SANS

A SANS Survey

Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey

Written by **Chris Crowley** and **John Pescatore**

Sponsored by:
ExtraHop

July 2019

Analyst Program

Executive Summary

This 2019 edition of the SANS Security Operations Center (SOC) Survey was designed to provide objective data to security leaders and practitioners who are looking to establish a SOC or optimize their existing SOCs. The goal is to capture common and best practices, provide defendable metrics that can be used to justify SOC resources to management, and to highlight key areas on which SOC managers can focus to increase the effectiveness and efficiency of security operations.

A few points are important in understanding the survey results:

Most of our respondents were from organizations headquartered in North America (57%) and Europe (17%), and most of their SOCs (123 of 355) had about 10 full-time employees—but staff size varied widely depending on organization size and sector.

We asked survey respondents whether they would participate in telephone or email drill-down interviews. About 15 responded, and we have included anecdotal information from these interviews. Most of the interviewees were from organizations with fewer than 15,000 employees.

SOCs' self-reported metrics indicate that they are most satisfied with the number of incidents they handle as well as the time it takes from detection to containment and eradication of the problem. The most frequently cited barriers to excellence were lack of skilled staff (58%) and the absence of effective orchestration and automation (50%).

For technology satisfaction across all NIST Cyber Security Framework (CSF) categories, the technology rated as highest performing was access control/VPNs (87%) in the protection category; while the lowest (of popular use) was AI/machine learning (ML) (53%) in the detection category.

We purposely kept many questions the same this year to investigate differences across multiple years, but there were major changes from 2018 to 2019. The aforementioned barriers didn't change, meaning that many SOC managers were unable to increase staff or use automation to make up the difference. Interview respondents who had success in improving SOC effectiveness and efficiency focused on increased SOC staff skills in key areas. The low satisfaction rating of the wildly hyped AI and machine learning tools is an indication that automation can augment staff skills, not replace staff.

The major avenues to improvement seem to be clearly articulating what services the SOC offers to the business (which leads to focus on building good use cases rather than buying new technology), and retaining staff by providing opportunities to learn and develop (although it helps to be the only SOC in town). Organizations frequently achieve good results by turning to external service providers to bolster their SOCs' capabilities—yet some organizations are resistant to involving external entities with security operations. We did see an uptick in organizations integrating network operations center (NOC) and SOC operations, an important way to increase both effectiveness and efficiency, especially when outsourcing is not feasible.

Key Results

- The most frequently cited barriers to excellence: lack of skilled staff (58%) followed by absence of effective orchestration and automation (50%)
- Highest-performing CSF technology: access control/VPNs (87%) in the protection category; lowest (of popular use): artificial intelligence (AI)/machine learning (ML) (53%) in the detection category
- For continued improvement:
  - Articulate services to the business.
  - Build use cases.
  - Retain staff through training and growth.
  - Use external managed security service providers (MSSPs) strategically to bolster weakness.
  - Closely coordinate with NOC/IT.

Explanation of Questions and Changes

The 2019 SANS SOC Survey questions were almost exactly the same as the 2018 questions. The intention was to minimize change because the questions were important to establishing and improving a SOC. With so few changes, we can complete year-by-year comparisons now and in the future. Results indicated no significant differences between 2018 and 2019. We attribute this mostly to the fact that little had changed in the top barriers SOC mangers listed.

To improve and expand the survey, we added detailed interviews to glean information from respondents that doesn't manifest well in datacentric questions. Further, because we don't have a defined population size (see the discussion in the 2018 SANS SOC Survey[1] for more details), the interviewees were selected by the following criteria:

- Job titles for most executive staff
- Areas of lower respondent representation

As a result, a SOC manager from the Asia-Pacific region would be included in preference to an additional CISO from North America, given that the respondent population is weighted heavily toward North America and Europe.

Another substantial change from the 2018 SANS SOC Survey is the inclusion of the NIST Cyber Security Framework as a mapping strategy for technology. The intention here was to capture not only what tools are used, but how they're being used. This approach, however, didn't provide the clarity we were hoping for. We'll use what we learned from this attempt to try a different approach in future surveys.

To help you with the various charts, we've applied color-coding. The rubric is:

Blue: Single-value chart

Grey: Multipart chart

Green: Satisfaction rating

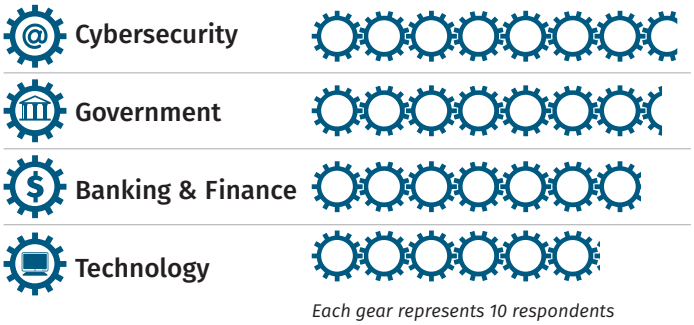
Yellow: Correlated to size or industry

Summary Demographics

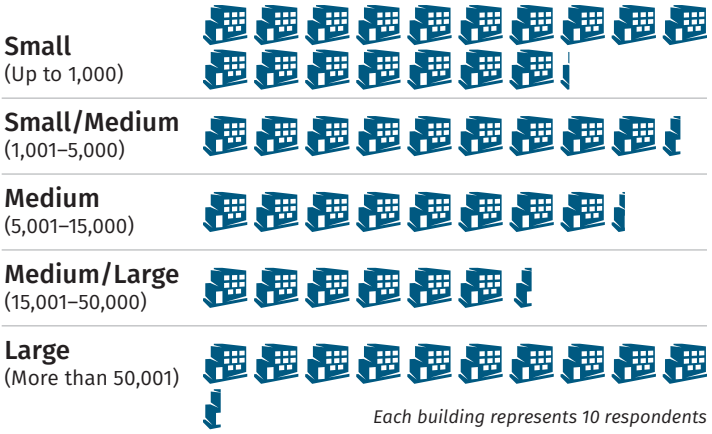
There's a push and pull regarding demographics. To try to provide everything for everyone, we have a simple infographic to familiarize you with our respondents, who were primarily from North America and Europe and in the cybersecurity industry as well as government, banking and finance, and technology. The individuals are technical staff, technical managers or SOC managers. The size of the organizations was distributed in the range from under 100 to over 100,000, with 101–1,000 being the single most common. See Figure 1 on the next page.

[1] "The Definition of SOC-cess? SANS 2018 Security Operations Center Survey," www.sans.org/reading-room/whitepapers/analyst/definition-soc-cess-2018-security-operations-center-survey-38570, p. 6. [Registration required.]

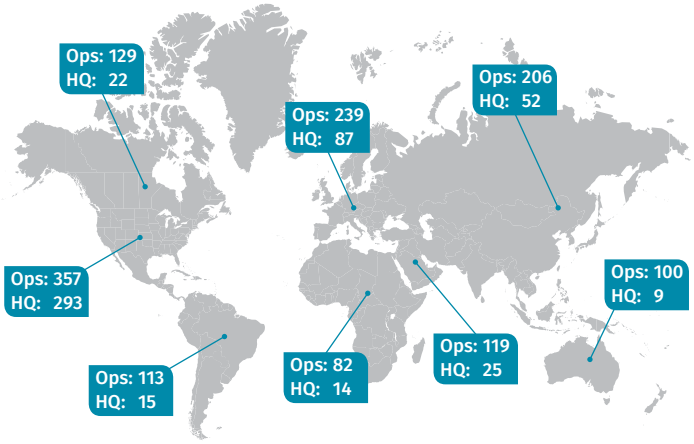
Top 4 Industries Represented



Organizational Size



Operations and Headquarters



Top 4 Roles Represented

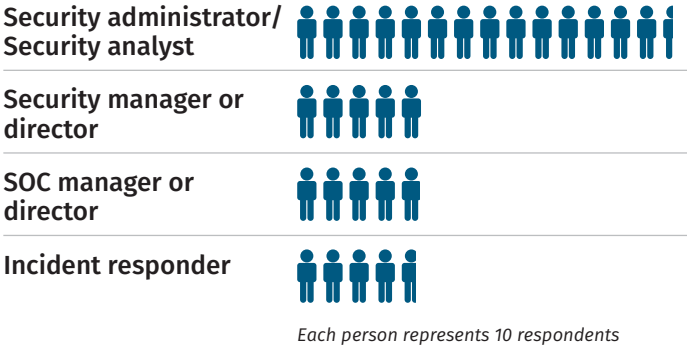


Figure 1. Key Demographic Information

Key Elements Defining a SOC

In the 2018 Survey we defined a SOC as: "A combination of people, processes and technology protecting the information systems of an organization through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects."[2] This hasn't changed. But there are a lot of terms that are often used interchangeably when people describe a security operations center. We asked what the SOC does internally, via outsourcing, or both. The ability to identify and respond to issues is the key aspect of the SOC and is frequently an internal capability. Architecture, planning and security administration are normal duties, as is ensuring that the organization's IT systems are in compliance with legal and industry requirements. Technical security assessments (such as penetration testing and vulnerability scanning), threat intelligence collection and use, and purple-teaming are less common, but still present. Perhaps next year we will try to find a consensus of attributes or capabilities that are the minimum requirements for characterizing something as a SOC. See Figure 2 on the next page.

Action Items

Clearly define what the SOC is and the measurable benefits (see the metrics section) it provides to your organization. Use this list as a basis to articulate the services offered and how they're offered.

For example: Detection is outsourced, triage from MSSP detection is internal; security architecture, vulnerability remediation, compliance verification and some pen testing are internal; incident handling is initially handled internally, with an outsourced contract for surge support; forensics isn't done unless the outsourced incident handling team does it. Other items not listed aren't done, such as threat intelligence, unless done in the course of staff duties.

[2] "The Definition of SOC-cess? SANS 2018 Security Operations Center Survey," www.sans.org/reading-room/whitepapers/analyst/definition-soc-cess-2018-security-operations-center-survey-38570, p. 4. [Registration required.]

SOC Capabilities

Enabling you to compare what your SOC does and how it functions with your peers' SOCs and functionality is a key goal of this survey. This section highlights the key SOC capabilities listed by respondents.

Outsourced Capabilities

A SOC is an expensive proposition with substantial operational costs and staffing needs. To minimize these costs, or to deal with staffing restrictions, organizations frequently look to outsource various aspects of their operations. The most commonly outsourced actions continue to be pen testing (and its permutations of red-teaming and purple-teaming), digital forensics and threat intelligence. It's interesting to note that pen testing and its variants are more frequently (as a ratio) done by "both"—internal teams and outsourcing. The core function of monitoring and detection is also frequently outsourced, usually (102 of 135 cases, or 76%) in a mixed in-house/outsourced arrangement, as seen Figure 3.

