resolution can occur within hours or days. Forty-two percent of respondents say the average time to resolve is months or even years.

Figure 7 On average, what is the MTTR for a security incident in your SOC?



Monitored or managed firewalls and intrusion prevention systems and intrusion detection systems are most often deployed within the SOC environment. Figure 8 presents the core services most often deployed today within the SOC environment. In addition to monitored or managed firewalls or intrusion prevention systems and monitored or managed intrusion detection systems, other services include managed vulnerability scanning of networks, servers, databases or applications and monitored or managed multifunction firewalls or unified threat management (UTM) technology.

Figure 8. The top five core services deployed within the SOC environment
More than one response permitted

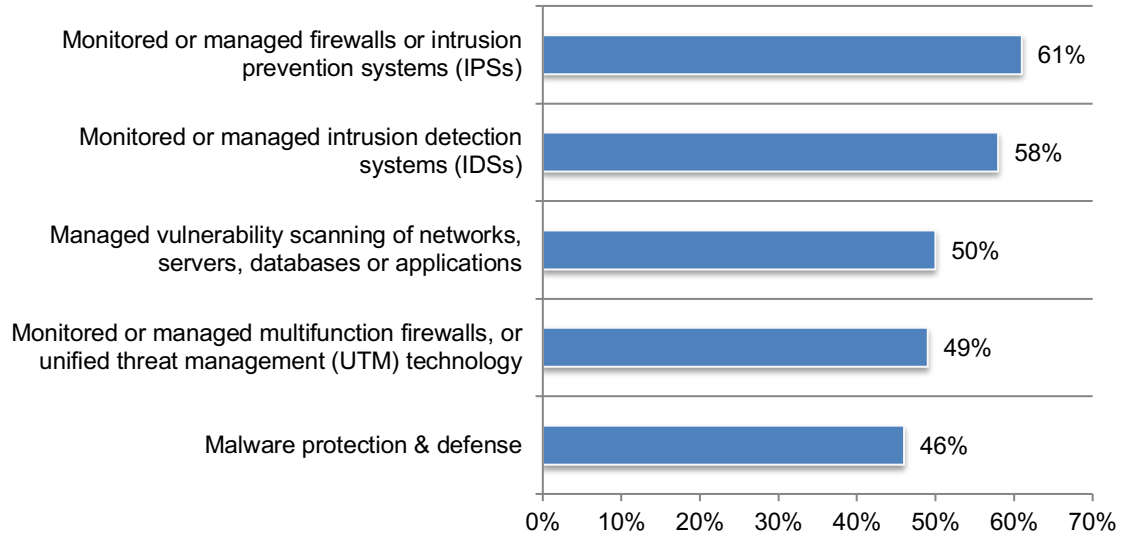
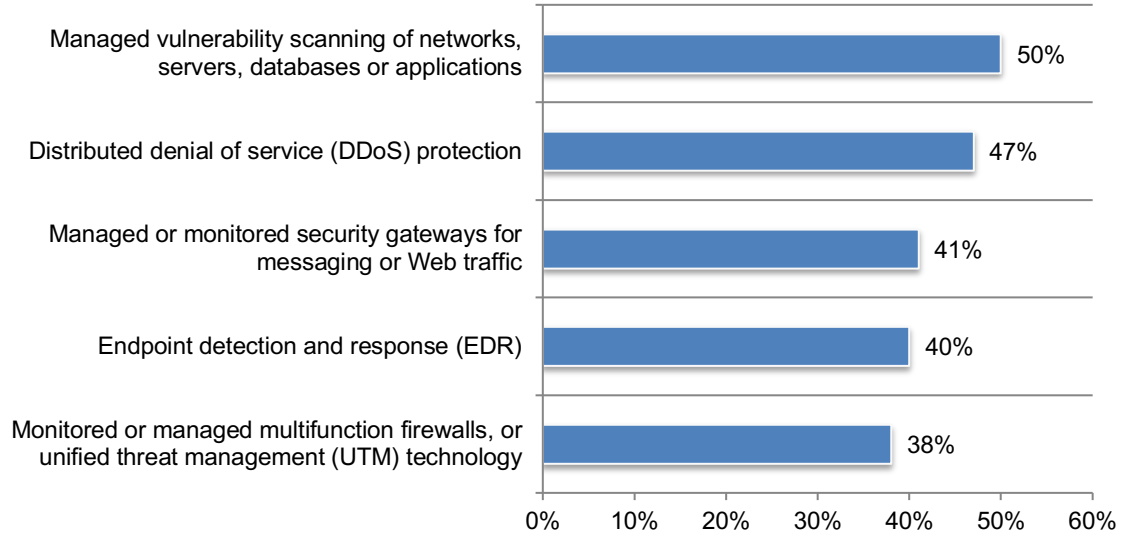


Figure 9 presents the top five services to be added to improve the cybersecurity posture. The most popular are managed vulnerability scanning of networks, servers, databases or applications and distributed denial of service (DDoS) protection (47 percent of respondents).

Figure 9. Top five services to be added within the next 12 months
More than one response permitted

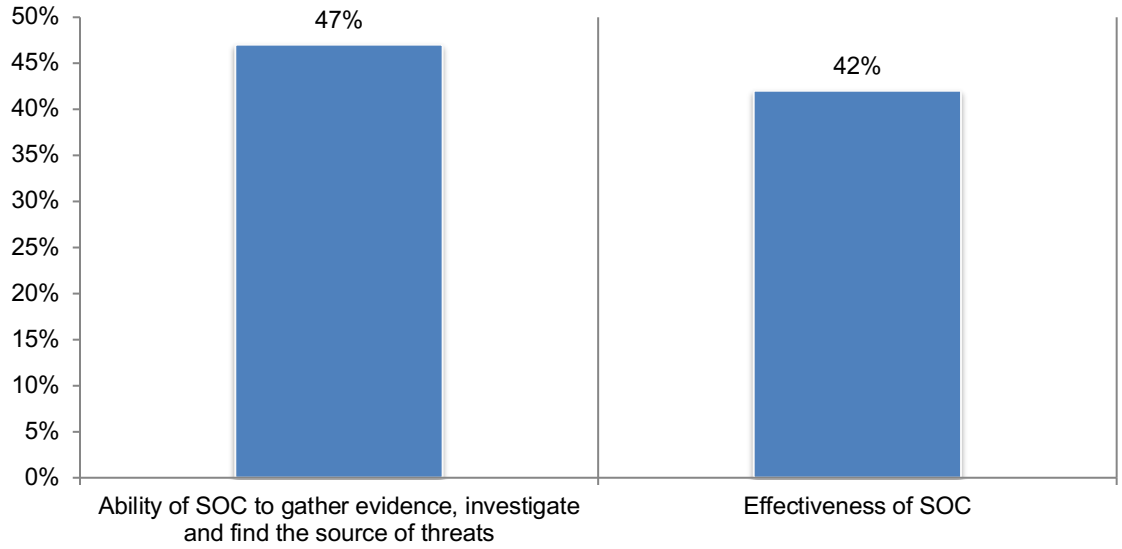


The SOC frustration factors

Despite the SOC's status as an essential component of business strategy, without full visibility into data and infrastructure, analysts view the SOC as being less effective and even painful to work in.

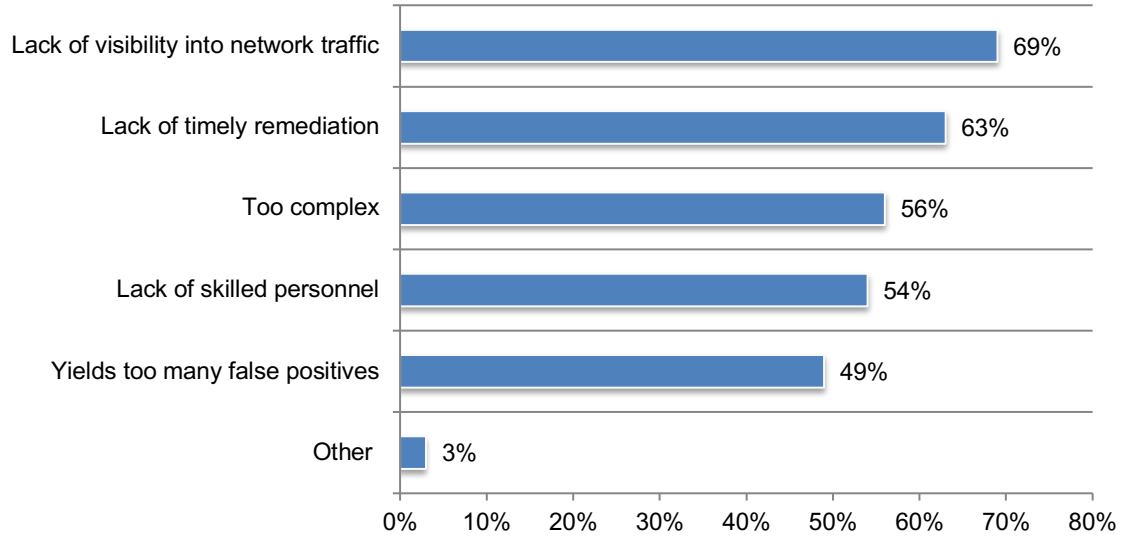
Organizations need to improve the effectiveness of their SOCs, including its ability to gather evidence, investigate and find the source of threats. As discussed previously, respondents say their SOCs are an important part of their cybersecurity strategy. However, when asked to rate the effectiveness of their organizations' SOC on a scale from 1 = not effective to 10 = highly effective, only 42 percent of respondents say it is highly effective. Less than half (47 percent) rate its ability to gather evidence, investigate and find the source of threats as very high, as shown in Figure 10.

