SANS

Analyst Program

Survey

SANS 2022 SOC Survey

Written by **Chris Crowley** and **Barbara Filkins**

May 2022

Chronicle

Executive Summary

The content of this year's SANS SOC Survey explores the ongoing development and progress of the security operations center (SOC). Herein we explore details of who answered the survey, the key takeaways we observe in their responses, and the challenges everyone seems to face. The survey explores what people consider SOC capabilities, as well as the staff, technology, deployment strategies, and the funding it takes to secure and operate this gamut.

So how are SOCs evolving? To date, our definition of a SOC remains conceptual, built around the capabilities required by business-specific goals of an organization. A SOC framework is not necessarily aligned with a reference architecture but comes from the technologies in use and the individuals who make up the SOC team to accomplish capabilities.

In planning this survey, we took a capabilities-based approach to determine the current SOC landscape, with the goal of surfacing results that can help you assess your performance compared with your peers. In that regard, here are the top five questions you might want to consider and our insights from this year's survey:

What Makes a SOC?

We consider that a SOC is defined by its capabilities and how these capabilities are prioritized by the organization owning the SOC. Capabilities are process-based, the related service driven by the business needs or mission statement of the organization.

We consider a SOC architecture as how organizations decide to arrange their staff and technology to gain visibility into protected systems, perform the required work, and take into account the complicated logistical and jurisdictional issues to address when monitoring information systems.

1. Are trends going in the right direction?

   Results from 2021 to 2022 show a decrease in both incidents and breaches from incidents. This is a positive trend, but the question is, can it continue?

2. Does staffing match growth?

   Hiring, retention, and turnover are key challenges. Consider comparing how your organization lines up against the survey results.

3. Do capabilities match business need?

   The leading items for survey respondents are detection/monitoring, vulnerability assessments, incident response, and alert triage and escalation with capabilities balanced between internal staffing and outsourced resources. How do the capabilities your organization defined rank against these results?

4. Is the technology working?

   What technologies received a grade of an A and why? Compare how your organization lines up against the survey results
   in the section "Staffing: Meeting the Key Challenges."

5. Are metrics measuring investment and what's effective?

6. Are the discrepancies noted by this report being taken into account as we move forward?

Survey Globalization

Something new this year, which the authors are extremely proud of, is that the survey questions and answers were translated into Spanish and Portuguese. The intention is that respondents who speak English as a second language or non-English speakers can provide responses and share thoughts succinctly and naturally. The intention is to scale this translation into more languages going forward. Optimistically, we'll cover Europe, the Middle East, and Asia with regionally specific languages to develop the SOC Survey into a truly global perspective on cybersecurity operations.

We all have our shortcomings, and this survey is no different. We'd love to hear from our readers on how to make it better if we didn't answer your question in the following content. If we didn't answer your questions (or you are skeptical of our findings) and you want to perform your own analysis of the data set in this survey, download it from https://soc-survey.com/2022.

SOC Landscape

When most of us think of a SOC, we probably envision some type of command center, housing InfoSec professionals who will detect, protect, and defend an enterprise from cyberattacks. Indeed, most respondents, at 47% *(n=519)* indicated that their SOC services are obligatory for their organization (see Figure 1), with the majority of 53% *(n=240)* citing their SOC size and structure as single and centralized, followed distantly by multiple, hierarchical SOCs at 19% *(n=85)*. See Figure 2.

But looking ahead 12 months, while survey results show the single, centralized SOC *(n=138)* as the leading deployment model, the real growth is occurring in cloud-based SOC services.[1] This opens the door to what we envision as the true definition of SOC, one based on capabilities rather than a formal structure. See Figure 3, noting that the second line ("Informal SOC, no defined architecture") doesn't seem to be an aspirational future state, because it represents low maturity.

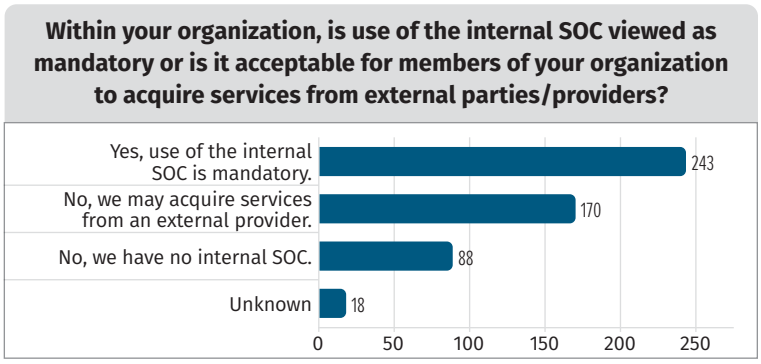

Figure 1. SOC Services Optional or Obligatory (Q3.2: n=519)