What activities are part of your SOC operations? What activities have you outsourced, either totally or in part, to outside services through a managed security service provider (MSSP) or in the cloud?
Leave blank those that do not apply. (N=360)

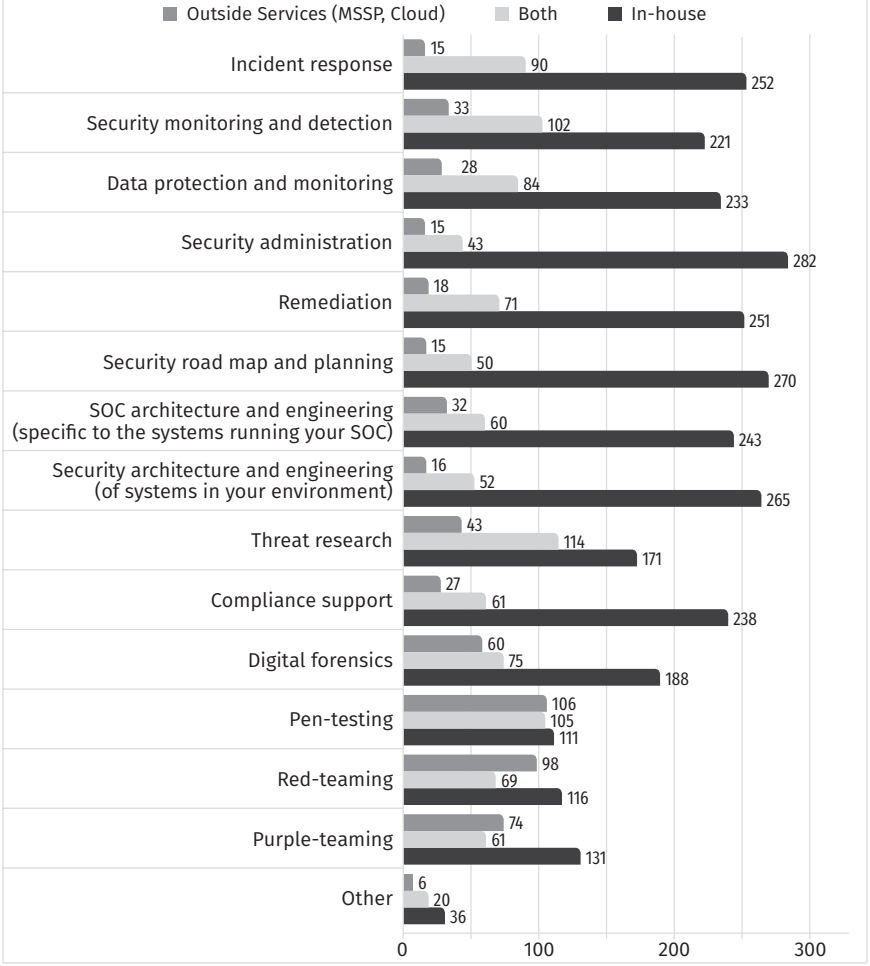


Figure 2. SOC Operations Activities

Outsourced Capabilities

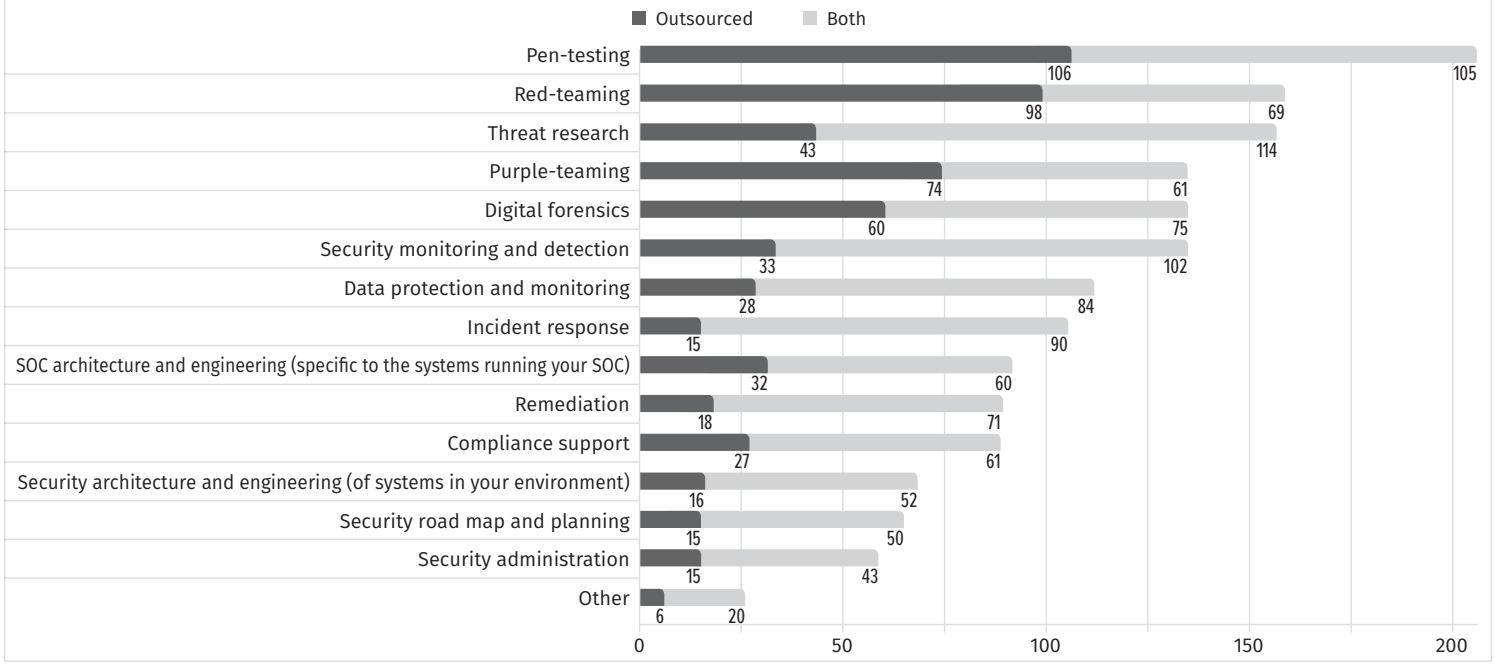


Figure 3. Outsourced SOC Capabilities

Many organizations keep these capabilities in-house (see Figure 4). This choice is likely indicative of organizations that have concerns about entrusting data to external entities or have experienced failures with outsourcing the capability and brought it back in-house. The most effective pen testing requires a strong understanding of how internal business processes operate and what the "crown jewels" of the business are. Cookie-cutter pen test engagements often miss the mark, because they lack this knowledge. These types of pen tests are typically done to meet a regulatory or industry requirement to pen test at least annually.

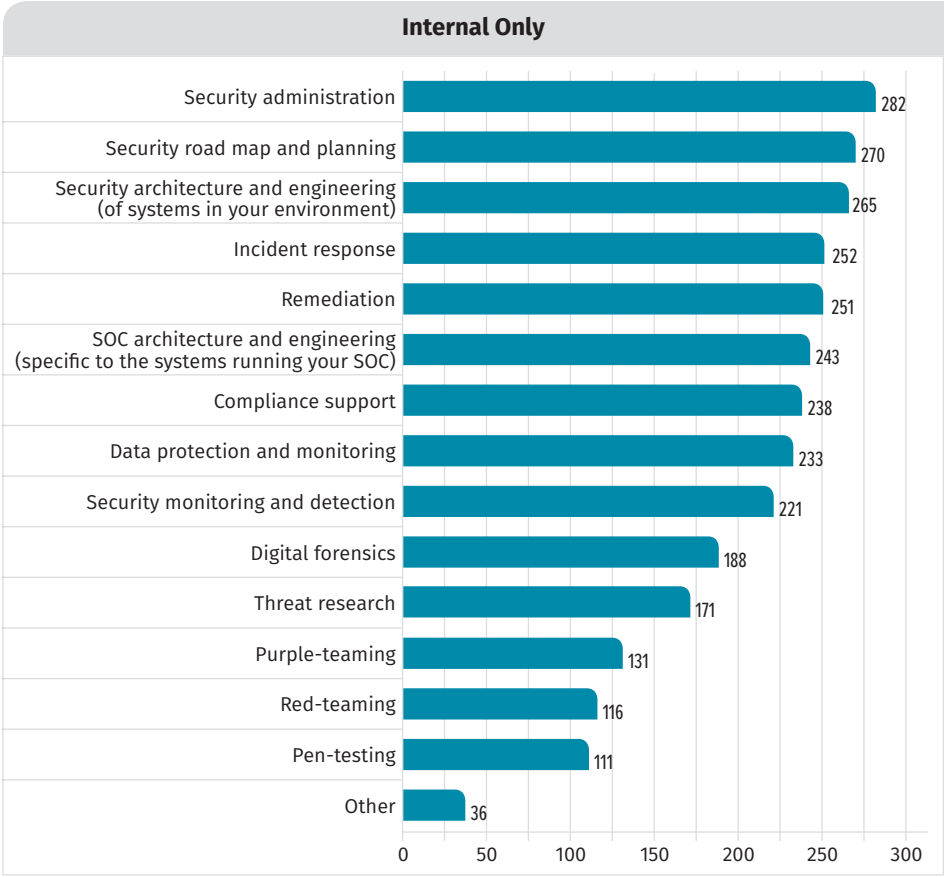


Figure 4. Internal SOC Capabilities

Here we turn to some of our in-depth interviews to shed further light on how people leverage outsourcing. Several telephone interview respondents were MSSPs. Other respondents were organizations that used MSSPs for monitoring and Tier 1 response. This gives a nice point and counterpoint on the perspective of MSSPs for security monitoring and detection.

The common thread from the MSSPs was that a new customer would invariably consume a higher level of SOC resources for the first six to nine months—until standard use cases were tuned to match the business operations:

> *"The early days of a new SOC customer can be a little bit hairy. The use case development won't be great. It'll be producing alerts that aren't working real well. It'll start to taper off as detection development improves and the efficiency of the work improves. Twenty use cases in month 1 will produce maybe twice as much consumption as 20 use cases at month 9."*

One customer of an MSSP for managed detection cited the need to communicate effectively with the service provider to achieve value:

> *"Make sure that your metrics for tracking the success of your SOC/security organization take into account contributing factors, such as incident communication and tasks assigned to other teams inside and outside of the organization, and that those parts are centrally documented. Having disjointed mixtures of communication internally and between you and your MSSP bouncing between email, IM, word of mouth and your CMS/ticket system can diminish a manager's visibility into day-to-day and week-to-week interactions between the SOC and the other technical teams in the company. This makes it more difficult to understand where to focus effort for improving the interaction between their people and processes to improve the organization as a whole."*

Action Items

Define an outsourcing strategy if you don't have one, and compare the capabilities you intend to outsource with what your peers are doing. Pay careful attention to articulating needs to providers if you intend to outsource, and keep reinforcing those expectations and assessing performance. If you haven't figured out the details of what you need from the service provider, anticipate 6–12 months of on-ramp time to achieve a normal steady state of operations.

Incident Handling

Once the SOC identifies a potential issue, initial verification is typically done by the SOC, which hands the incident off to a response team to conduct preliminary containment actions and further investigation. This is when the incident response (IR) process begins. Most of the respondents keep IR in-house (266 of 282 responses, or 94%). Of the internal responders, most (204 of 266 responses, or 77%) IR teams are part of the SOC. See Figure 5.

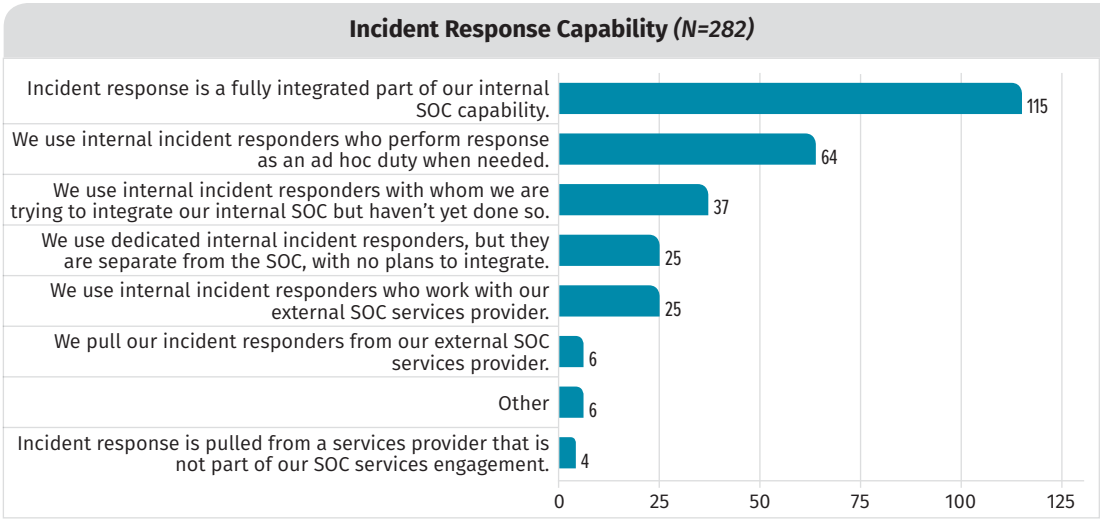


Figure 5. IR Capabilities

Action Items

Do a tabletop walk-though of a common incident scenario and one that is more unusual. Use that walk-through to demonstrate that the IR strategy you have in place is the optimal one for your organization. If it is not optimal, build an improvement plan to get better.