Figure 10. How effective is your SOC and its ability to gather evidence, investigate and find the source of threats?
7+ responses on a scale of 1 = not effective to 10 = highly effective
7+ responses on a scale of 1 = no ability to 10 = high ability



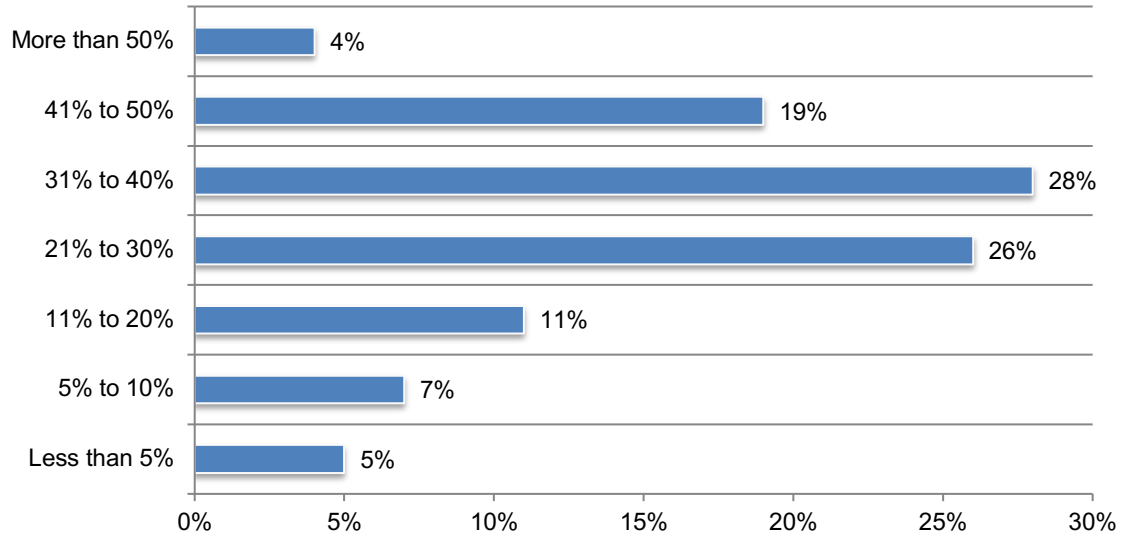
Of those respondents who rate their SOC as ineffective (58 percent of respondents), the primary reasons are the lack of visibility into network traffic and timely remediation (69 percent and 63 percent of respondents, respectively), as shown in Figure 11.

Figure 11. What can make the SOC ineffective?
More than on response permitted



The SOC budget in many organizations is inadequate. The average annual cybersecurity budget for organizations represented in this study is $26 million. As shown in Figure 12, only 4 percent of respondents say more than 50 percent of the cybersecurity budget will be allocated to their SOC. The average allocation is 30 percent of the total cybersecurity budget.

Figure 12. What percentage of your cybersecurity budget will fund the SOC this year?
Extrapolated value = 30%

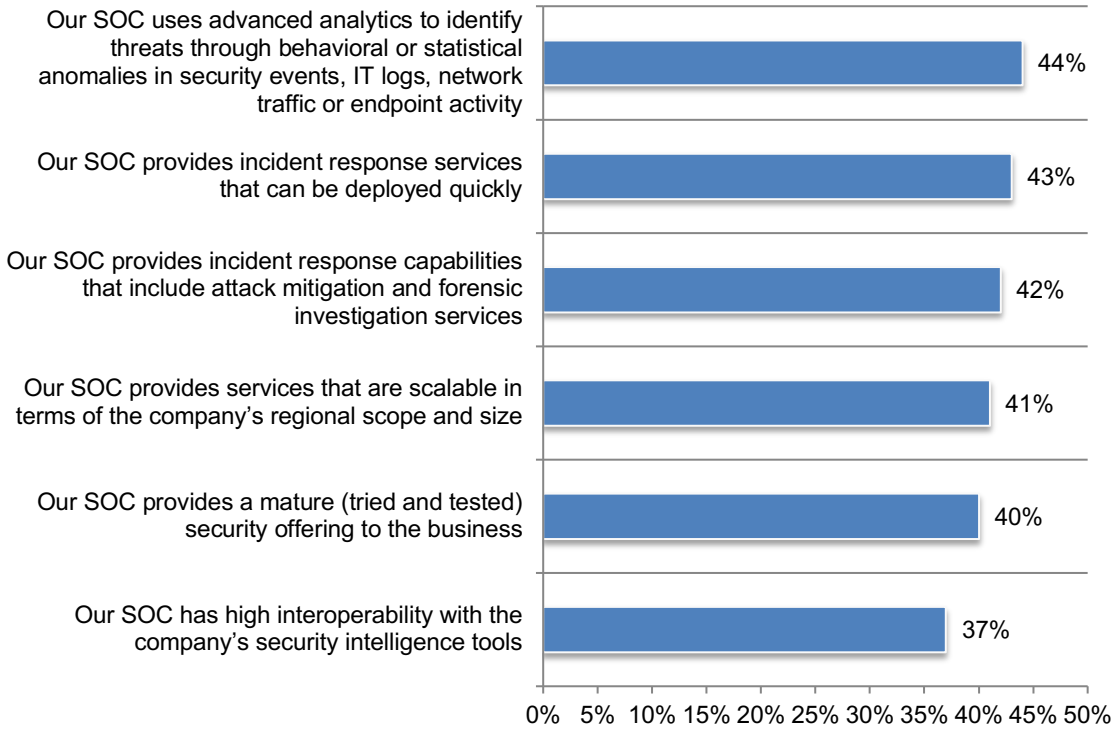


Most SOCs do not have high interoperability with the organization's security intelligence tools. Figure 13 presents six factors that can influence the ability of the SOC to effectively prevent, detect, analyze and respond to cybersecurity incidents. However, the majority of organizations are not ensuring their SOCs have incorporated these tools.

Specifically, only 37 percent of respondents say their SOCs have high interoperability with their organizations' security intelligence tools and only 40 percent say their SOC is a mature (tried and tested) security offering. Other areas in need of improvement are the scalability of SOC services and incident response plans that have the capability to mitigate and investigate services and can be deployed quickly.

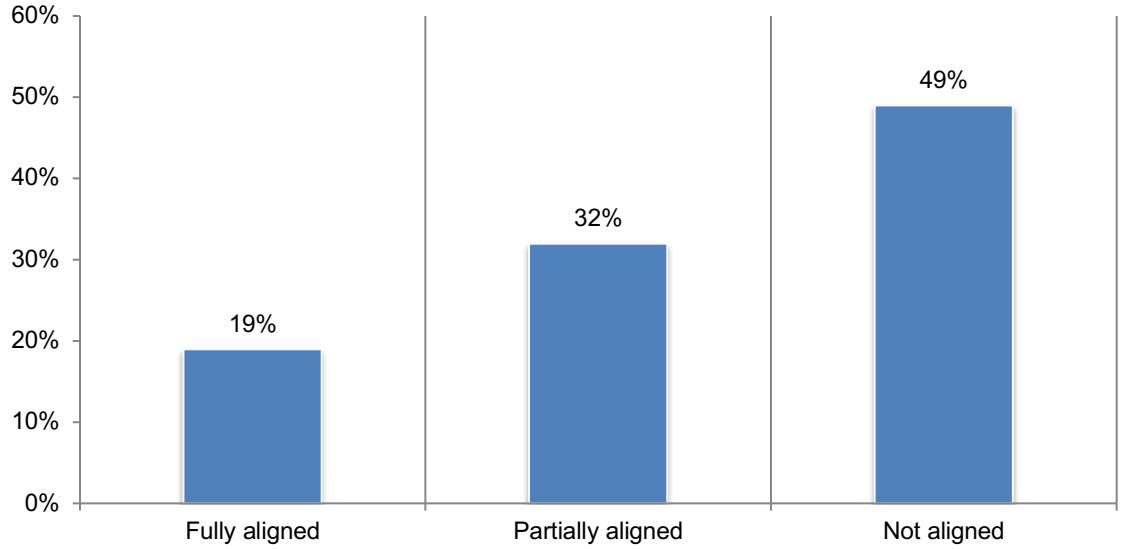
As discussed previously, many organizations are not effective in gathering evidence and investigating in order to find the source of threats. As shown, only 44 percent of respondents say the SOC uses advanced analytics to identify threats through behavioral or statistical anomalies in security events, IT logs, network traffic or endpoint activity.