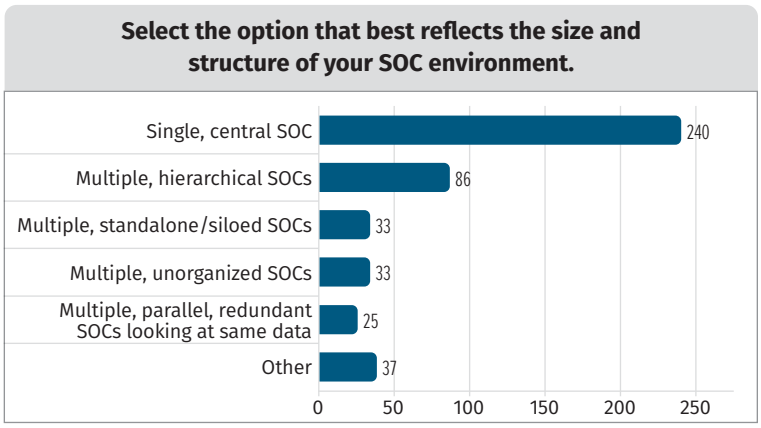

Figure 2. Structure of SOC (Q3.5: n=454)

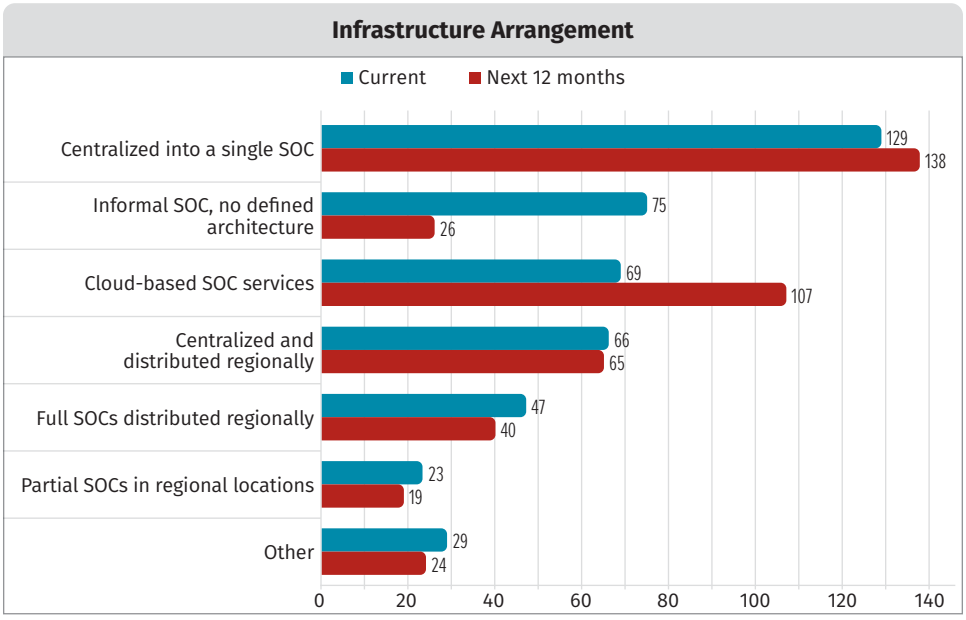

Figure 3. Infrastructure Arrangement Sorted by Current Deployment (Q3.6: n=454)

[1] If expressed as a growth percentage (future/current counts divided by current count), the growth in the cloud-based SOC services sector is 55%, whereas the growth in the central SOC is 7%. All other arrangements indicate a decline in the next 12 months.

Meeting the Key Challenges

Given that SOC capabilities mirror key security functions, such as incident response, we looked at the survey responses to see if the challenges to fully utilizing SOC capabilities would follow those barriers faced by most security professionals.

Not surprisingly, high staffing requirements is the biggest stumbling block *(46 of 235 respondents)*, followed by a lack of skilled staff *(34)*. A lack of automation and orchestration *(32/235)* followed. The fourth largest challenge—a lack of management support *(23)*—brings the top four barriers to account for 57% *(135/235)* of all responses. See Figure 4.

We wanted to hear the respondents' challenges in their own words, so we gave a free format opportunity to write it down. The word cloud in Figure 5 captures a frequency-weighted depiction of the words used in the responses. Human resources issues, money, and management support are repeated almost universally.