Knowledge Management

During telephone interviews conducted with a sample of the survey respondents, we asked what knowledge management tools they used to document process-related knowledge across the team and support both repeatability of operations and the ability to quickly bring on new analysts. Smaller SOCs (fewer than five analysts) relied on more informal methods such as "one gigantic OneNote document" or the use of SharePoint. Larger SOCs were commonly using Jira for trouble tickets and were using Confluence for collaboration. Larger SOCs that were integrated with IT or the NOC tended to use ServiceNow or BMC Remedy for trouble tickets and had no access to Confluence. SharePoint dominated these large, integrated SOCs.

None of the interviewees was using a formal playbook, although one was budgeting to move from SharePoint to a formal playbook solution.

Action Items

Develop your system for capturing tribal lore into documented internal guidance for new and seasoned staff. Capture the pain points from onboarding new SOC staff so the next iteration has a smoother transition into effective performance within the SOC. Document the necessary and optional training for staff. Document details of high-profile incidents that have occurred in the past so new SOC members understand the organization's past negative experiences and can try to avoid them.

MSSP

Of our 517 responses, 302 (58%) of the SOCs represented in the survey aren't service providers. The SOC is primarily an internal phenomenon in our survey's population, with 412 of the 517 respondents (80%) stating their "customers" are internal to the organization. Roughly three out of four (74%) of those internal entities do not self-identify as a service provider to the organization. See Table 1.

Table 1. MSSP Self-Identification

Yes, customers outside of my organization	105
Yes, internal service provider	110
No	302
Answered	**517**

For those who consider themselves internal service providers, 75 of 111 (68%) are the mandatory provider, meaning that members of the organization are required to purchase services from the SOC and may not hire an outside service.

Action Items

Determine whether becoming a service provider for your organization is the right way to offer your SOC service. Such a model is tenable only when the SOC is somewhat mature and the organization has a good security culture. The "internal MSSP" approach will drive maturity, efficiency, performance and customer orientation. If you launch this strategy too soon, you risk losing the funding needed to achieve maturity as constituents move to external providers.

Technology Coverage

Which assets are monitored by the SOC (and which are not) is typically based on resource constraints. Because organizations cannot defend everything, it is interesting to see when organizations choose to leave assets exposed or less protected.

Budget and staffing constraints often mean that SOCs focus on IT systems only, and not operational technology (OT) or other specialized systems. Only a small number of SOCs (10%) say they have all of the smart systems present in their environment covered by the SOC. See Figure 6.

Leaving smart systems unprotected is common practice per the above chart. Only 62 of the 353 respondents said they know they're monitoring "smart systems." About a third of the respondents (121) said they know they don't monitor these systems and intend not to monitor them. "Unsure" and "we haven't inventoried them yet …" are implied risk decisions that result from failing to integrate security into the IT procurement and deployment process.

Does your SOC support nontraditional computing devices such as smart sensors, building devices, building monitoring, manufacturing, industrial control systems and other items considered as part of the Internet of Things? *(N=353)*

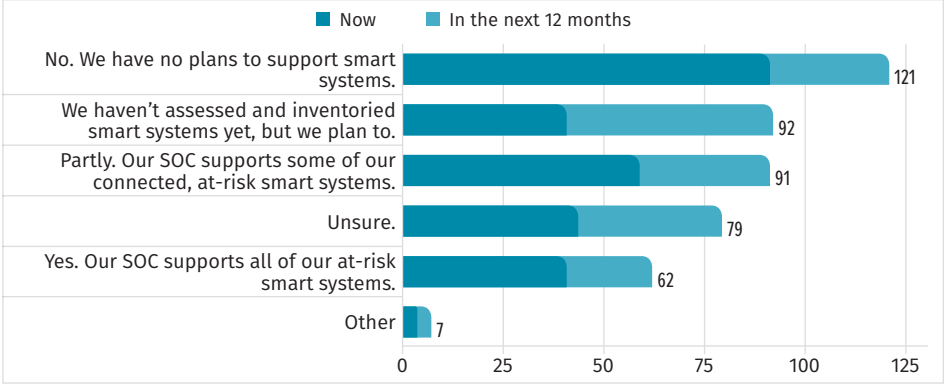


Figure 6. Support for Nontraditional Devices

SOCs struggle to monitor and track current assets. Having an accurate inventory of all endpoints and users in a network can be a challenge. The root of the problem comes from the fact that IT operations has the same problem—even IT organizations that have matured enough to establish configuration management databases (CMDBs) rarely find that the CMDB is even 80% accurate at any given time. SOC asset inventory approaches that rely on host-based agents can at best match this level. SOCs that add network scanning or credentialed access approaches are often in the position of telling IT operations that the CMDB is incomplete or out of date. The increased use of infrastructure-as-a-service (IaaS) by IT has created blind spots for traditional network scanning approaches, however. SOCs need to develop the capability of integrating information from inventory and asset management tools available in all IaaS offerings. This seems to be a perennial failure of SOCs, as seen in Figure 7.

Do you have a full inventory of endpoints on your network so that, if you have an issue with a specific IP address, you're able to correlate that asset to a known system owner and/or responsible user? *(N=314)*

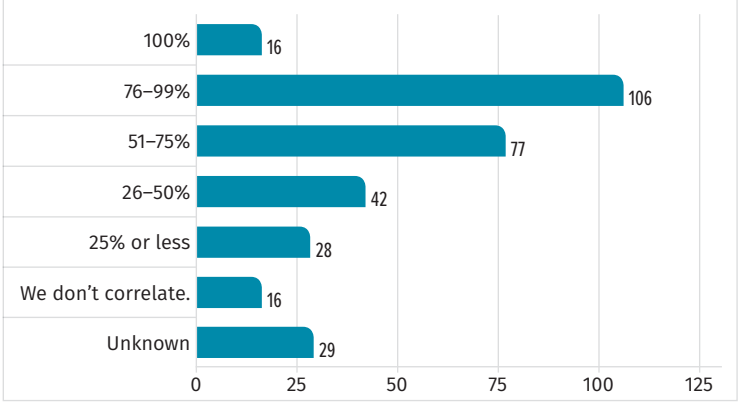


Figure 7. Endpoint Inventory Mapped to Asset Owners

A significant percentage of endpoints cannot be correlated to a specific user, hampering response and remediation operations. Not much has changed on this front since last year; as seen in Table 2, the values are nearly identical.

Table 2.
Year-Over-Year Endpoint Mapping Capabilities

	2019	1018
Unknown	29	28
We don't correlate.	16	25
25% or less	28	26
26–50%	42	31
51–75%	77	64
76–99%	106	103
100%	16	19
	314	**296**

The best way to address the monitoring of and response to new technologies is to ensure that SOC teams are aligned with the IT operations of the organization. Although we saw some improvement this year, most SOCs still aren't fully leveraging the potential of interactions with the NOC. If you aren't consistently leveraging this "sibling" in your organization, you're missing efficiency and knowledge opportunities. An encouraging portion (34%) of SOCs are capable of doing this, with 122 of 363 respondents saying they are either fully integrated or effectively working together. See Figure 8.

What is your SOC's relationship to your network operations center (NOC)? *(N=363)*

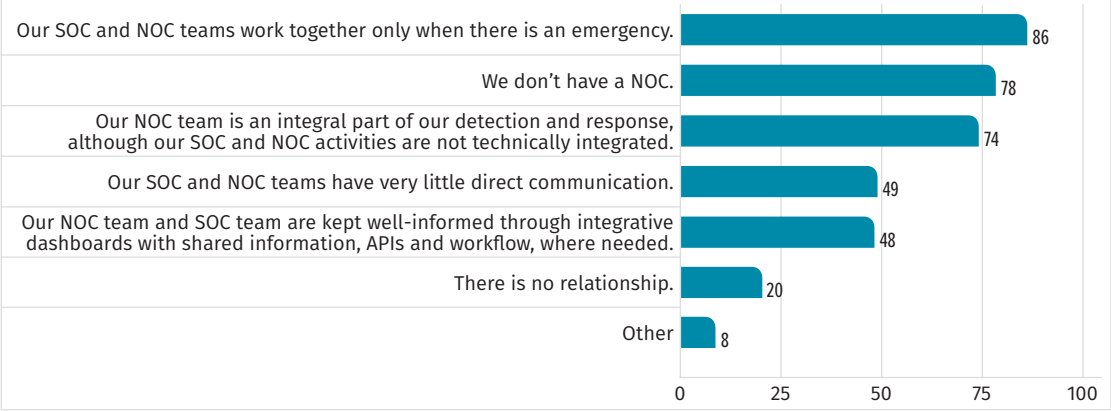


Figure 8. SOC/NOC Relationship

Funding for SOCs

How organizations acquire security funding for SOCs is very tightly coupled to the governance structure of the organization. No single pattern emerged from the survey or the interview responses. A few points did come across from our interviews.

No SOC manager reported having to work with a "zero-based budget" and justify SOC staffing and technology budgets from scratch each year.

Action Items

Leverage native capability or add external monitoring software to all new cloud, IoT and mobile projects for coverage. Vendors have solutions ready to help you. Play catch-up, if necessary, to monitor devices that are already deployed. Continue to expand coverage of all standard IT systems, and more closely align with IT operations to keep pace with changing organizational demands. If your organization says it can't do this, look to other institutions that have accomplished closer integration for examples of how to accomplish this effort. There is usually a managed operational capability and consensus on inclusion of security in place before technological solutions can be deployed effectively.

Some SOCs are funded as a "tax" on business units, whether or not the business unit decided to use the SOC services. This provided an incentive to business units to use the centralized SOC services and provided a stable base of funding. This model was commonly used when centralized network services or IT in general were an automatic cost.

SOCs using MSSP services were generally able to simply pass along increases in prices from the MSSP. MSSPs often provide metric and benchmark data across their customers that allow MSSP customers to justify new or increased funding in internal security controls and operations.

Action Items

Identify potential funding vehicles that are currently unutilized or underutilized. Make use of metrics to demonstrate value provided by the SOC. Look for ways to share your newly acquired assets with NOC and governance, risk management and compliance (GRC) teams to drive closer coordination and unify efforts.

SOC Size

Security managers often ask how many staff members are required to run a SOC effectively. It is our intention to provide some numbers that will enable you to compare your SOC with others. There's a danger in doing so, of course. All SOCs are not equal. The other SOCs may be underfunded and not performing well, so the number of employees based on this consensus might not reflect the status or maturity of your organization. More sophisticated and persistent attackers might be targeting your organization rather than focusing on this survey's other respondents—meaning you need more people to thwart this adversary. Caveat lectorem.

Overall Responses

We asked respondents to describe the size of their SOCs in two general staff roles: analysts and those involved in maintaining the SOC systems.

The number of analysts employed in SOCs falls primarily in the two-to-five range (123 responses, or 35%). This is not calibrated based on organization size, just overall responses to the survey, as seen in Figure 9.

Similarly, the number of those assigned to maintain systems also falls mostly in the two-to-five range (119, or 34%), as seen in Figure 10.