Figure 13. Challenges to an effective SOC
Strongly Agree and Agree responses combined



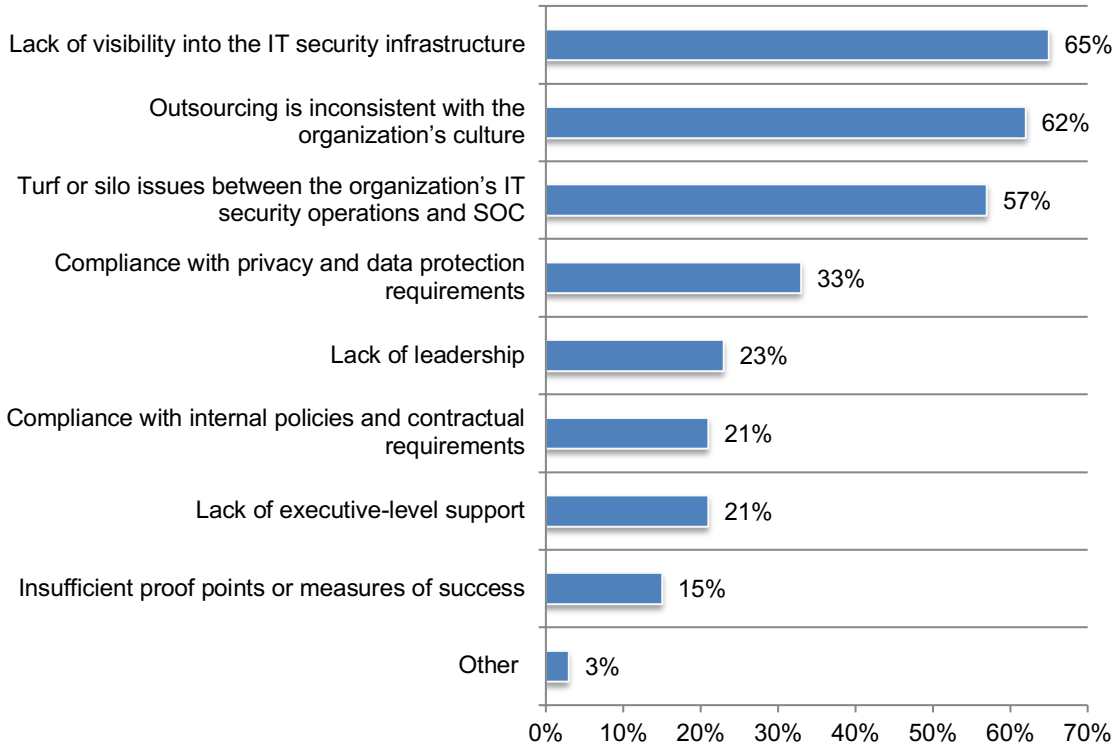
SOCs are not aligned with the objectives and needs of the business. According to Figure 14, only 19 percent of respondents say the objectives of the SOC are fully aligned with their organizations' business needs. Forty-nine percent of respondents say they are not aligned at all. As a consequence, it is difficult to have senior leadership's support and commitment to providing adequate funding for investments in technologies and staffing.

Figure 14. Within your organization, are SOC objectives aligned with business needs?



Could a lack of alignment between IT security operations and the SOC affect the ability to successfully manage the SOC? According to Figure 15, 57 percent of respondents say turf or silo issues between the organization's IT security operations diminishes the successful operation of the SOC. Sixty-five percent of respondents say the lack of visibility into the IT security infrastructure affects SOC operations. While many respondents see outsourcing as a means to improve the SOC operations, 62 percent of respondents say outsourcing is inconsistent with the organization's culture.

Figure 15. What do you see as the main barriers to successfully operating the SOC?
Three responses permitted

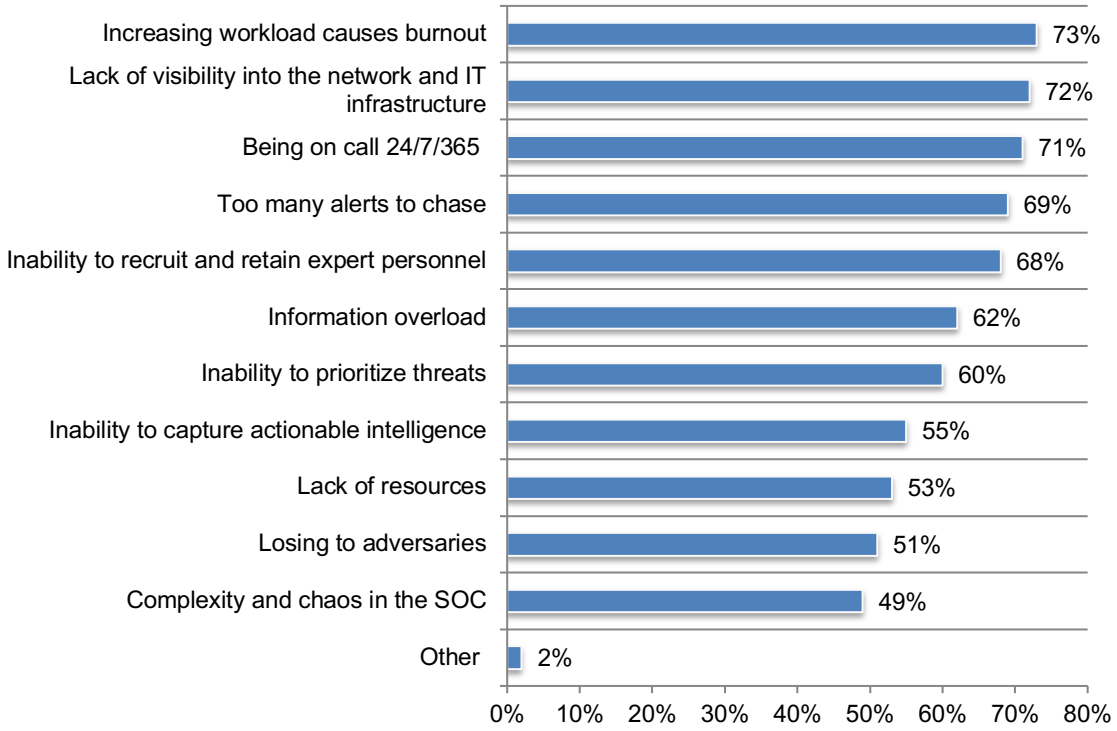


The problem of SOC team burnout and alert fatigue

IT security personnel are approaching burnout as they spend increasingly more time on threat investigation while complexity and chaos, alert fatigue and workload grow, and the talent pipeline thins out.

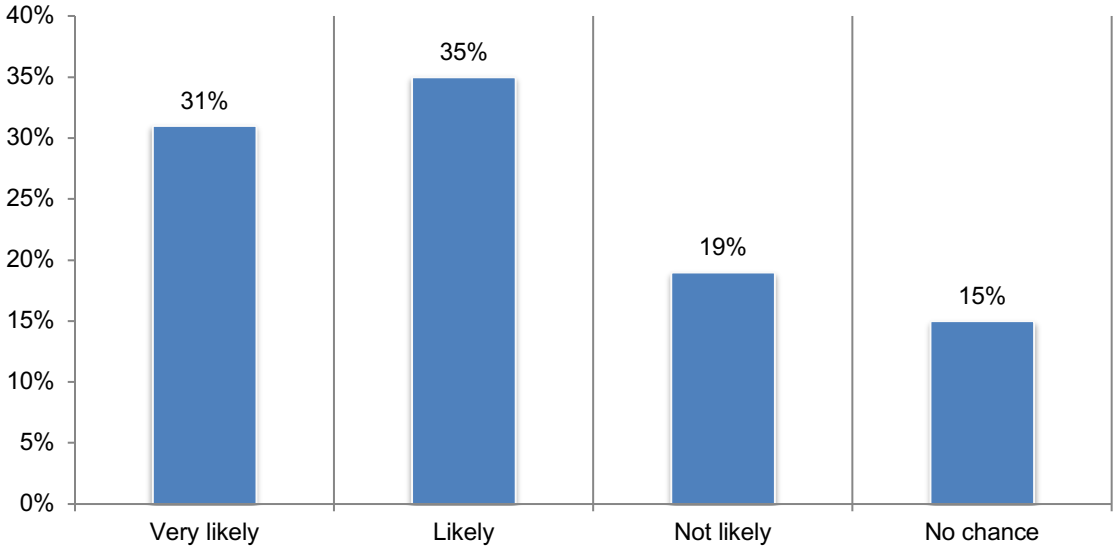
IT security personnel say working in the SOC is painful. Respondents were asked to rate the "pain" of the SOC security personnel's experience in meeting their daily job requirements from a scale of 1 = no pain to 10 = very painful. Seventy percent of respondents say working in the SOC is very painful and the number one reason is the increasing workload causes burnout followed by a lack of visibility into the network and IT infrastructure. They also cite being on call 24/7/365 and having too many alerts to chase, as shown in Figure 16.

Figure 16. what makes working in the SOC painful?
More than one response permitted



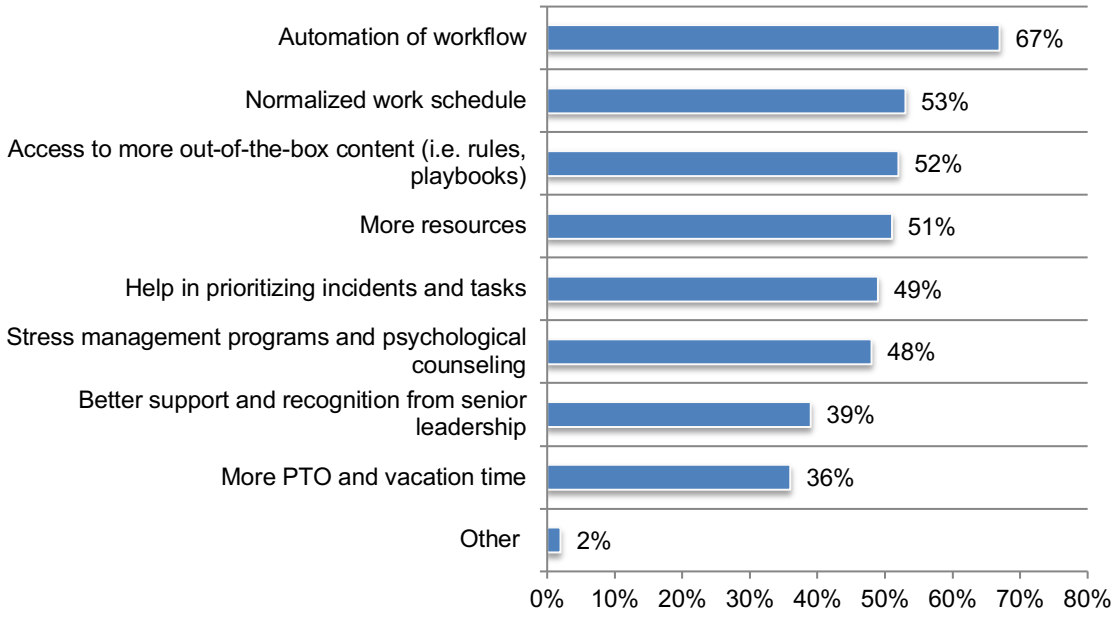
The stress of working in a SOC makes it difficult to hire and retain experienced IT security practitioners. Sixty-five percent of respondents say the stress of working in the SOC caused them to consider changing careers or leaving their jobs. According to Figure 17, 66 percent of respondents say it is very likely or likely that experienced security analysts would quit the SOC.