What is the greatest challenge (barrier) with regard to full utilization of your SOC capabilities by the entire organization? ***Select the best option.***

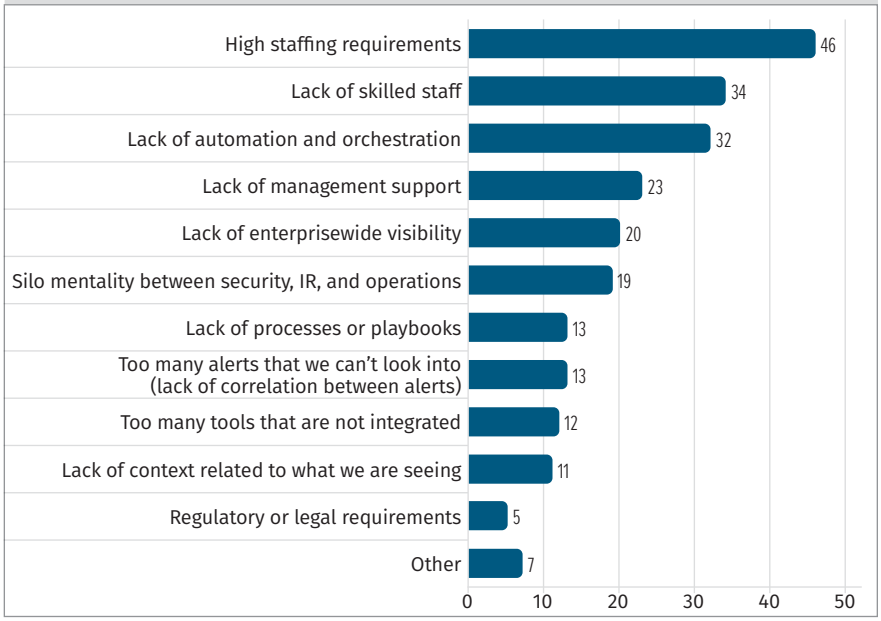

Figure 4. Challenges to Using SOC Capabilities (Q3.61: n=235)

Figure 5. Barriers to SOC Use (Q3.59: n=130)

Demographics

Survey respondents provided insight from their personal experiences with results heavily influenced by individuals whom SANS asked to participate in the survey through outreach and marketing efforts. To conduct a survey at this level of detail, we depend on respondents to volunteer 30 to 60 minutes of their time to answer thought-provoking and detailed questions. It is the opinion of the authors that we still don't have a globally representative sample of cybersecurity operations centers, but we're striving to get there. Figure 6 provides a snapshot of the demographics for the respondents to the 2022 survey.