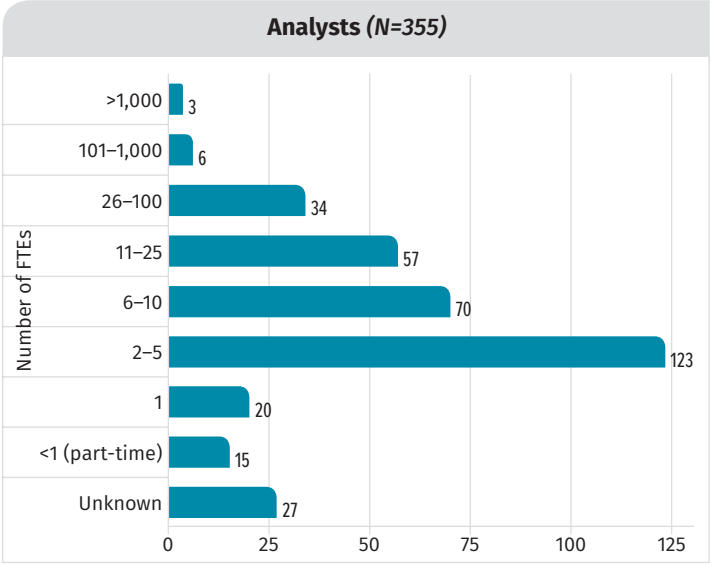


Figure 9. Full-Time Analysts Who Use SOC Systems and Services

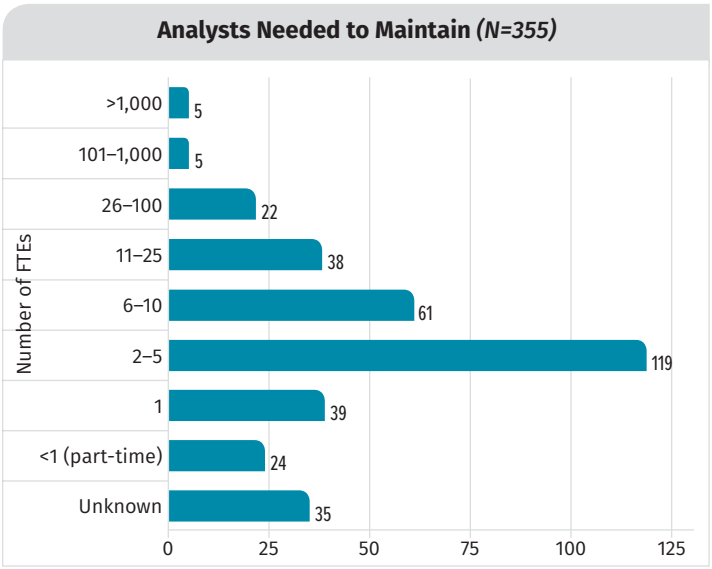


Figure 10. FTEs Needed to Maintain SOC Systems and Services

Adjusted Responses by Organization Size

Taking into account the organization size is probably a worthwhile dimension to add to provide a more relevant comparison. Table 3 provides a glimpse at the number of SOC team members.

Table 3.
SOC Team Analysts by Organization Size

Organization Size (by Workforce Size)	Common Number of Analysts
<10,000	2–5 (99 of 204)
10,000–15,000	6–10 (9 of 20)
15,001–100,000	11–25 (23 of 67)
>100,000	26–100 (13 of 37)

These numbers are within typical norms for IT and IT security staffing. Surveys by Gartner and others have typically shown that a 10,000 employee organization will have on the order of 300 IT staff and 9 security staff.[3] This represents an average of 3% of employee headcount for IT staff and 3% of IT staff headcount for security. The spread for the majority falls between 2–5% for each of the ratios. Where an organization falls in that range is not strictly budget-driven—lower staff levels with higher budgets for training and tools often provide higher levels of service. Overall business governance and how IT services are governed and delivered are usually the biggest factors affecting staffing ratios. This question's correlation to organization size always results in interesting outliers. The winner this year: the respondent who indicated that the organization size is greater than 100,000, but there's only one part-time analyst in the SOC. If that's you, the authors of this paper want to visit your SOC to see how it functions. See Figure 11.

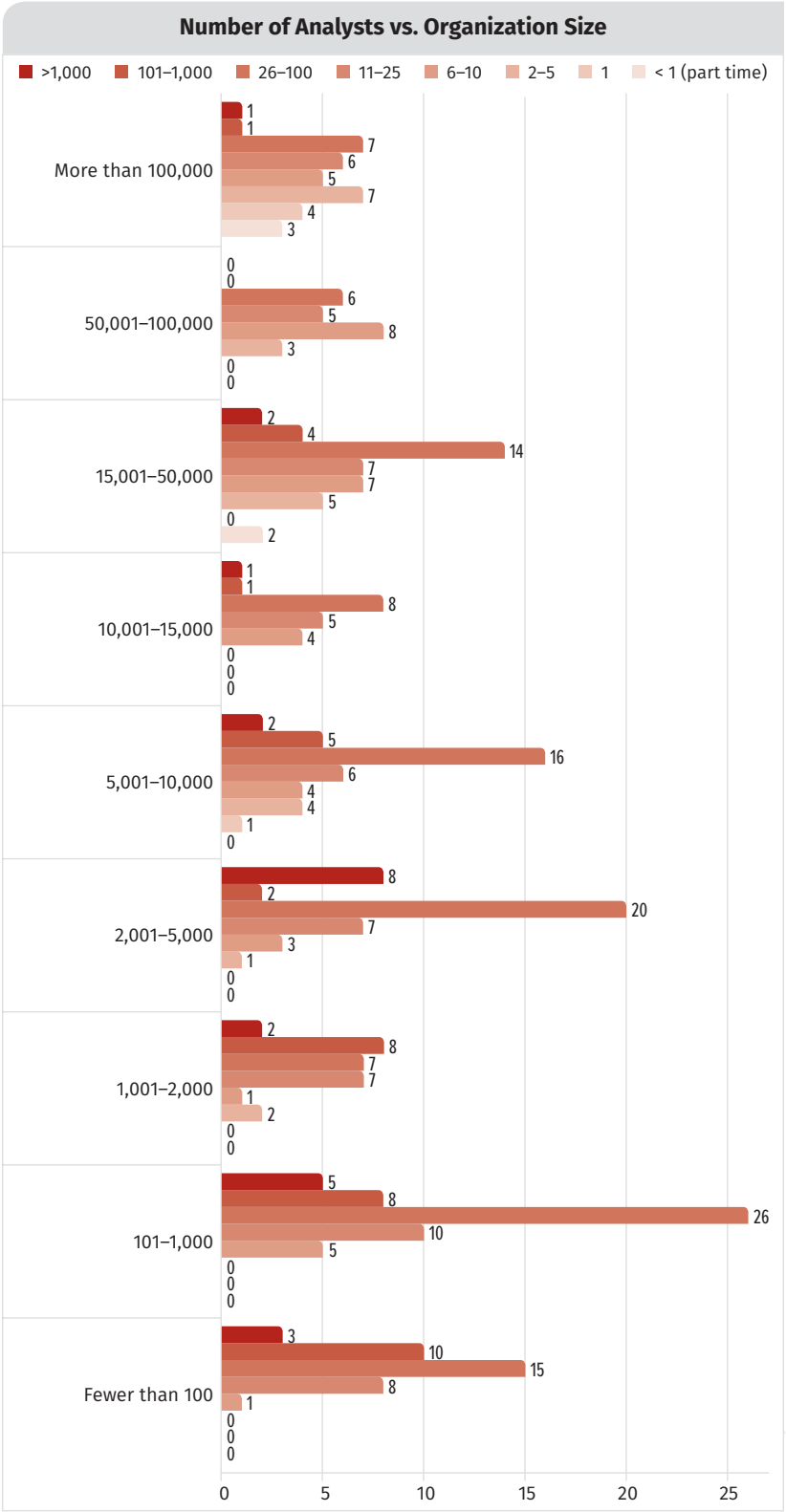


Figure 11. Number of Analysts by Organization Size

Hiring and Retention Interview Questions Insights

Since we're talking about the number of people in the SOC, we want to address effective hiring and retention of the right SOC analysts and maintainers. Respondents said that stability of personnel in the

[3] www.gartner.com/document/code/316640?ref=grbody&refval=3832268 [Subscription required.]

SOC overcomes a lot of obstacles. Teams that work together for long periods of time essentially develop common "playbooks," even if they are not formally documented or automated. The best of both worlds is a stable team that has taken the time to document the processes used, shortening the training time for new employees, making the typical surge staffing during emergencies more effective and reducing the disruption of unplanned staff leaves. Accomplishing low turnover came from involving analysts in use case and detection development, providing career growth and enabling regular rotation opportunities to keep people learning. Of course, among SOC teams reporting the lowest turnover, the major common denominator turned out to be a physical location in remote locations!

Action Items

First, determine if the size comparison provided here is applicable for the situation your SOC is in. It might not be an effective or fair comparison. Look at the size depicted, then develop a justification for adding staff if that's what you think this survey suggests. If you need to add staff, reach out to existing employees looking for a career development path into security to retain institutional knowledge and provide an incentive for everyone to do their job well.

A variety of hiring/staffing strategies are in use across respondents. Many use MSSPs for L1/L2 monitoring and high-level analysis, thus eliminating the need to continually fill the higher-turnover roles. Those using MSSPs focus on education and skill enhancement of internal staff to enhance productivity instead of increasing staffing levels. For those staffing the SOC internally, the internal network and IT organization are often the first places for recruitment. Leadership knows those people have both the IT skills and some level of knowledge of the business. Internship programs were frequently cited as well.

> *"We are using intern[s] [in] real job programs to find new hires for SOC shifts. We are also training system or network guys to transform them [in]to security engineers."*

SOC Architectures

The SOC might be an entity housed in a single room in one location, or it might be a globally distributed, follow-the-sun type of structure. We asked the respondents about their current structure and how they intend to change that structure in the next year. Their responses are illustrated in Figure 12.

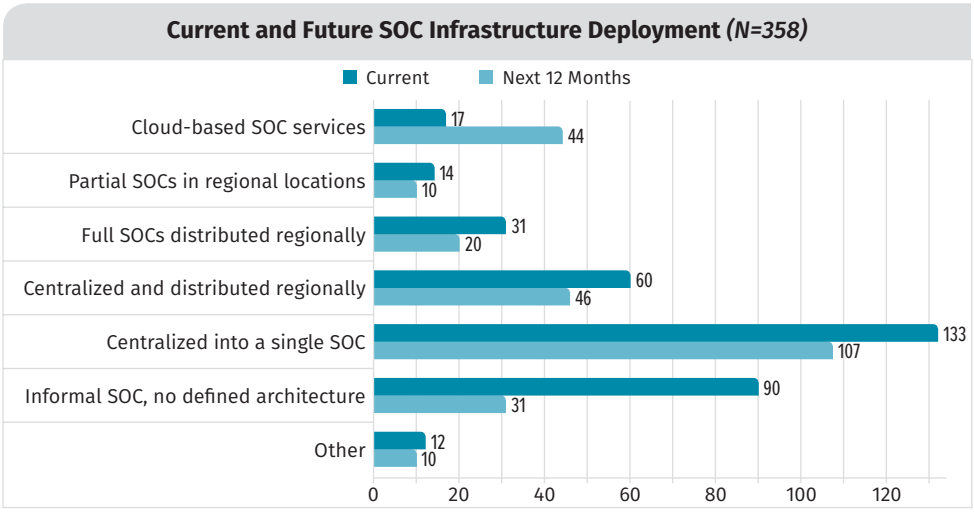


Figure 12. Current and Future SOC Infrastructure Deployment

It is difficult to account for the permutations of these different arrangements. Most common, by far, is the single centralized SOC addressing all data. This centralization is problematic because of data protection laws and regional variation of requirements, as well as tactical understanding of the systems in use. Interestingly, a small percentage of these respondents will be moving away from this architecture in the coming year.