Figure 17. What is the likelihood that the above pain factors would cause experienced security analysts to quit the SOC?



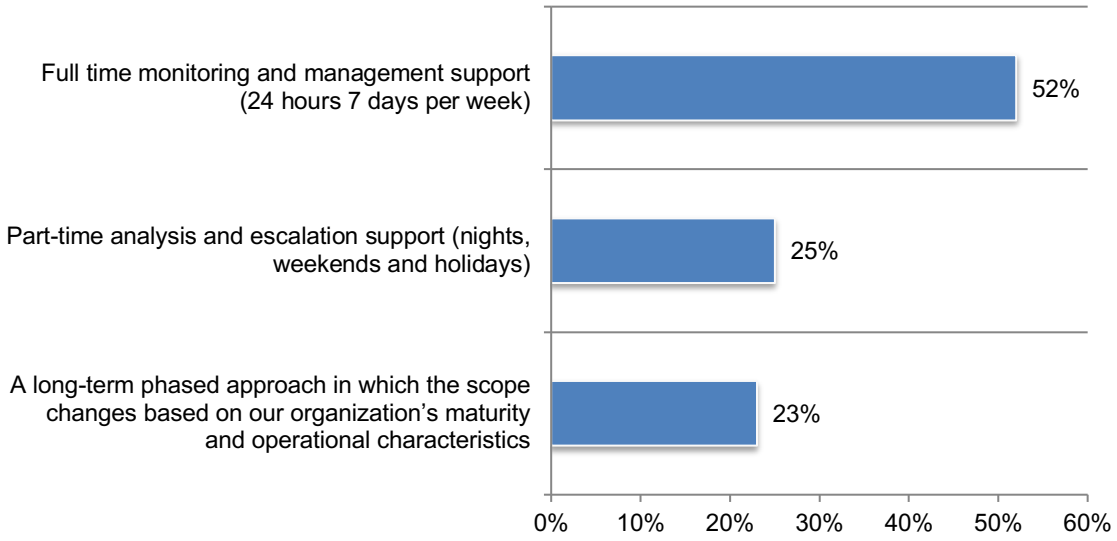
To reduce the pain, respondents say automation and a normalized work schedule would be helpful. According to Figure 18, most respondents are not looking for more vacation time but seek an automation of workflow and normalized work schedule.

Figure 18. What steps can be taken to alleviate your SOC team's pain?
More than one response permitted



Most SOCs are providing full time monitoring and management support (24/7/365). Despite the pain caused by increased workload, 52 percent of respondents say their SOCs are providing round the clock monitoring and support. Only 23 percent of respondents say their approach is long-term based on the maturity of the organization and operational characteristics, as shown in Figure 19.

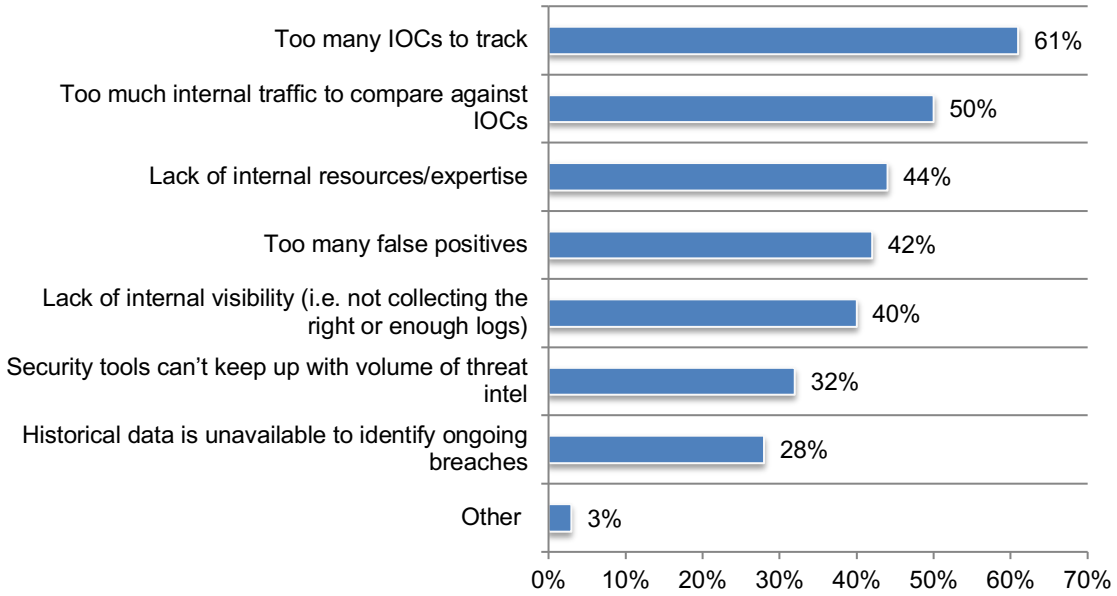
Figure 19. What best describes your SOC's coverage, scope of monitoring and engagement?



The ineffectiveness of threat hunting teams is a frustration. Fifty-four percent of respondents say their organizations have a threat hunting team; however, 45 percent of these respondents say it does not effectively leverage threat hunting to prevent incidents from happening while 16 percent are unsure.

As shown in Figure 20, the effectiveness of the threat hunting team is diminished because of too many IOCs to track (61 percent of respondents), too much internal traffic to compare against IOCs (50 percent of respondents) and lack of internal resources/expertise (44 percent of respondents).

Figure 20. What challenges does your threat hunting team face?
Three responses permitted

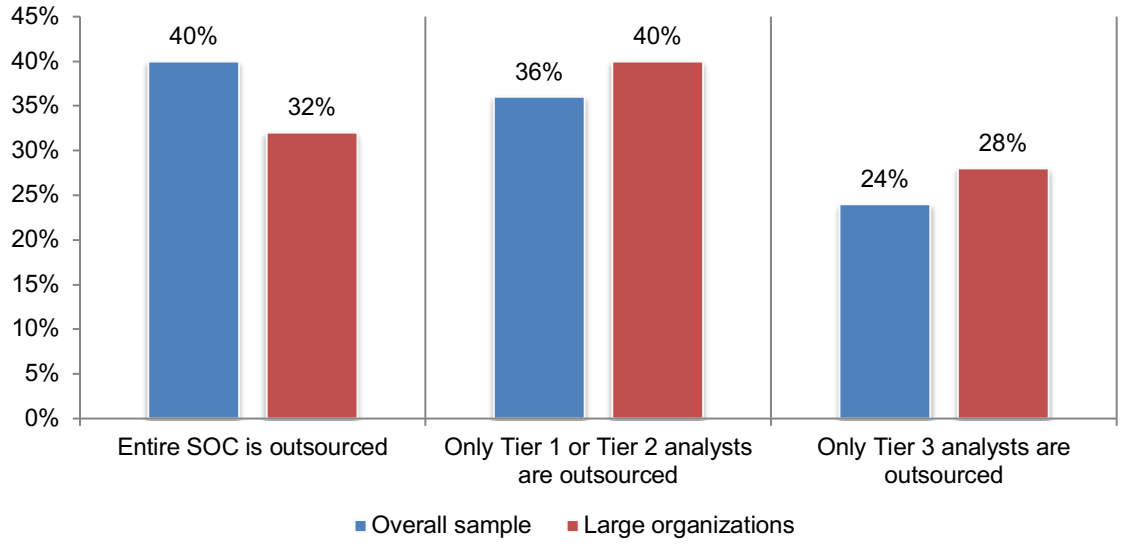


Why organizations outsource SOC responsibilities

Organizations turn to outsourcing SOC responsibilities due to restrictions on resources and budgeting, but show demand for an in-house SOC in the event of a budget increase or significant loss due to a security breach.