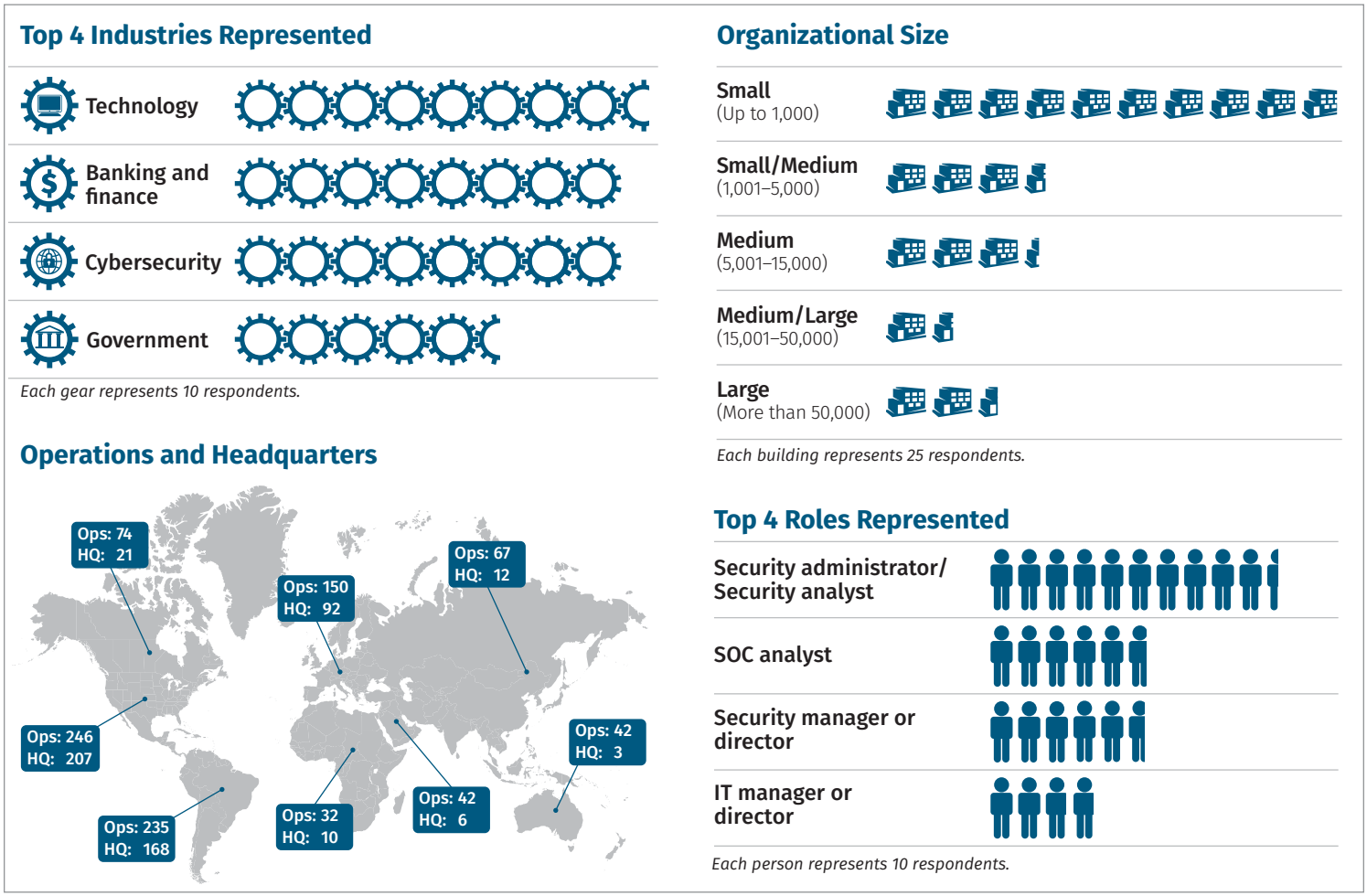

Figure 6. SOC Survey Respondent Demographics

Demographic Highlights

- The majority of respondents are from smaller organizations. Of the 519 participants who answered, half (50%) are from organizations with fewer than 1,000 people. This tendency toward smaller organizations may be due to fact that the high-tech and cybersecurity companies function in a technology support role and, traditionally, have smaller staff.
- Respondents are primarily in high tech, financial, cybersecurity, or government. If you're in one of these sectors and don't have a SOC, your peers likely do.

- Of the 519 respondents, 270 (52%) have analyst, administrator, or architect roles, while 214 (41%) serve as managers, directors, or c-level executives. The remaining 35 (7%) listed their roles as other. The other roles included specific forms of analyst, engineer, specialist, and manager not specifically cited in the list of choices but still cyber-focused. There were several educator, consultant, repair, sales, and other write-in titles which had no corresponding choice in the list.
- The respondents' companies are primarily based in North America, Latin America, and Europe. Previous years' SOC surveys speculated the prevalence of North American and European organizations as a feature of who participated, rather than a feature of the actual prevalence of SOCs globally. This year's report and survey targeted Latin America, and this region took the second among headquarters for the first time. Our mission for this survey going forward is to continue similar outreach globally.

Factors for SOC Success

Survey readers tell us that they frequently seek budget, technology, and staff based on the results and insights described in our SOC surveys. The authors take this seriously. We're providing the guidance in this section around some key questions you should ask yourself and your organization to help you make difficult choices. And we have included a few key findings from this survey to help you guide your decisions and requests.

Success Factor One: Are Trends Going in the Right Direction?

This year's survey, more respondents as a percentage *(48%)* answered "No," indicating their organization had not suffered an intrusion in the past 12 months. This statistic is better than last year's SOC survey, where 39%[2] answered "No." In the way the question is phrased, more people responding "No" indicates fewer incidents occurring. Of course, there were numerous responses that expressed ignorance *(71, 14%)* or unwillingness *(47, 9%)* to acknowledge if a breach happened. See Figure 7.

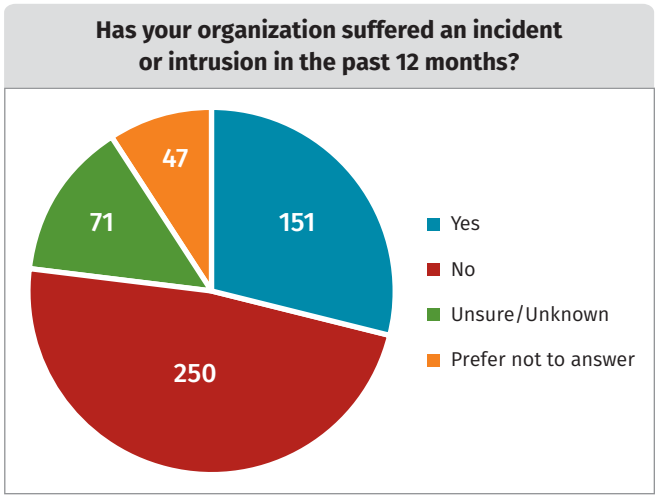

Figure 7. Intrusions/Incidents in the Past 12 Months (Q3.3: n=519)

Of the respondents who had an intrusion, we followed up with the next logical question: Did this result in a breach? Of the 128 people who answered Question 3.4, 68 responses *(53%)* indicated that the intrusion didn't result in a breach (see Figure 8). In comparison to the 2021 SOC Survey, 95 responses were collected to the "result in a breach" question, and 47% of those said