It's telling that many organizations are moving to cloud services for their SOC architecture (from 17 currently to 44 in the coming year). This approach realizes the gains typically associated with cloud services for IT: fault tolerance and the perception of lower cost of operation. However, a recent Google cloud outage illustrates the risks that must be considered: The Google response team was dependent on cloud-based collaboration tools during investigation and restoration operations. These tools didn't work during the outage, greatly complicating security operations.[4] Cloud service providers do have outages and while most fall within the bounds of published SLAs, SOCs might have regulations (Europe's GDPR and others), as well as critical needs that require uptime of certain tools and processes.

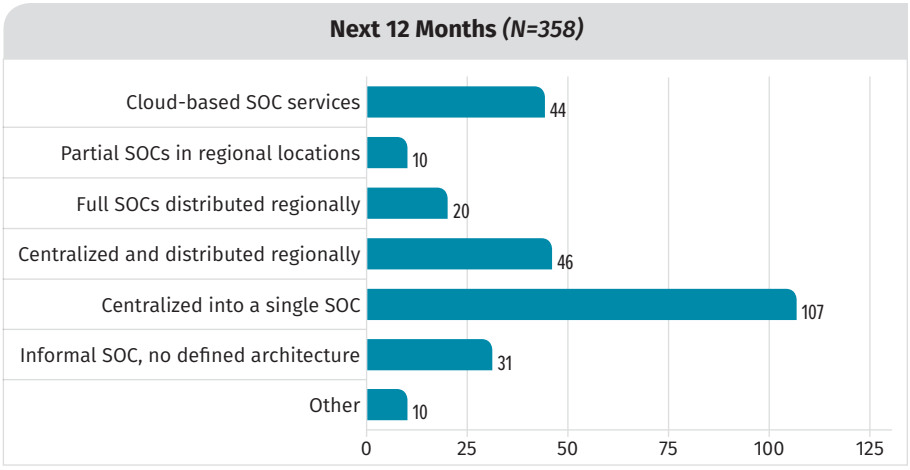


Figure 13. Expected SOC Change in Next 12 Months

Perhaps most rewarding is that those with no defined SOC architecture should decrease from 90 today to 31 in the coming year. That move represents a significant improvement. The fact that 31 organizations will still be following a technique commonly derided as, "Fire, aim, ready!" highlights the potential for continued development of the implementation of SOCs in all organizations. See Figure 13.

Action Items

If you don't have a defined architecture for your SOC, start the process today! Develop a clear picture of what architecture you are authorized to deploy. Address regional data protection laws. Plan for optimized architecture to gain efficiency and increase alignment with system needs.

Technology in Use

Most organizations think of technology rather than the processes and people involved when they set out to create a SOC. This is typically because it is easier to quantify the technology aspect of the SOC. Further, the technology is absolutely necessary, so it needs to be purchased and operated.

This year we attempted to map to the NIST Cybersecurity Framework categories to bundle technologies into identification, protection, detection, response and recovery roles, recognizing that many tools have multiple functions. While these categories are useful for illustrating core needed capabilities to management, in reality there is a lot of overlap between the categories.

Overall, people are satisfied with the tools. Judging by the raw numbers of tools we placed in each category based on their primary functions, vendors are primarily selling tools in the "protection" and "detection" categories. If you're a vendor, take note. There's a lot of room in helping organizations with the identification, response and recovery categories.

[4] www.sans.org/newsletters/newsbites/xxi/44

Identification

Respondents report high levels of satisfaction with SIEM products, but when asked about the two key functions provided by SIEM (log management and risk assessment), satisfaction was much higher for log management, as seen in Figure 14.

Many organizations are using a "compliance/reporting SIEM" and another product for risk analysis, assessment and prioritization. As previously noted, satisfaction with asset inventory tools remains low, even though the technologies are mature. Lack of IT operations maturity and increased use of IaaS are the primary drivers.

For each technology used for identification, defined by the CSF as "develop[ing] an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities," rate your satisfaction with its performance. *(N=345)*

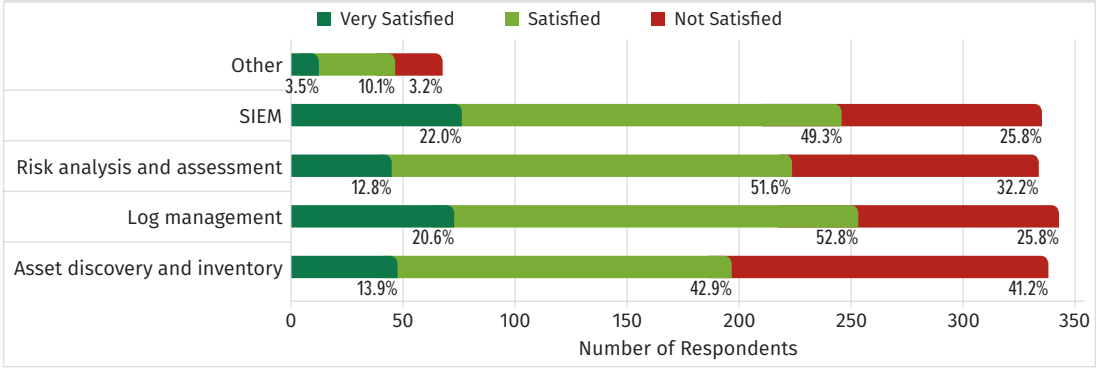


Figure 14. Identification Technology Performance Satisfaction

Protection

Despite many claims that "the perimeter is dead," the traditional perimeter protection capabilities received the highest level of satisfaction: access control/VPN, web proxy, next-generation firewall, ingress filtering, etc. See Figure 15.

Until businesses start sending paychecks to customers and shipping products to employees, there will be the need for a perimeter. The key is extending the traditional on-premises perimeter to include the cloud and mobile business operations as part of the monitored and protected portfolio of assets.

Internally focused and host-based protection approaches, such as data loss prevention (DLP) and whitelisting, continue to see low levels of satisfaction. These technologies not only require continual tuning to avoid false positives but they often require the cooperation of IT operations, which complicates deployment and operations.

For each technology that you use for protection, defined by the CSF as "develop[ing] and implement[ing] appropriate safeguards to ensure delivery of critical services," rate your satisfaction with the performance of the technology. *(N=314)*

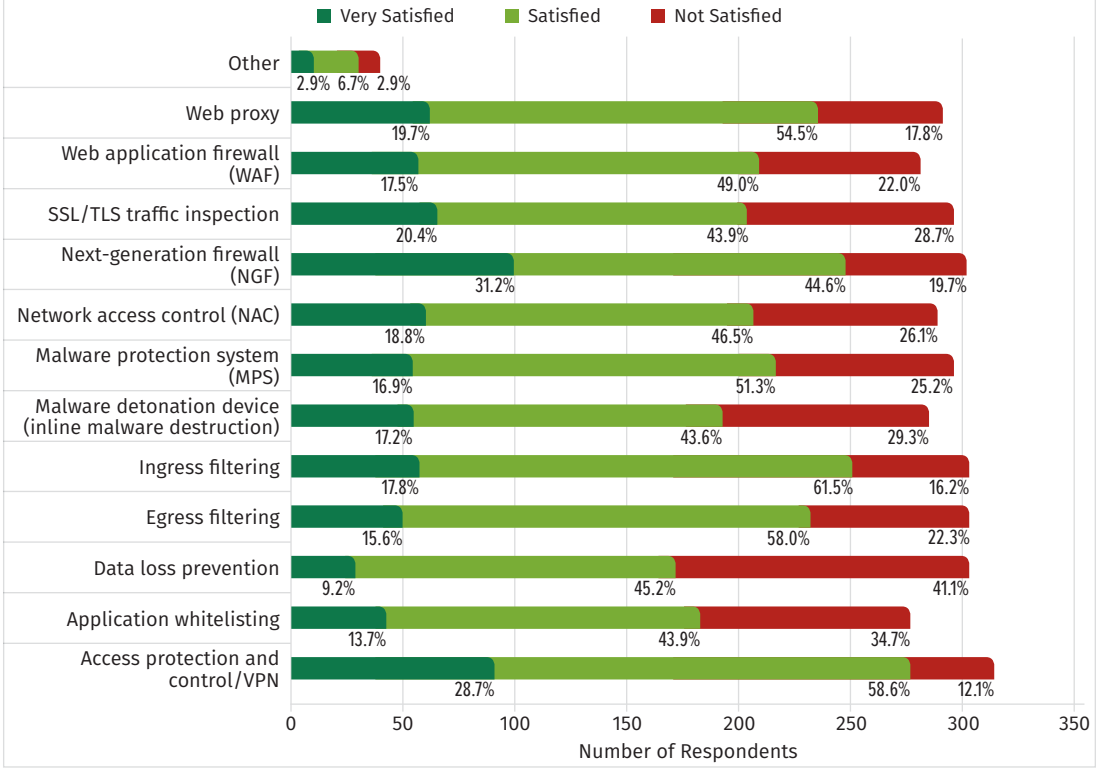


Figure 15. Protection Technology Performance Satisfaction

Detection

Network-based detection tools got the highest levels of satisfaction, as seen in Figure 16.

As pointed out earlier, when asset inventory accuracy levels are low, network-based tools are more effective than host-based tools that depend on agents being present on every endpoint. Organizations that have integration between NOC and SOC can have high levels of visibility and rapid detection, even on IaaS-based systems.

The highest count of dissatisfaction came from AI/machine learning tools. These technologies can effectively augment skilled staff, but they have been overhyped as solving the staffing problem on their own. The key areas of complaint center around frequent false positives, requiring high levels of involvement by knowledgeable and skilled analysts. Tool vendors should be competing on low levels of false positives, as opposed to focusing only on low levels of false negatives.

For each technology that you use for detection, defined by the CSF as "develop[ing] and implement[ing] appropriate activities to identify the occurrence of a cybersecurity event," rate your satisfaction with the performance of the technology. *(N=312)*