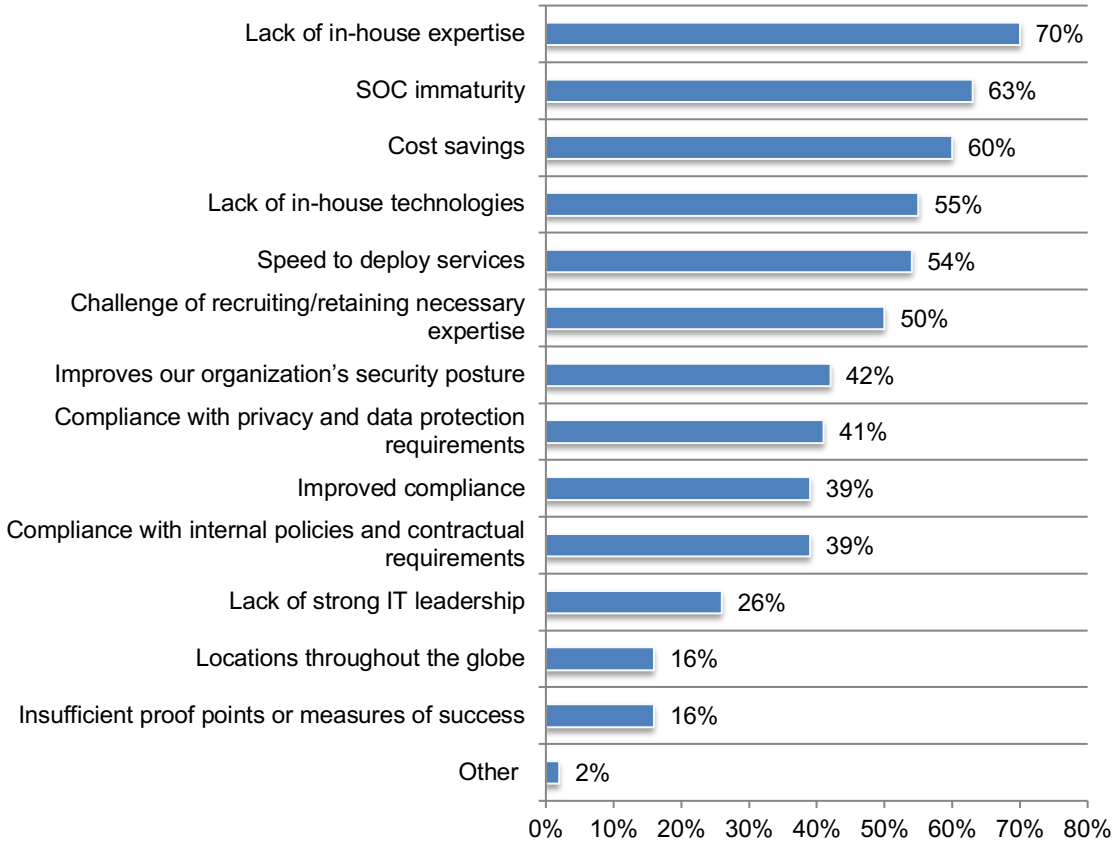
Organizations outsource because of a lack of in-house expertise. Fifty-eight percent of respondents say their organizations outsource all or part of their SOC. According to Figure 21, 40 percent outsource the entire SOC and 36 percent outsource only Tier 1 or Tier 2 analysts.

Figure 21. What best defines your outsourcing strategy?



The decision to outsource is based on the lack of internal resources. As shown in Figure 22, the inability to have an expert in-house SOC team and the necessary technologies, which leads to the immaturity of the SOC, drives the decision to outsource. Sixty percent of respondents say outsourcing of their SOC saves money, which is important because many respondents cite budgetary constraints as a problem in having a successful SOC.

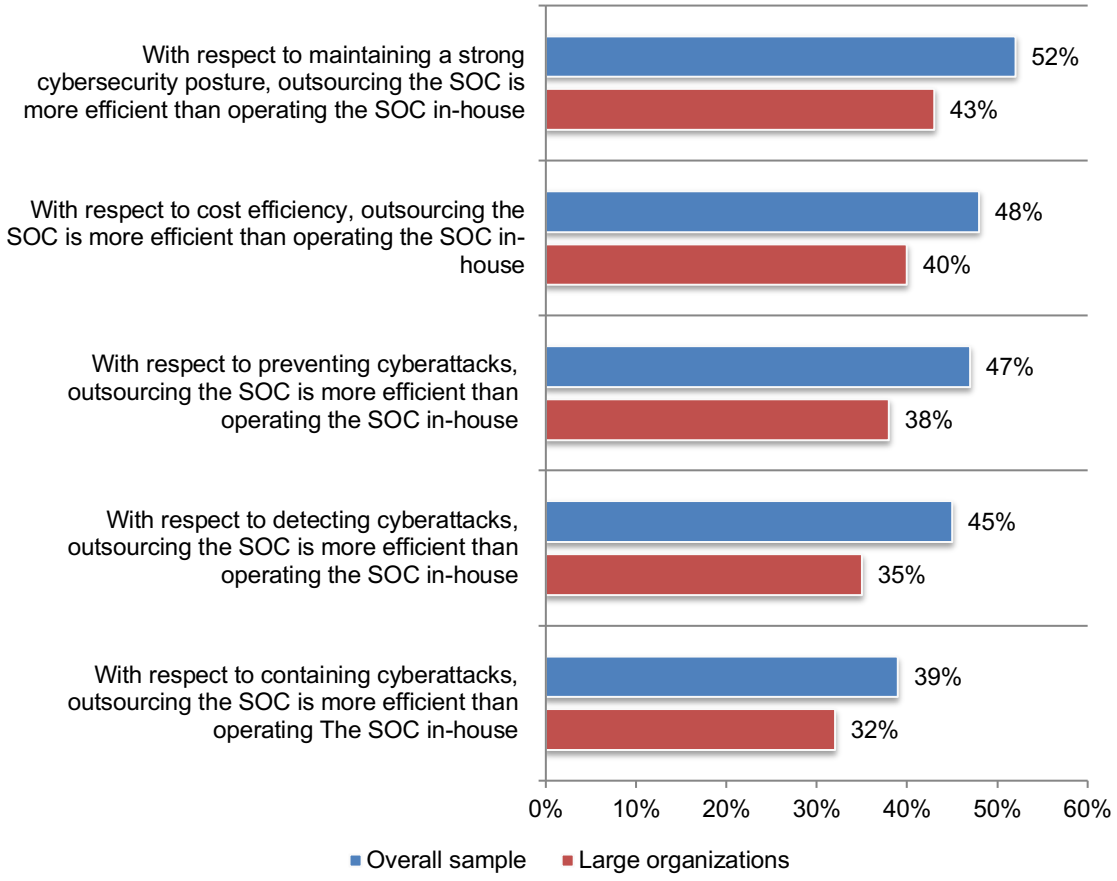
Figure 22. Why did your organization decide to outsource?
More than one response permitted



The decision to outsource is often made to achieve greater efficiencies and cost effectiveness. Once again, we compare the overall sample of respondents to large organizations. Respondents were asked to compare on-premise SOC operations to their outsourced SOC operations.

According to Figure 23, the primary benefits are efficiencies in achieving cybersecurity goals (52 percent of respondents) and reducing costs (48 percent of respondents). Only 39 percent of respondents say containing cyberattacks is more efficient and less than half say that detecting and preventing cyberattacks is more efficient when outsourcing the SOC. Large organizations, as shown in the figure, are less likely to believe outsourcing is more effective than on-premise.

Figure 23. How services provided by a managed service provider compare to those provided in-house
Strongly agree and Agree responses combined

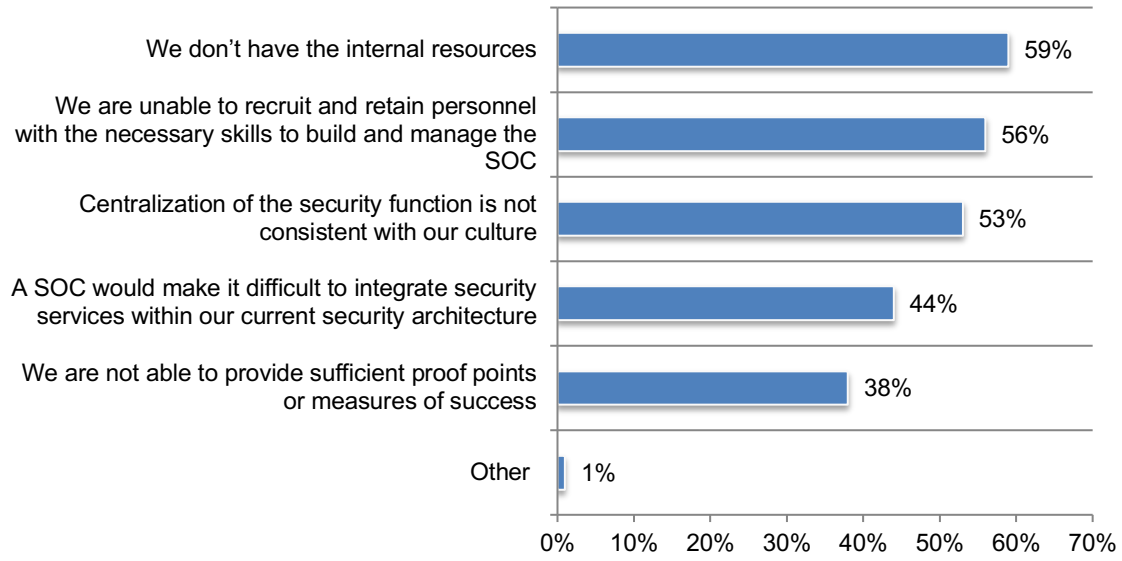


Special section: Why organizations do not have a SOC

In the previous sections of the report, all findings were based on organizations that have a SOC. However, we did ask individuals who were screened out of the completion of the survey why they do not have a SOC and what would motivate them to have a SOC. These respondents were not included in the research. Their responses are presented in this section.