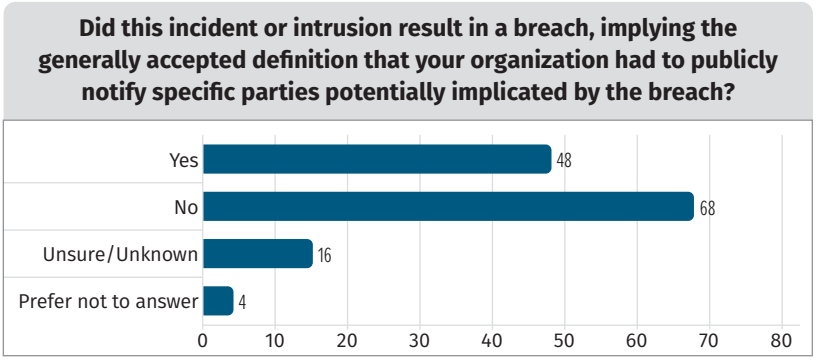

Figure 8. Breaches in the Past 12 Months (Q3.4: n=136)

[2] "A SANS 2021 Survey: Security Operations, Center," October 2021, www.sans.org/white-papers/sans-2021-survey-security-operations-center-soc/?socsurvey=1, p. 2. [Registration required.]

"No." In other words, in 2022 more people answered that the intrusion did not result in a breach, which is an improvement. Bravo for finding and stopping it! We started asking this question in 2021, and so far, the trend seems to be going in the right direction.

We didn't have a follow-on question related to what enabled the detection and removal of the intrusion prior to the breach. There are a multitude of other reports and surveys documenting the details of breach and loss from the cybersecurity community. But we will continue to assess if this trend of success we are seeing in reduced incidents and subsequent breaches can be attributed to the presence of a SOC.

ACTION: Track metrics to ensure your trends are moving in the right direction.

Success Factor Two: Does Staffing Match Growth?

This year staffing levels remained fairly consistent with the past. The most popular SOC size is 2–10 people, with 66 of 234 respondents selecting that answer.[3] See Figure 9.

Despite a constant team size year after year in the survey, staff turnover and retention are leading concerns. Staff turnover remains high: 70% for individuals with five or fewer years of experience, with the majority remaining in their current position for fewer than three.

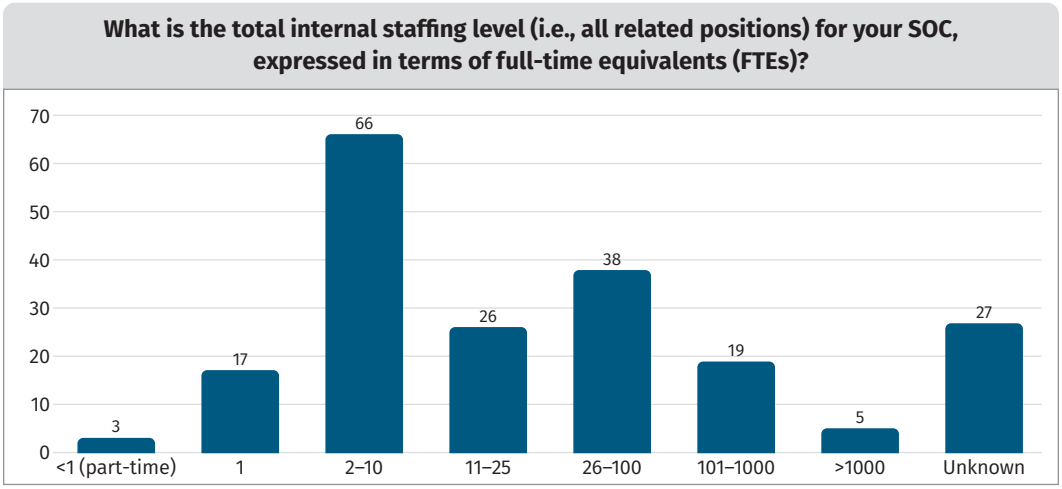

Figure 9. SOC Size by Number of FTEs (Q3.46: n=234)

Retaining talent is also critical, requiring a critical and continual pitch by the SOC to organizational management. This pitch needs to be supported by metrics that demonstrate value and clear planning to articulate expected improvements. Organization management considers the business operational environment and weighs the cyber threats against the business impacts.

ACTION: Compare how your organization lines up against the survey results in the section "Staffing: Meeting the Key Challenges."

Success Factor Three: Do the Capabilities Fit the Business Need?

We will go into detail on capabilities in a later section, but if your team isn't performing against one or more of these capabilities listed in Figure 16 (see page 11), your team probably won't be considered a SOC.

The leading items for survey respondents are detection/monitoring, vulnerability assessments, incident response, and alert triage and escalation, with capabilities balanced between internal staffing and outsourced resources.

ACTION: Rank the capabilities your organization defined against these results.

[3] Please note that this is not organizational size or sector adjusted.

Success Factor Four: Is Technology Working?