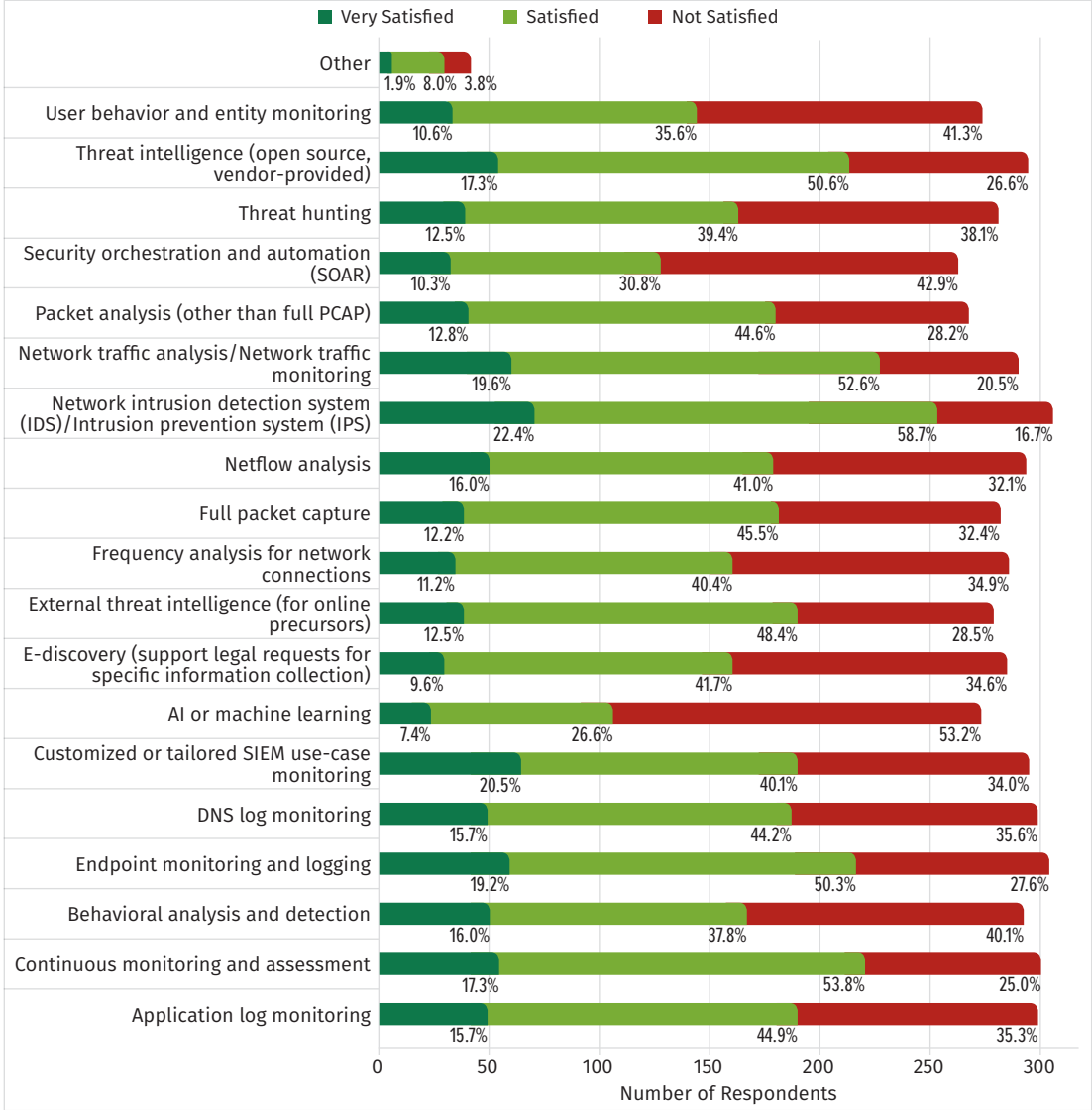


Figure 16. Detection Technology Performance Satisfaction

Response

DDoS filtering services have matured and received high levels of satisfaction. Deception technologies are not yet widely used and had much lower counts of satisfied customers. Endpoint detection and response (EDR) agents on endpoints fall in the middle—market penetration is rising, probably due to vendor improvements in the manageability and accuracy of the tools. See Figure 17.

For each technology that you use for response, defined by the CSF as "develop[ing] and implement[ing] appropriate activities to take action regarding a detected cybersecurity incident," rate your satisfaction with the performance of the technology. *(N=273)*

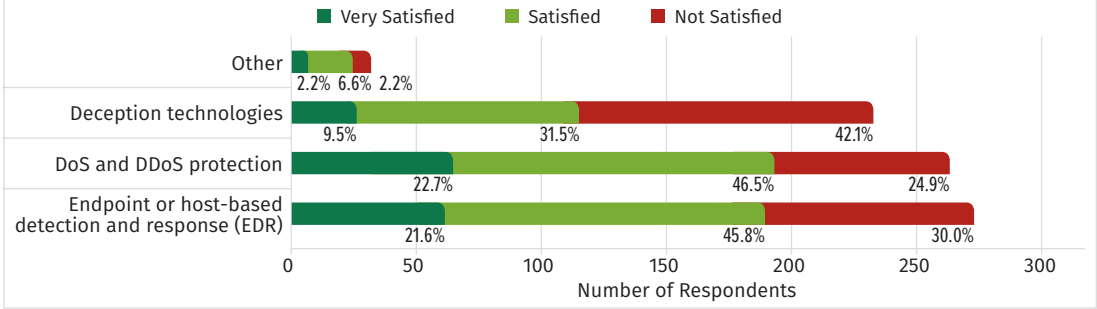


Figure 17. Response Technology Performance Satisfaction

Recovery

Recovery from the inevitable issue should be fast, effective and complete. Leveraging business continuity and disaster recovery plans that address normal operational interruption should be where organizations start. Well-managed IT operations should have the ability to effectively and rapidly restore a system that was affected. The most "very satisfied" responses were for gold standard refreshment, frequently accomplished through virtualization. This doesn't seem to address the data content, but it's a great capability to have in place. See Figure 18.

For each technology that you use for recovery, defined by the CSF as "develop[ing] and implement[ing] appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident," rate your satisfaction with the performance of the technology. ***(N=268)***

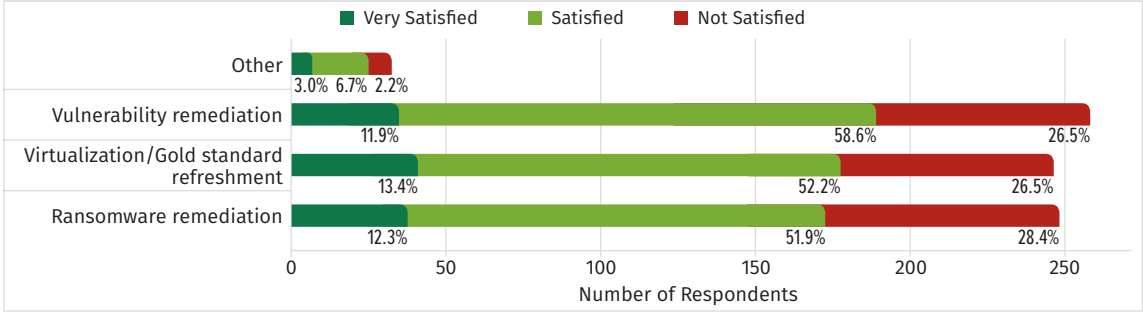


Figure 18. Recovery Technology Performance Satisfaction

Flaw remediation is something that would be better undertaken before a security incident. We hope the people reporting satisfaction with the performance of these tools are helping to prevent the incident in the first place by remediating flaws.

That vendor products exist to specifically remediate ransomware (and people are primarily satisfied with them) is tacit acknowledgment that data backup and restoration solutions aren't the preferred way to recover the information that had been on systems. The phenomenon of ransomware has been interesting to observe over the past few years, as attackers have monetized compromised systems through ransomware instead of DDoS and other bot-like behavior. Cryptocurrency mining appears to be the other primary monetization scheme, since it doesn't require a human to choose to pay the ransom.

Action Items

Check your technology. If you're dissatisfied in a technology or category where most other respondents are satisfied, you're either using the technology incorrectly, or your technology selection methods have led you to choose the wrong product.

If you're a tool vendor or developer and are looking for a less crowded area of the market, seek ways to help your customers develop remediation.

Have a way to verify the integrity of your data, or to recover data if it is lost from any sort of incident, including ransomware.

Metrics in Use

There's an ongoing trend in the service industry to ask for feedback. Stepping out of a ride-share vehicle, you'll frequently hear, "Please give me a five-star review if you can!" Some organizations are obsessed with scoring five stars on feedbacks and reviews. Little wonder, since the ranking score is often what drives customers to select one establishment over another.

In the information security field, we select the more austere strategy of defining metrics and service level objectives for the SOC. For good reason, too! This isn't about people's opinions. What's actually important is quantifiable, objective assessment of performance.

Most people rely on the SIEM to merge event data with other security-related data. SIEM-based correlation of event data is one source of SOC metrics, but respondents report low levels of satisfaction with the area of the technology. The SIEM is the technical tool from which much data for metrics can be derived. It's insightful to observe how this event data correlation drives our assessment of SOC performance. We can easily count the items logged, and this is where most people stop with their metrics. See Figure 19.

How does your SOC correlate and analyze event data, IoCs and other security- and threat-related data? ***Select those that most apply. (N=275)***

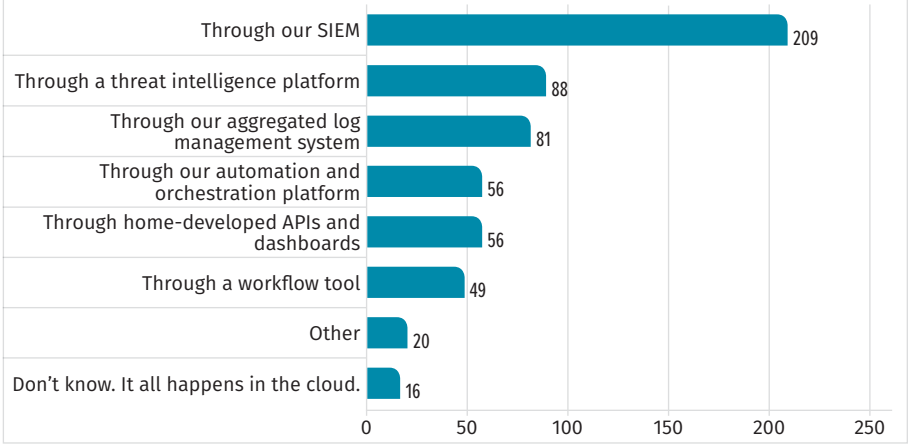


Figure 19. Correlation and Analysis of Event Data, IoCs and Other Data

The more difficult metrics to develop assess how this collection of data provides value to the institution. The metrics we asked about were many and varied (see Figure 20). In addition to the inquiry about each metric's use, we also checked how they were used.

That a quantity-based metric such as the "number of incidents handled" is the most common response is not at all surprising: It's easy to count; it's easy to extract this data in an automated fashion; and it's an easy way to proclaim, "We're doing something!" Or, "We did more this week than last week!" That respondents say "consistently met" to this is fascinating. How can an organization predict how many problems there will be in a given time frame?

Metric—A measure used to evaluate a process quantitatively

Service Level Objective—An expected performance value

Which of the following metrics do you use to track and report your SOC's service or performance? ***(N=145)***