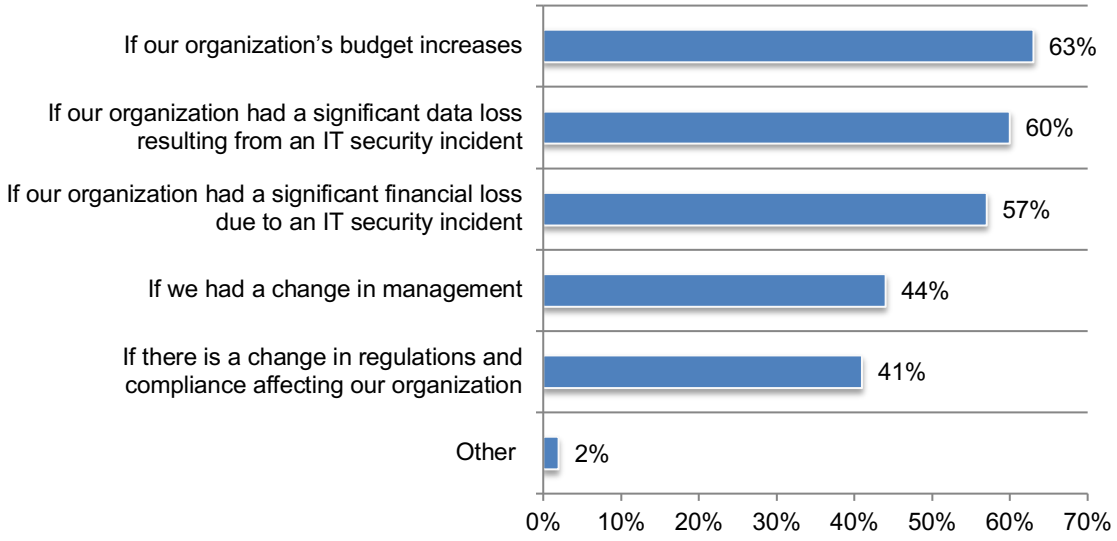
A lack of internal resources and the inability to recruit and retain personnel are cited as the main reasons for not having a SOC. The reasons for not having a SOC are shown in Figure 24 and the primary reasons are not having internal resources and the inability to recruit and retain personnel with the necessary skills to build and manage the SOC. The difficulty in integration of the SOC's security services with their security architecture deters many organizations from having a SOC.

Figure 24. Why does your organization not deploy or plan to deploy a SOC?
More than one response permitted



More budget would encourage organizations to have a SOC. Respondents without a SOC recognize the importance of having adequate budget to ensure the success of a SOC, as shown in Figure 25. However, a data breach resulting from an IT security incident would also motivate an organization to deploy a SOC, demonstrating that organizations are prioritizing budget over strengthening their security postures.

Figure 25. What would motivate your organization to deploy a SOC?
More than one response permitted



Conclusion and Recommendations

Organizations are frustrated because they recognize that the SOC is critical to their cybersecurity strategy, but struggle with its effectiveness when confronted with challenges such as budgets, lack of visibility into critical infrastructure, organizational culture and maturity, including whether to outsource, and business alignment. In addition, the limited talent pipeline, increased workloads, and alert fatigue is causing severe stress among analysts – enough to consider a career change. These factors do not bode well for setting a SOC up for success, but the research also suggests organizations can consider the following actions.

1. **Address analyst burnout.** Leaders face a mandate to reduce the stress and pain that comes with working in the SOC. The inability to have enough experienced security analysts will prevent organizations from improving the SOC. The number one recommendation from respondents is to automate workflow, followed by normalizing the work schedule, having access to more out-of-the-box content and having more resources. By paying attention to these basic needs, leaders will foster a more successful SOC, and overall a stronger security posture.

2. **Create stronger alignment between the SOC and the business**. Often, the needs of the business and the needs of the SOC are in alignment – everyone wants a stronger security posture, but not at the expense of an oversubscribed budget. Leaders should create opportunities for leaders of each silo to discuss and prioritize objectives, and better address the turf and silo issues between the SOC and IT security operations. Not only will this create more strategic security processes, it will in all likelihood help increase the amount of budget allocated to the SOC.

3. **Support analyst talent with security operations technologies.** Respondents noted part of their security operations strategies is to wait for a negative impact before dedicating larger budgets toward personnel and technology, and they largely believe that while an outsourced SOC is cost-effective, it is subpar to an in-house SOC. Leaders should support their existing personnel and help to build the effectiveness of the security function by creating stronger alignment between the SOC and security intelligence tools, as well as investing in technologies that will address the security problems cited in the research, such as a lack of full visibility into the network traffic, lack of timely remediation, lack of interoperability with other security solutions and too many false positives.

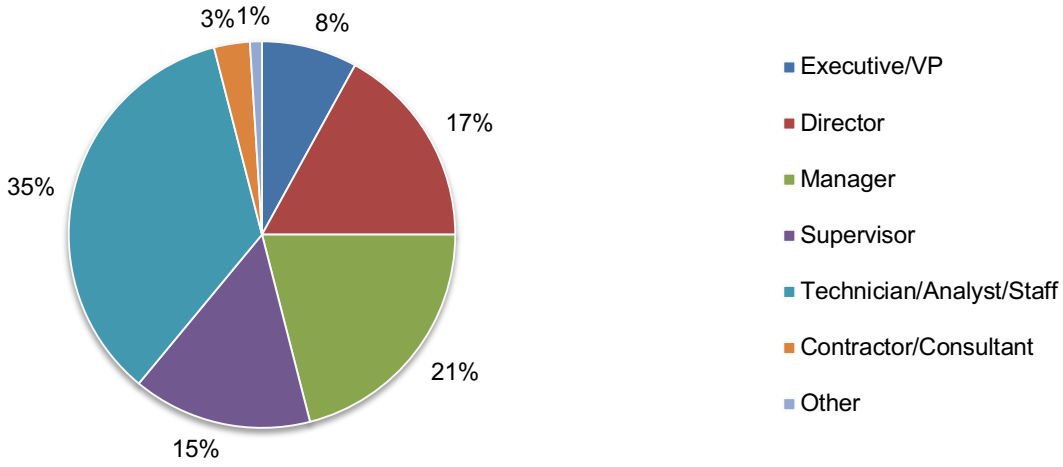
Part 3. Methods

The sampling frame is composed of 15,495 IT and IT security practitioners in organizations that have an SOC. As shown in Table 1, 607 respondents completed the survey. Screening removed 53 surveys. The final sample was 554 surveys resulting in a 3.6 percent response rate.

Table 1. Sample response	Freq	Pct%
Total sampling frame	15,495	100.0%
Total returns	607	3.9%
Rejected or screened surveys	53	0.3%
Final sample	554	3.6%

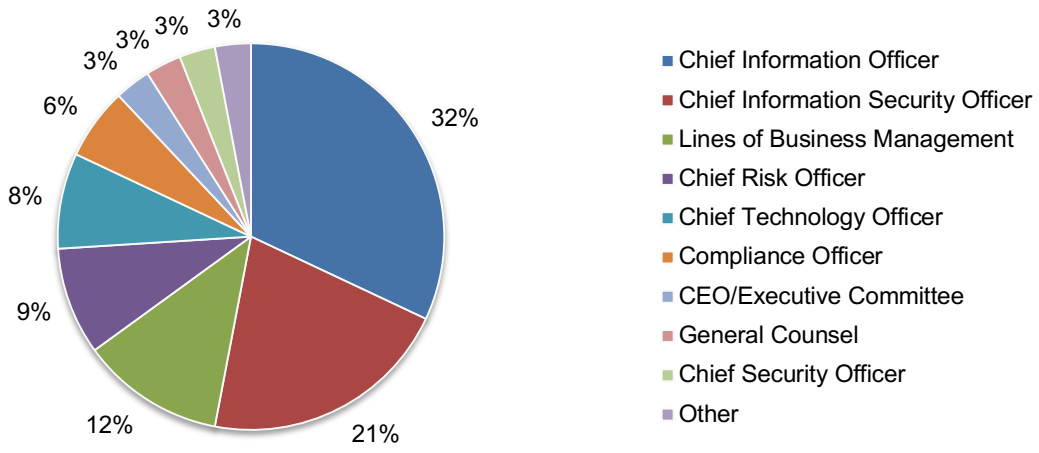
Pie Chart 1 reports the current position or organizational level of the respondents. More than half of respondents (61 percent) reported their current position as supervisory or above. Thirty-five percent of respondents reported their current position as technician/analyst/staff.

Pie Chart 1. Current position or organizational level



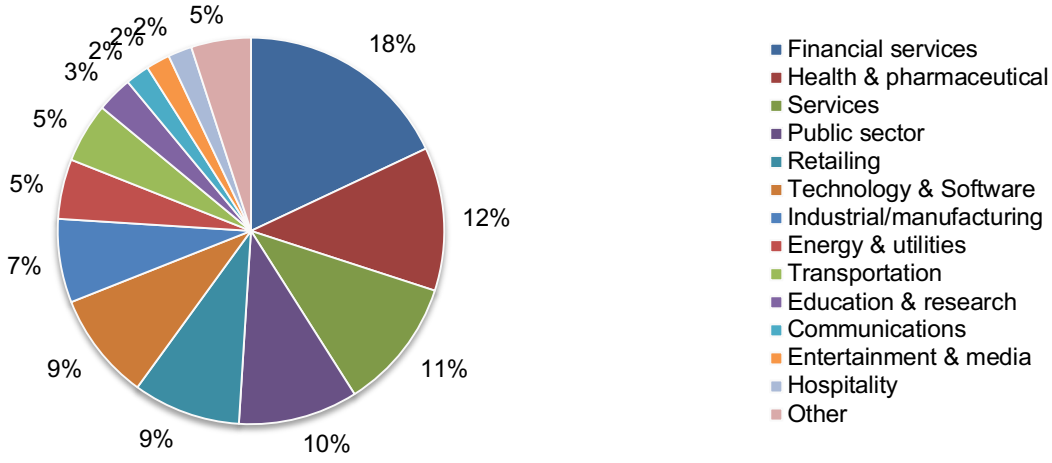
As shown in Pie Chart 2, 32 percent of respondents report to the chief information officer, 21 percent of respondents report to the chief information security officer, 12 percent of respondents report to the lines of business management and 9 percent of respondents indicated they report to the chief risk officer.