Technology elicits strong opinions from most cybersecurity professionals. This year, we assigned our technologies a GPA based on the grades individual respondents assigned to each technology. The more successful technologies are focused on the mature and stable as opposed to the new and exciting, but even the leading technologies only got a B– overall.

ACTION: Explore the section "Technology: What Is Getting a Passing Grade?" to see how to assess your technologies as well as the part on tying the capabilities together.

Success Factor Five: Are Your Metrics Really Measuring the Effectiveness of Your Investment?

With an increased emphasis on staffing as a leading challenge/barrier to SOC effectiveness, organizations must consider how executive management not only listens but also acts on what their SOC leadership is telling them. Although 39% reported that executive management and SOC leads work closely together in allocating funds for cybersecurity, 55% believe the decision is wholly that of executive management, despite any recommendations from the SOC team. And although 41% report that management pays close attention to the recommendations and needs of SOC leads with regard to hiring and retaining skilled, experienced staff for defending the enterprise, 55% again think that, while executive management may again listen, they do not act on the urgency to retain, not just hire, skilled staff.

ACTION: Calculate a metric that measures the effectiveness of the SOC.

Staffing: Meeting the Key Challenges

Let's first talk about people. There is no change in overall SOC team size from previous years. Again, 2–10 staff members is the most commonly cited team size, regardless of the size of the organization. See Figure 10.

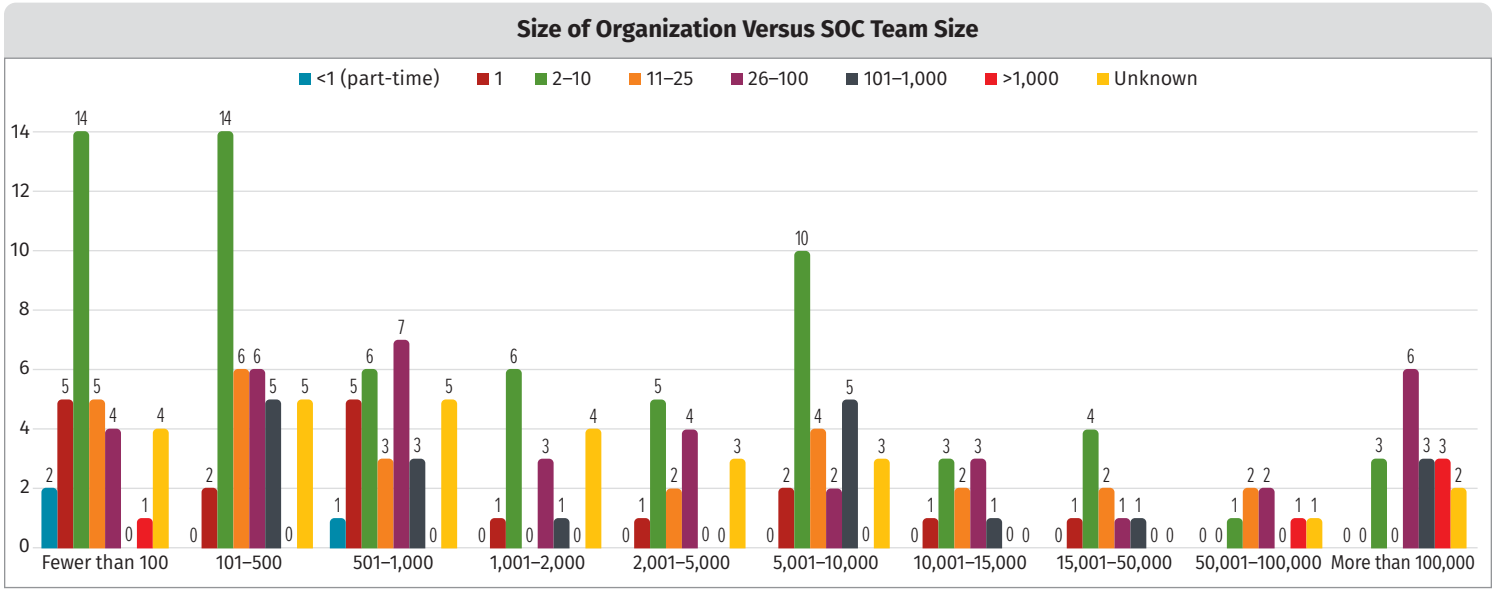

Figure 10. Size of Organization Versus SOC Team Size

The top two barriers to full SOC utilization are staffing-related (see Figure 5). What are respondents saying about the challenges they face? Frequent turnover appears to be the first obstacle. In Figure 11, we see that the average duration of employment is predominantly less than five years, with the most cited *(n=84)* remaining one to three years before leaving.