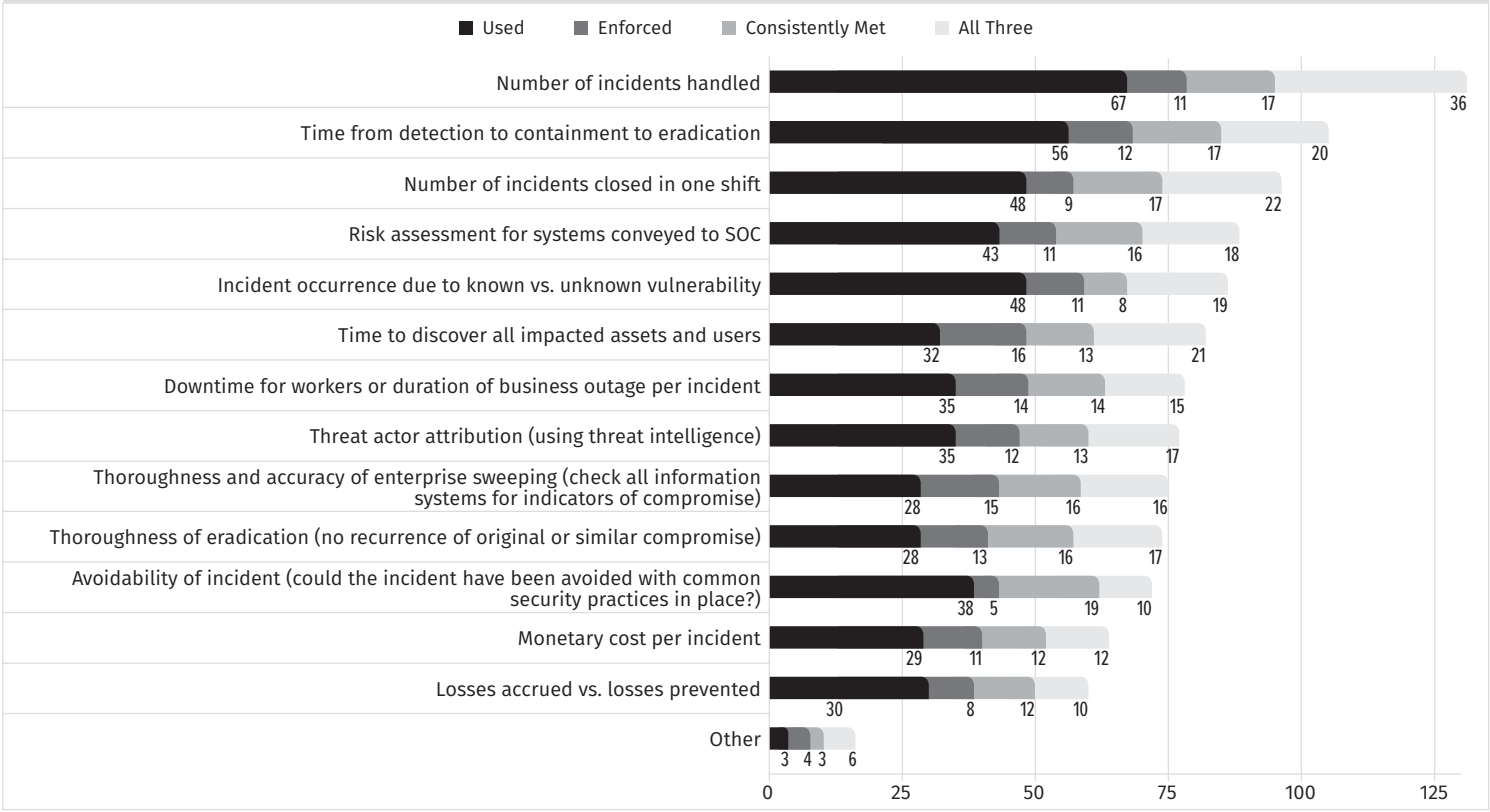


Figure 20. Tracking and Reporting Metrics

The fact that the "losses accrued vs. losses prevented" metric isn't frequently measured isn't surprising. It's hard to calculate—even for business unit managers. The data sources are nebulous and based on estimates or the speculation of events that didn't happen. But, it is useful even in an estimated form.

From the telephone interviews, we found that almost all organizations are increasing their ability to provide accurate time-based metrics. SIEM and log data are useful to identify the volume of events over time spans of months. These tools fall short, however, of being able to provide metrics showing the time to detect, respond and resume normal operations. The common statement was that such time-based metrics were desired, but it wasn't clear where to get accurate data for calculating them.

Also from the interviews, it seems the trend is to move away from "dumb" metrics that encourage bad behavior or cheating the system. Metrics tracking ticket closures per analyst or by the team members of a shift resulted mostly in creation of junk tickets that could easily be closed, or the use of "cut and paste" info into useful ticket fields.

How are metrics tracked and reported? *(N=150)*

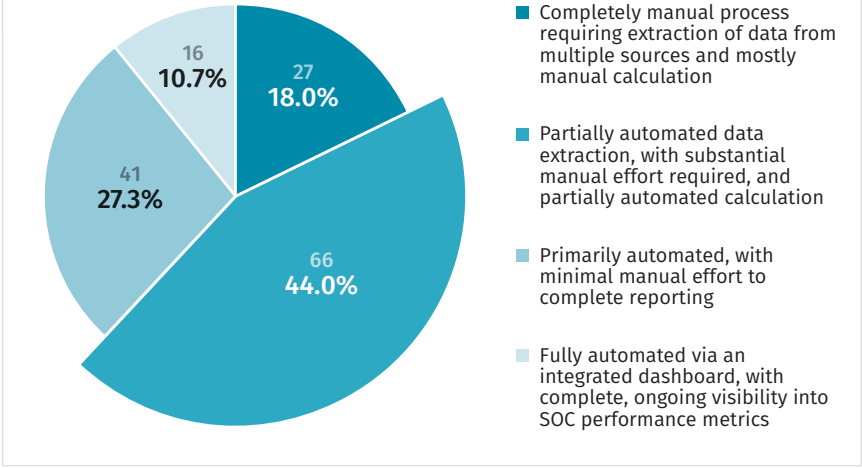


Figure 21. Tracking and Reporting of Metrics

Metrics are supposed to be an objective measurement based on readily available data. Few (16, or 11%) of our respondents have been able to fully automate their metrics, as illustrated in Figure 21.

Larger organizations that have a governance/risk/compliance team or function tended to use more formal methods of establishing business-relevant, meaningful risk metrics to present in SOC reporting. Those without a formal GRC function tended to use ad hoc methods or direct involvement of the CISO for risk tracking.

Action Items

Measure your bad self. You'll learn more about how to improve your SOC performance. Improve your measurement methodology for "incident avoidability" and "losses prevented vs. losses accrued."[5] Work to further automate data collection and metric calculations.

Shortcomings and Problems

We asked what barriers organizations face that are preventing their SOCs from becoming fully integrated within the organization. Then, we looked back to last year's answers to see if these barriers are different, and they're present in nearly the same proportions. Lack of staff who can accomplish the necessary tasks for the SOC is the most commonly cited shortcoming. Tools are blamed for not being integrated, as well as for failing to perform the task of automating work away from analysts. Other commonly cited themes are lack of organizational support in general, as well as the IT portion of the organization specifically. See Table 4 on the next page.

[5] www.youtube.com/watch?v=RwO-uT2jh6E

Table 4. Challenges to Full Integration and Utilization of a Centralized SOC Service Model Year-over-Year

	2019		2018	
Lack of skilled staff	57.7%	157	61.9%	148
Lack of automation and orchestration	49.6%	135	52.7%	126
Too many tools that are not integrated	43.0%	117	47.7%	114
Lack of management support	37.1%	101	37.2%	89
Lack of processes or playbooks	36.8%	100	42.7%	102
Lack of enterprisewide visibility	36.0%	98	41.8%	100
Too many alerts that we can't look into (lack of correlation between alerts)	32.0%	87	33.9%	81
Silo mentality between security, IR and operations	30.2%	82	30.1%	72
Lack of context related to what we are seeing	25.4%	69	18.8%	45
High staffing requirements	25.0%	68	27.2%	65
Regulatory or legal requirements	9.2%	25	12.6%	30
Other	4.8%	13	8.8%	21
Answered		**272**		**239**

From the interviews, the obstacles fall into some major categories:

1. **Unavoidable realities of life.** Lack of skilled staff and management support are the top obstacles whether IT security, IT operations or business managers are queried. Business managers have learned that business-relevant metrics are key to getting management support and approval for resources.
2. **Governance issues**. Silos between organizations, legal/regulatory requirements, etc. can be overcome, but they require interpersonal skills that aren't always present in highly skilled cybersecurity analysts and SOC managers. It requires self-discipline to expand outside of one's own area of expertise to learn about others' objectives, requirements and needs.
3. **Lack of integration and maturity of SOC processes.** These are areas that SOC teams can make the most progress against, and the 2019 survey did show some improvement in these areas.
4. **Technology.** Selection and use of technology are perennial problems.

Technology is often looked at as a way to overcome obstacles, but it is considered a problem itself when it doesn't solve them. During the phone interviews, respondents expressed frustration with the hype around the effectiveness of machine learning in addressing some of these obstacles. "Monitor everything, and big data/machine learning systems will sort it all out" seems to be a great way to sell a lot of product. The solution the interviewees considered productive was to leverage business and threat knowledge to drive use-case development, which in turn identifies what to monitor and how to detect an undesirable state.

While overhyped technologies were seen as the enemy on the outside, the internal enemy was the challenge of gaining visibility into useful endpoints. Production OT systems and IoT devices seemed especially problematic in this arena. There is no simple answer here. The resolution commonly mentioned is to have good working relationships throughout the organization to identify common benefits and collaboration opportunities in use of technology.

Action Items

Compare your sense of what you consider to be barriers with that of your peers. If staffing is your main issue, implement hiring and training recommendations from the "Hiring and Retention Interview Questions Insights" section. Orchestrate and automate your systems to augment the work of analysts and help minimize their shortcomings.

Detailed Demographics

Maybe you skipped to this section from the graphic at the beginning of this paper. Maybe you have arrived at this final section after diligently reading all the details and charts. This section is intended to explain who the respondents are that provided the data we used for the preceding charts.

Industry

Respondents were mostly cybersecurity people, followed by representatives from the government, banking and finance, and technology industries. The next largest response was "Other," which comprised such write-in responses as: oil/gas/mining, construction, consulting, environmental, legal, logistics/infrastructure and real estate. See Figure 22.

There are several opportunities to cross-walk the sector to any given question. One interesting sector-based cross-reference was for the requirement to purchase services from the SOCs self-identifying as "service providers." Education is most willing to allow the choice of an internal or outsourced SOC when an internal SOC is available, with the utilities and government sectors being the next most likely to allow external SOCs. Our results here are limited by small sample-size issues, which are apparent in Figure 23.

Organization Size

The organizations that responded have a broad distribution in size. The range of responses across the categories was no less than 5% of responses and no more than 20% of responses. We can take this to mean that the responses are generalized across organization sizes. See Table 5.

Table 5.
Total Workforce Size, Including Employees and Contractors

Organization Size	Responses
Fewer than 100	70
101–1,000	102
1,001–2,000	40
2,001–5,000	54
5,001–10,000	56
10,001–15,000	27
15,001–50,000	64
50,001–100,000	37
More than 100,000	67