Pie Chart 2. Primary person you or your leader reports to



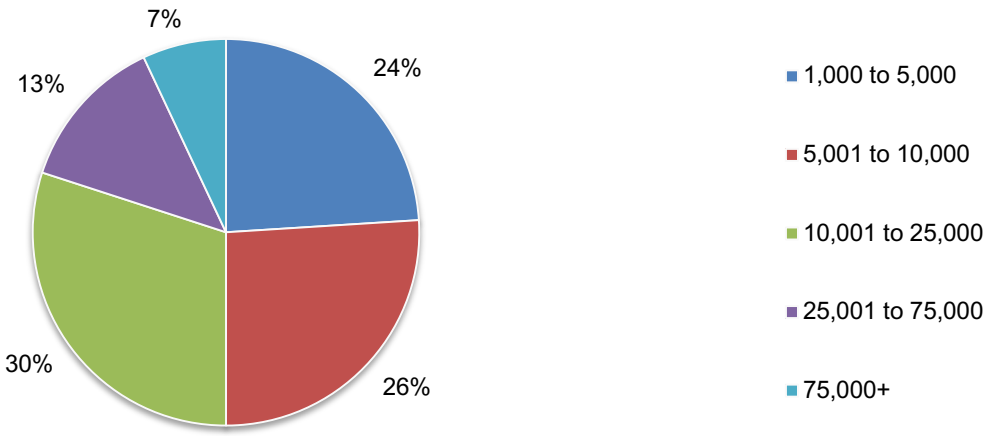
Pie Chart 3 reports the primary industry focus of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceuticals (12 percent of respondents), services (11 percent of respondents), public sector and retail sector, each at 9 percent of respondents respectively.

Pie Chart 3. Primary industry focus



According to Pie Chart 4, half of the respondents (50 percent) are from organizations with a global headcount of over 10,000 employees.

Pie Chart 4. Worldwide headcount of the organization



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals from organizations that have a SOC. Because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, the possibility remains that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between March 11 and April 5, 2019.

Survey response	Freq	Pct%
Total sampling frame	15,495	100.0%
Total returns	607	3.9%
Rejected surveys	53	0.3%
Final sample	554	3.6%

Part 1. Screening questions

S1a. Does your organization deploy a SOC?	Pct%
Yes [Go to Q1]	60%
No, but we plan to deploy a SOC [Go to S1d]	18%
No [Go to S1b]	22%
Total	100%

S1b. If no, why does your organization not deploy (or plan to deploy) a SOC? Select all that apply.	Pct%
We don't have the internal resources	59%
A SOC would make it difficult to integrate security services within our current security architecture	44%
We are not able to provide sufficient proof points or measures of success	38%
Centralization of the security function is not consistent with our culture	53%
We are unable to recruit and retain personnel with the necessary skills to build and manage the SOC	56%
Other (please specify)	1%
Total	251%

S1c. If no, what would motivate your organization to deploy a SOC? Please check all that apply.	Pct%
If our organization had a significant financial loss due to an IT security incident	57%
If our organization had a significant data loss resulting from an IT security incident	60%
If there is a change in regulations and compliance affecting our organization	41%
If our organization's budget increases	63%
If we had a change in management	44%
Other (please specify)	2%
Total	267%

S1d. When does your organization plan to deploy a SOC?	Pct%
Within the next 6 months	30%
Within the next year	37%
More than one year	18%
Do not know when this will happen	15%
Total	100%

S1e. What services would you like your SOC to provide? Please select all that apply.	Pct%
Management of security intelligence technologies	55%
Network security management (NSM)	51%
Endpoint detection and response (EDR)	48%
Monitored or managed firewalls or intrusion prevention systems (IPSs)	65%
Monitored or managed intrusion detection systems (IDSs)	63%
Monitored or managed multifunction firewalls, or unified threat management (UTM) technology	59%
Managed or monitored security gateways for messaging or Web traffic	62%
Security analysis and reporting of events collected from IT infrastructure logs	48%
Reporting associated with monitored/managed devices and incident response	45%
Managed vulnerability scanning of networks, servers, databases or applications	50%
Distributed denial of service (DDoS) protection	43%
Monitoring of advanced threats defense	36%
Other (please specify)	3%
Total	628%

Part 2. Background

In the following research sections, only respondents employed in organizations with a SOC are allowed to participate.

Q1. Which of the following best describes your role in the cybersecurity function within your organization? Please check all that apply.	Pct%
Setting priorities	44%
Determining strategy	35%
Building architecture	50%
Assessing risks	52%
Implementing technologies	63%
Managing spending	47%
Evaluating & selecting vendors	50%
Investigating threats	56%
Patching vulnerabilities	61%
Total	458%

Q2a. Following are core services typically deployed within the SOC environment. Please check all SOC services provided by your organization today.	Pct%
Management of security intelligence technologies	30%
Network security management (NSM)	29%
Endpoint detection and response (EDR)	34%
Monitored or managed firewalls or intrusion prevention systems (IPSs)	61%
Monitored or managed intrusion detection systems (IDSs)	58%
Monitored or managed multifunction firewalls, or unified threat management (UTM) technology	49%
Managed or monitored security gateways for messaging or Web traffic	37%
Security analysis and reporting of events collected from IT infrastructure logs	28%
Reporting associated with monitored/managed devices and incident response	30%
Managed vulnerability scanning of networks, servers, databases or applications	50%
Distributed denial of service (DDoS) protection	42%
Malware protection & defense	46%
Monitoring of advanced threats	32%
Use of honeypot and other countermeasures	19%
Threat hunting	37%
Incident response and remediation	35%
Total	617%

Q2b. Does your organization plan to add any of the following services to support your organization's IT security posture within the next 12 months? Please check all that apply.	Pct%
Management of security intelligence technologies	27%
Network security management (NSM)	35%
Endpoint detection and response (EDR)	40%
Monitored or managed firewalls or intrusion prevention systems (IPSs)	33%
Monitored or managed intrusion detection systems (IDSs)	33%
Monitored or managed multifunction firewalls, or unified threat management (UTM) technology	38%
Managed or monitored security gateways for messaging or Web traffic	41%
Security analysis and reporting of events collected from IT infrastructure logs	44%
Reporting associated with monitored/managed devices and incident response	40%
Managed vulnerability scanning of networks, servers, databases or applications	50%
Distributed denial of service (DDoS) protection	47%
Malware protection & defense	25%
Monitoring of advanced threats	31%
Use of honeypot and other countermeasures	36%
Threat hunting	36%
Total	556%

Q3. How important is your organization's SOC to its overall cybersecurity strategy?	Pct%
Essential	27%
Very important	40%
Important	19%
Not important	9%
Irrelevant	5%
Total	100%

Q4. Within your organization, are SOC objectives aligned with business needs?	Pct%
Fully aligned	19%
Partially aligned	32%
Not aligned	49%
Total	100%

Q5. What best defines the IT infrastructure that houses your SOC?	Pct%
Mostly cloud	29%
Mostly on-premise	47%
Combination of cloud and on-premise	24%
Total	100%

Q6a. Do you outsource all or part of your organization's SOC?	Pct%
Yes	58%
No	42%
Total	100%

Q6b. If yes, what best defines your outsourcing strategy?	Pct%
Entire SOC is outsourced	40%
Only Tier 1 or Tier 2 analysts are outsourced	36%
Only Tier 3 analysts are outsourced	24%
Total	100%

Q6c. If yes, why did your organization decide to outsource?	Pct%
Lack of in-house expertise	70%
SOC immaturity	63%
Lack of in-house technologies	55%
Improves our organization's security posture	42%
Lack of strong IT leadership	26%
Compliance with privacy and data protection requirements	41%
Compliance with internal policies and contractual requirements	39%
Insufficient proof points or measures of success	16%
Cost savings	60%
Speed to deploy services	54%
Locations throughout the globe	16%
Challenge of recruiting/retaining necessary expertise	50%
Improved compliance	39%
Other (please specify)	2%
Total	573%

Q6d. If yes, how do the SOC services provided by a managed service provider compare to services directly provided in-house (e.g., built by your organization's IT department) Please provide your efficiency rating for each one of the following five attributes.	
Q6d-1. With respect to cost efficiency, outsourcing the SOC is more efficient than operating the SOC in-house (e.g., built by your organization's IT department).	Pct%
Strongly agree	22%
Agree	26%
Unsure	15%
Disagree	21%
Strongly disagree	16%
Total	100%

Q6d-2. With respect to preventing cyberattacks, outsourcing the SOC is more efficient than operating the SOC in-house (e.g., built by your organization's IT department).	Pct%
Strongly agree	22%
Agree	25%
Unsure	19%
Disagree	20%
Strongly disagree	14%
Total	100%

Q6d-3. With respect to detecting cyberattacks, outsourcing the SOC is more efficient than operating the SOC in-house (e.g., built by your organization's IT department).	Pct%
Strongly agree	20%
Agree	25%
Unsure	21%
Disagree	23%
Strongly disagree	11%
Total	100%

Q6d-4. With respect to containing cyberattacks, outsourcing the SOC is more efficient than operating The SOC in-house (e.g., built by your organization's IT department).	Pct%
Strongly agree	16%
Agree	23%
Unsure	17%
Disagree	26%
Strongly disagree	18%
Total	100%

Q6d-5. With respect to maintaining a strong cybersecurity posture, outsourcing the SOC is more efficient than operating the SOC in-house (e.g., built by your organization's IT department).	Pct%
Strongly agree	25%
Agree	27%
Unsure	13%
Disagree	21%
Strongly disagree	14%
Total	100%

Q7. In your opinion, are the data collected and used in your SOC too sensitive or confidential to be stored in the cloud environment?	Pct%
Yes, most of the time	17%
Yes, some of the time	43%
No	40%
Total	100%

Q8. What best describes the coverage, scope of monitoring and engagement level of your SOC?	Pct%
Part-time analysis and escalation support (nights, weekends and holidays)	25%
Full time monitoring and management support (24 hours 7 days per week)	52%
A long-term phased approach in which the scope changes based on our organization's maturity and operational characteristics	23%
Total	100%