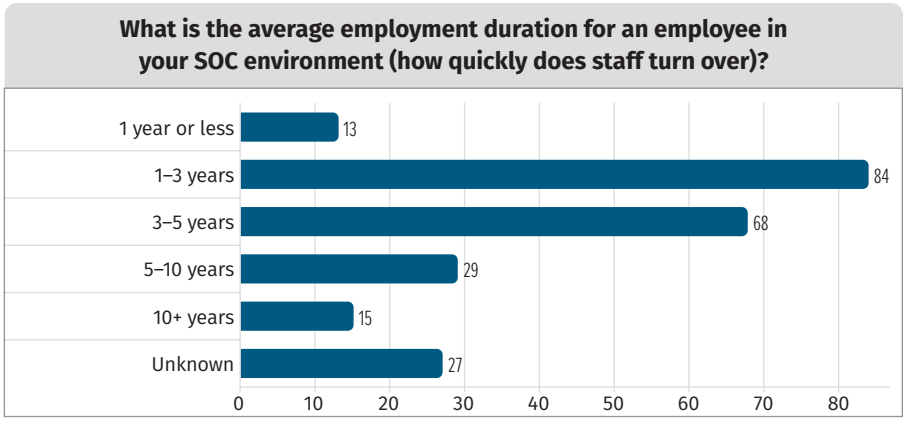

Figure 11. Average Employment Duration (Q3.48: n=236)

So, what are most effective methods of retaining staff? The leading approach is to provide staff clear career progression *(n=76)*, as shown in Figure 12. The authors see this as providing two benefits:

- Employees stay with the organization longer, reducing the cost of hiring and training new staff.
- People who want to grow and develop within an organization tend to be more productive and effective employees.

Employees who have a mind to grow and develop are likely caring workers. If you don't facilitate that growth, they'll find it in a different company that has a plan in place for career growth.

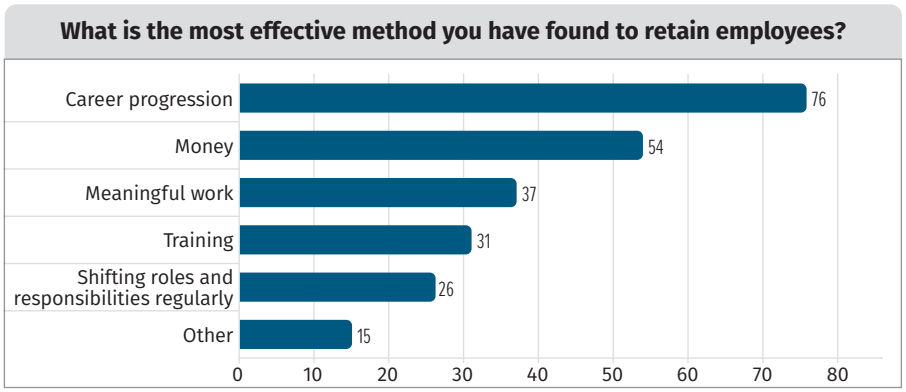

Figure 12 Retention Methods (Q3.49: n=239)

Retention seems to be an important part of managing the SOC team, implying likely negotiation between SOC and organizational management to address key factors to keep staff: career plan assurance with additional training, monetary incentives, work-life balance, and relaying the value of the work performed.

The short story of our guidance here is calculate the costs involved in hiring new staff. Show the value proposition by comparing the hiring cost to the cost of training and developing existing staff.

So, what did the respondents say about their management's investment in staff? Many respondents *(n=96)* indicated that organizational management coordinates with SOC management and team leads to hire and retain the right people to defend the environment. But, while this indicates that the situation many be improving from past surveys, the balance *(n=129)* still feels that executive management may listen, but they do not act on the urgency to retain, not just hire, skilled staff. See Figure 13.

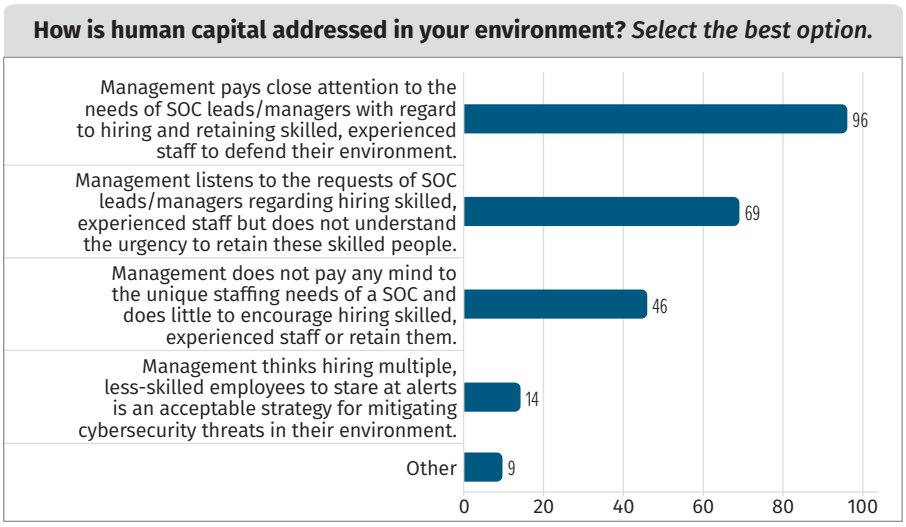

Figure 13. Human Capital Management Approach (Q3.53)

Working Remotely

The pandemic forced a new reality on the workplace. Working remotely is now the norm. And that includes the SOC team. You probably already allow your SOC staff to work remotely. If you don't, you're competing for that staff with companies that do. See Figure 14.