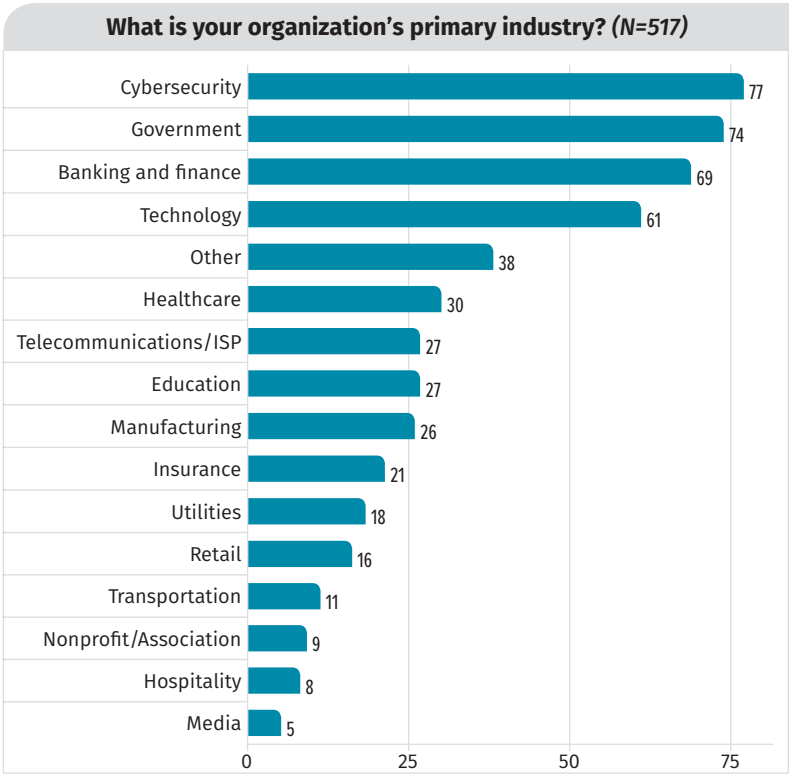


Figure 22. Organizations by Industry

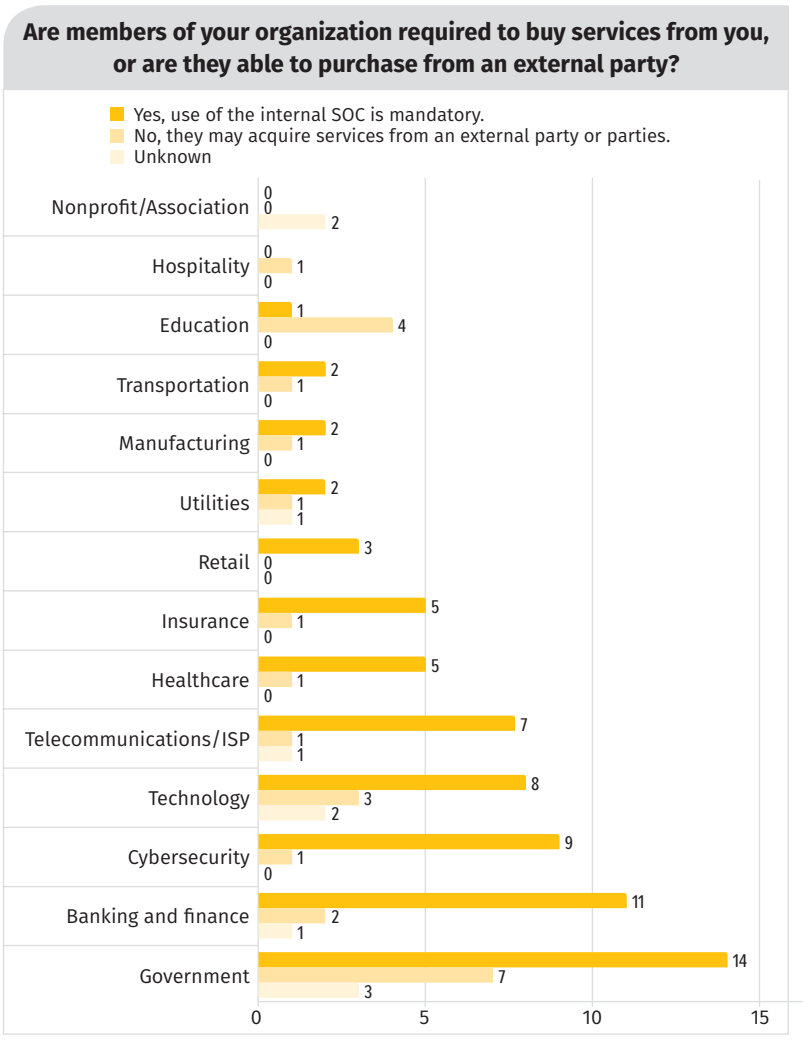


Figure 23. Internal vs. External Services

Individual Respondent's Role

The individuals responding are overwhelmingly skewed to the "security administrator/security analyst" role. Almost a third of responses (28%) are self-identified in that role. The good news is that the respondents are in the thick of the details of the SOC. Technical roles totaled 290 responses, whereas management, director and executive roles totaled 192, excluding the "other" responses.

Of the 39 "other" responses, three were nontechnical titles: "director ...," "... team leader," "... project manager." The rest were a variation on analyst, consultant, engineer, technician and specialist. This brings the grand total to 326 technical roles and 195 management roles. See Figure 24.

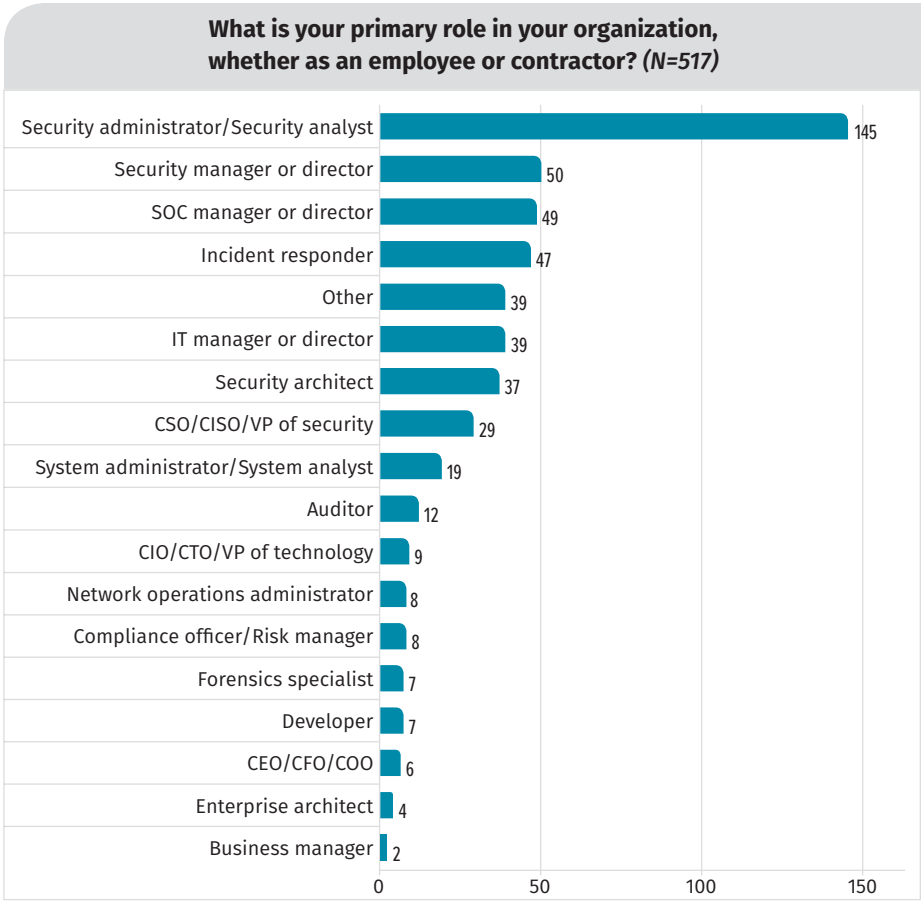


Figure 24. Organizational Roles

Geography

Laws and industry requirements are primary drivers for security implementation. Tradition, organizational culture, and employee cultural backgrounds are strong contributors to the strengths and weaknesses of the SOC. Hence, the answers we received are driven by these background pressures and flavored by these cultural inclinations. Our respondents are overwhelmingly headquartered in North America: 61.0% (United States: 57%, Canada 4%) and Europe: 17%, as seen in Figure 25.

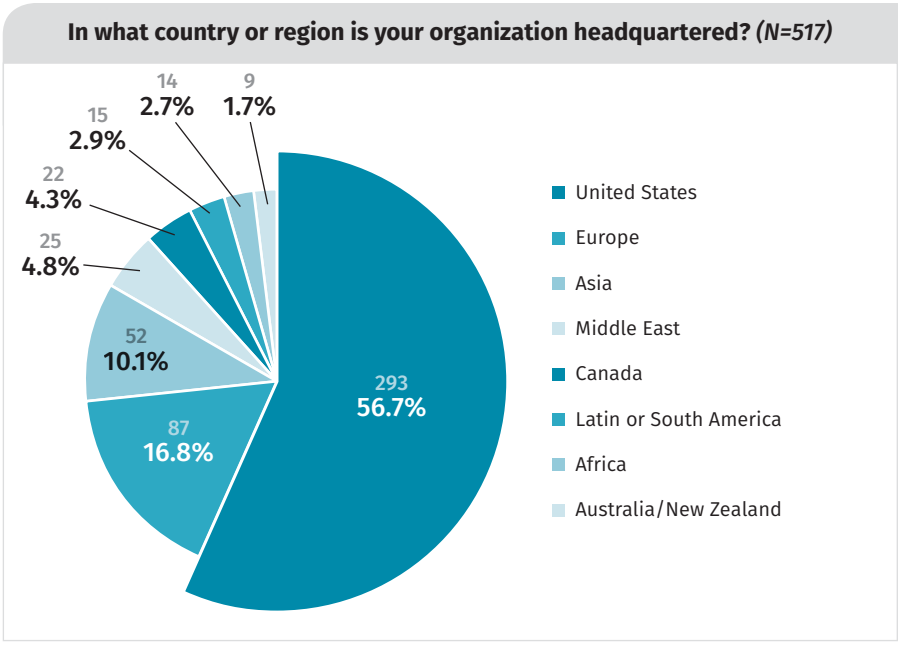


Figure 25. Organizations by Country/Region

Their systems are global, but follow the focus of headquarters in North America and Europe. Figure 26 illustrates the regions in which organizations have systems in operation.

One inference from these two charts is that North American and European countries are likely to also operate IT systems in Australia/New Zealand. Our speculation is that this is common due to cultural and linguistic compatibility for business ventures.

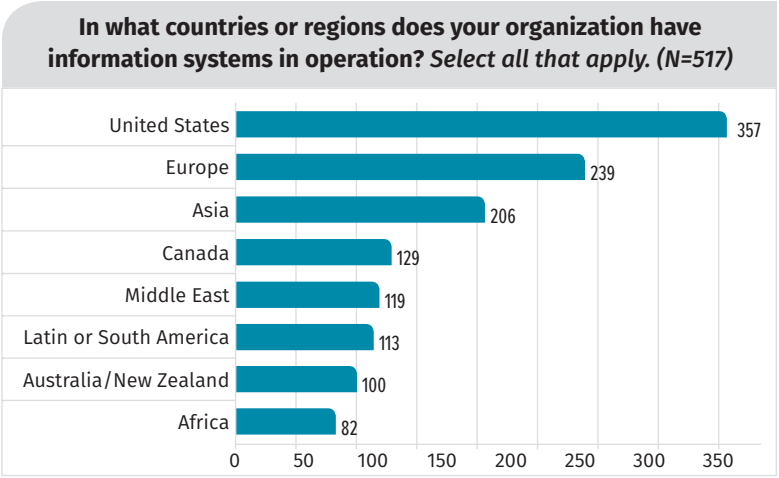


Figure 26. Information Systems by Country/Region

MSSP or not MSSP?

We wanted to know whether the respondent's organization is an MSSP for two primary reasons. First, when a respondent has an organizational size of 1,001–2,000 with 1,000 SOC analyst positions (an actual response in this survey), it is insightful to validate that this is in fact an MSSP. Second, it tracks the inclination of the SOC to consider itself a service offering, as opposed to an immutable part of the IT service portfolio. See Figure 27.

Figure 27. MSSP Self-Identification

Summary

Going strictly by the numbers, not much changed for SOC managers from 2018 to 2019. However, just staying in place against these powerful currents is impressive, considering the rapid movement of critical business applications to cloud-based services, growing business use of "smart" technologies driving higher levels of heterogeneous technology, and the overall difficulties across the technology world in attracting employees.

Lack of skilled staff, budget and effective automation are the most commonly cited reasons for failing to achieve excellence in existing SOCs. To gain management support for resources, SOC managers need to move beyond quantity-based metrics (how many raindrops hit the roof) to business-relevant metrics (zero production downtime due to rain getting through the roof).

The hype around automation technologies is still ahead of actual performance, but it took a while for the computers to beat chess masters, too. SOC operations are among the most challenging environments, as threat behavior, business processes and IT technologies change constantly (if the pieces on the chessboard could move in arbitrary ways while the number of squares on the board went up and down randomly, humans might still be winning). Machine learning tools are proving effective in augmenting skilled analysts or enabling lesser-skilled analysts to focus on the most likely true positives first.

We identified many action items for you throughout this report. At the top of the list is clearly articulating what services are offered by the SOC to the business. Identify business-relevant metrics to show how an investment in SOC capabilities or enhancement will benefit the bottom line. Then, work with the business to build use cases and gain access to the data you need to monitor around those use cases.

Your SOC needs good people. Retain staff by keeping people interested, or establish the SOC in an isolated location so they have no alternative. External service providers (MSSPs) bolster SOC capability frequently with good results by organizations, and it is not uncommon to outsource and retain some staff to do that functionality internally.

About the Authors

Christopher Crowley, a senior SANS instructor and course author for SANS courses in Managing Security Operations and Incident Response Team Management, holds multiple certifications. He received the SANS 2009 Local Mentor of the Year award for excellence in providing mentor classes to his local community. Chris is a consultant based in Washington, D.C., who has more than 20 years of experience in managing and securing networks. His areas of expertise include network and mobile penetration testing, mobile device deployments, security operations, incident response and forensic analysis.

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this survey's sponsor:

ExtraHop