Q9. What do you see as the main barriers to successfully operating the SOC? Please check the top three choices.	Pct%
Lack of executive-level support	21%
Lack of leadership	23%
Lack of visibility into the IT security infrastructure	65%
Turf or silo issues between the organization's IT security operations and SOC	57%
Outsourcing is inconsistent with the organization's culture	62%
Compliance with privacy and data protection requirements	33%
Compliance with internal policies and contractual requirements	21%
Insufficient proof points or measures of success	15%
Other (please specify)	3%
Total	300%

Q10. Using the following 10-point scale, please rate the effectiveness of your organization's SOC.	Pct%
1 or 2	8%
3 or 4	21%
5 or 6	29%
7 or 8	26%
9 or 10	16%
Total	100%
Extrapolated value	5.92

Q11. What can make your organization's SOC ineffective? Please select all that apply.	Pct%
Lack of timely remediation	63%
Lack of visibility into network traffic	69%
Too complex	56%
Lack of skilled personnel	54%
Yields too many false positives	49%
Other (please specify)	3%
Total	294%

Q12. Using the following 10-point scale, please rate the ability of your organization's SOC to gather evidence, investigate and find the source of threats.	Pct%
1 or 2	11%
3 or 4	18%
5 or 6	24%
7 or 8	26%
9 or 10	21%
Total	100%
Extrapolated value	6.06

Part 3. IT security personnel activities

Q13. Who **leads** your organization's SOC team? Please select only one choice.	Pct%
Chief information officer	21%
Chief technology officer	5%
Chief information security officer	25%
Chief security officer	3%
Head, enterprise risk management	7%
Head, lines of business (LOB)	18%
No one function (shared ownership)	19%
Other (please specify)\	2%
Total	100%

Q14. What are the most time-consuming tasks for your organization's IT security personnel. Please select your top 5 choices.	Pct%
Create, modify and update intrusion detection systems (IDS)	27%
Create, modify and update security information event management (SIEM) systems	36%
Discover vulnerabilities in information systems	33%
Evaluate and deconstruct malware software	47%
Install firewall and data encryption programs	43%
Maintain security records of monitoring and incident response activities	25%
Monitor compliance with security regulations	31%
Perform cyber and technical threat analyses	50%
Prevent hacker intrusion	50%
Produce situational and incident-related reports	15%
Remediate security issues	46%
Respond to requests for specialized cyber threat reports	43%
Use big data analytics to pinpoint security threats	51%
Other (please specify)	3%
Total	500%

Q15. What activities are most important to achieving the objectives of your organization's SOC? Please select your top two choices.	Pct%
Threat hunting	30%
Investigations	57%
Forensics	39%
Incident response	53%
Recovery operations	21%
Total	200%

Q16. Using the following 10-point scale, please rate the "pain" your organization's SOC security personnel experience in meeting their daily job requirements.	Pct%
1 or 2	9%
3 or 4	8%
5 or 6	13%
7 or 8	25%
9 or 10	45%
Total	100%
Extrapolated value	7.28

Q17a. What makes working in the SOC painful? Please select all that apply.	Pct%
Information overload	62%
Lack of resources	53%
Increasing workload causes burnout	73%
Being on call 24/7/365	71%
Inability to capture actionable intelligence	55%
Too many alerts to chase	69%
Inability to prioritize threats	60%
Lack of visibility into the network and IT infrastructure	72%
Inability to recruit and retain expert personnel	68%
Complexity and chaos in the SOC	49%
Losing to adversaries	51%
Other (please specify)	2%
Total	685%

Q17b. Have any of the above pain factors caused you to consider changing careers or leaving your job?	Pct%
Yes	65%
No	35%
Total	100%

Q17c. What is the likelihood that the above pain factors would cause experienced security analysts to quit your organization's SOC?	Pct%
Very likely	31%
Likely	35%
Not likely	19%
No chance	15%
Total	100%

Q18. What steps can be taken to alleviate SOC analysts' pain? Please select all that apply.	Pct%
More resources	51%
Better support and recognition from senior leadership	39%
Help in prioritizing incidents and tasks	49%
Automation of workflow	67%
Access to more out-of-the-box content (i.e. rules, playbooks)	52%
More PTO and vacation time	36%
Normalized work schedule	53%
Stress management programs and psychological counseling	48%
Other (please specify)	2%
Total	397%

Q19. Do you believe security analysts in your organization feel current threat hunting processes make them want to quit?	Pct%
Yes	52%
No	48%
Total	100%

Part 4. SOC security practices

Q20. To the best of your knowledge, which of the following types of exploits or compromises has your SOC identified over the past 12 months? Please check all that apply.	Pct%
Advanced persistent threats (APT)	29%
Botnet attacks	63%
Clickjacking	13%
Cross-site scripting	35%
DDoS	56%
Exploit of existing “known” vulnerability	80%
Malicious insider	68%
Ransomware	27%
Rootkits	25%
Spear phishing	69%
SQL injection	35%
Malware attack	98%
Zero-day attack	60%
Man-in-the-middle attack	56%
Other (please specify)	2%
Total	716%

Q21a. Does your organization track Mean Time to Remediate (MTTR)?	Pct%
Yes	48%
No	52%
Total	100%

Q21b. If yes, on average what is the MTTR for a security incident in your SOC?	Pct%
Within hours	9%
Within days	13%
Within weeks	36%
Within months	24%
Within one year	12%
More than one year	6%
Total	100%

Q22a. Does your company invest in threat intelligence feeds?	Pct%
Yes	51%
No	49%
Total	100%

Q22b. If yes, do threat intelligence feeds combine open source and paid feeds?	Pct%
Yes	54%
No	46%
Total	100%

Q22c. If yes, does your organization develop custom feeds based on the following?	Pct%
Industry	58%
Business	55%
Technology profile	60%
Our organization does not develop custom feeds	28%
Total	201%

Q23a. Does your organization have a threat hunting team?	Pct%
Yes	54%
No	46%
Total	100%

Q23b. If yes, what challenges does your threat hunting team face? Please select the top three choices.	Pct%
Too many IOCs to track	61%
Too much internal traffic to compare against IOCs	50%
Too many false positives	42%
Security tools can't keep up with volume of threat intel	32%
Historical data is unavailable to identify ongoing breaches	28%
Lack of internal resources/expertise	44%
Lack of internal visibility (i.e. not collecting the right or enough logs)	40%
Other (please specify)	3%
Total	300%

Q23c. If yes, does your SOC effectively leverage threat hunting to prevent incidents from happening?	Pct%
Yes	39%
No	45%
Unsure	16%
Total	100%

Part 5. Attributions (Strongly Agree and Agree response). Please rate the following statements using the agreement scale below each item.	Pct%
Q24. Our SOC provides a mature (tried and tested) security offering to the business.	40%
Q25. Our SOC offers 24/7/365 threat monitoring and management.	52%
Q67. Our SOC has high interoperability with the company's security intelligence tools.	37%
Q27. Our SOC provides services that are scalable in terms of the company's regional scope and size.	41%
Q28. Our SOC demonstrates commitment to achieving a strong security posture.	50%
Q29. Our SOC provides incident response services that can be deployed quickly.	43%
Q30. Our SOC is effectively managed.	49%
Q31. Our SOC helps us to better understand the external threat environment through the collection and analysis of information on attackers, methods and motives.	56%
Q32. Our SOC leverages insight gained from monitoring a large number of security events from a global customer base.	48%
Q33. Our SOC uses advanced analytics to identify threats through behavioral or statistical anomalies in security events, IT logs, network traffic or endpoint activity.	44%
Q34. Our SOC provides incident response capabilities that include attack mitigation and forensic investigation services.	42%
Q35. Our SOC effectively mitigates the risks after they are identified.	40%
Q36. Rich threat intelligence feeds are core to effective threat hunting.	57%
Q37. Threat intelligence context enriches data from the SIEM to support threat hunting and incident response.	55%

Part 6. Budget Questions

Q38. Are you responsible for managing all or part of your organization's cybersecurity budget this year?	Pct%
Yes	53%
No **(**Go to part 7)	47%
Total	100%

Q39. Approximately, what is the dollar range that best describes your organization's cybersecurity budget this year?	Pct%
Less than $5 million	8%
$5 to $10 million	38%
$11 to $50 million	41%
$51 to $100 million	11%
More than $100 million	2%
Total	100%
Extrapolated value (US$ millions)	$ 26.00

Q40. Approximately, what percentage of your organization's cybersecurity budget will go to SOC activities this year?	Pct%
Less than 5%	5%
5% to 10%	7%
11% to 20%	11%
21% to 30%	26%
31% to 40%	28%
41% to 50%	19%
More than 50%	4%
Total	100%
Extrapolated value	0.30

Part 7. Your role

D1. What organizational level best describes your current position?	Pct%
Executive/VP	8%
Director	17%
Manager	21%
Supervisor	15%
Technician/Analyst/Staff	35%
Contractor/Consultant	3%
Other	1%
Total	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	Pct%
CEO/Executive Committee	3%
Lines of Business (LoB) Management	12%
General Counsel	3%
Chief Information Officer	32%
Chief Technology Officer	8%
Compliance Officer	6%
Human Resources VP	1%
Chief Security Officer	3%
Chief Information Security Officer	21%
Chief Risk Officer	9%
Other	2%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food service	1%
Communications	2%
Defense & aerospace	1%
Education & research	3%
Energy & utilities	5%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	12%
Hospitality	2%
Industrial/manufacturing	7%
Public sector	10%
Retailing	9%
Services	11%
Technology & Software	9%
Transportation	5%
Other	3%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
1,000 to 5,000	24%
5,001 to 10,000	26%
10,001 to 25,000	30%
25,001 to 75,000	13%
75,000+	7%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.