Organizations now need to balance the ease of hiring and retaining staff who expect to work remotely versus the increased difficulty in training, developing, and onboarding staff working from home.

So, what factors do organizations take into consideration for a SOC staff analyst to work remotely from home? The leading consideration *(n=165)* is if the platform supports it. (See Figure 15.) We take this to mean that the data sensitivity is weighed against the risk of accessing the data from off-premises, and a risk-weighted decision is made about the work from home. This seems a reasonable consideration that can be made in coordination with risk management around the sensitivity of the systems protected.

The next few considerations, however, are more of a SOC management judgment call based on the individual's performance and perceived skill set *(n=139)*. But the growth in remote work/work from home due to the pandemic appears to have changed how organizations determine whether an individual can work remotely. In 2022, work ethics rose to the third most important evaluation factor *(n=115)*: 43% in 2022 versus 33% in 2021. (Note: While an individual's work ethic seems a reasonable basis for consideration for remote work, it might be hard to quantify fairly. Ostensibly, the rationale here is that those with a lesser work ethic are motivated to be more effective by the oversight provided on-premises.)

Do you allow SOC staff analysts to work remotely?

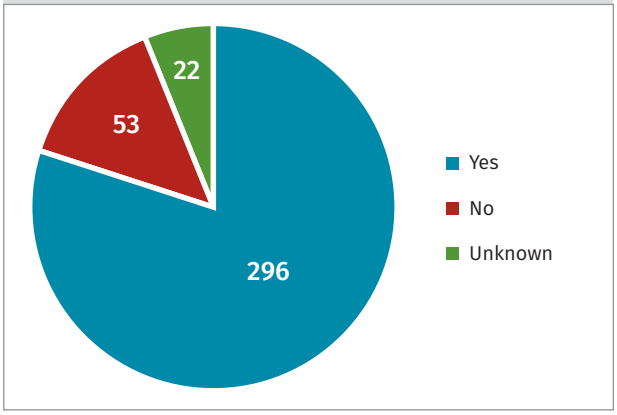

Figure 14. Remote Work (Q3.13: n=371)

The authors concur that few organizations can justify an on-premises-only SOC based on data sensitivity. While some organizations must maintain this security posture for specific reasons, in general this position is becoming more difficult to justify.

What factors are considered in determining whether a SOC staff analyst can work remotely? *Check all that apply.*

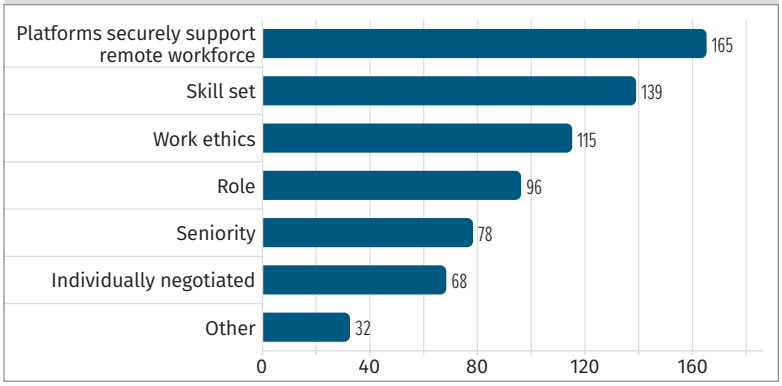

Figure 15. Factors in Work From Home (Q3.14: n=266)

Capabilities: Does Your Team Count as a SOC?

Do you ever wonder if your team counts as a SOC? You're not alone. We asked respondents to identify the capabilities they have within their SOC. Figure 16 shows a count-based, ranked list of what the most respondents said they do. The leading items are detection/monitoring *(376)*, vulnerability assessments *(373)*, incident response *(373)*, and alert triage and escalation *(373)*.

We define a SOC through capabilities and architecture. So, if you're not performing the capabilities listed in Figure 16 either internally and/or by outsourcing, that particular group wouldn't be considered a SOC.

Much of what SOCs do can be outsourced, so we wanted to understand what SOCs choose to outsource. There is basically no change in the outsource portfolio from previous years' SOC surveys. See Figure 17, where the data from Figure 16 is re-sorted by how many respondents outsource that capability.

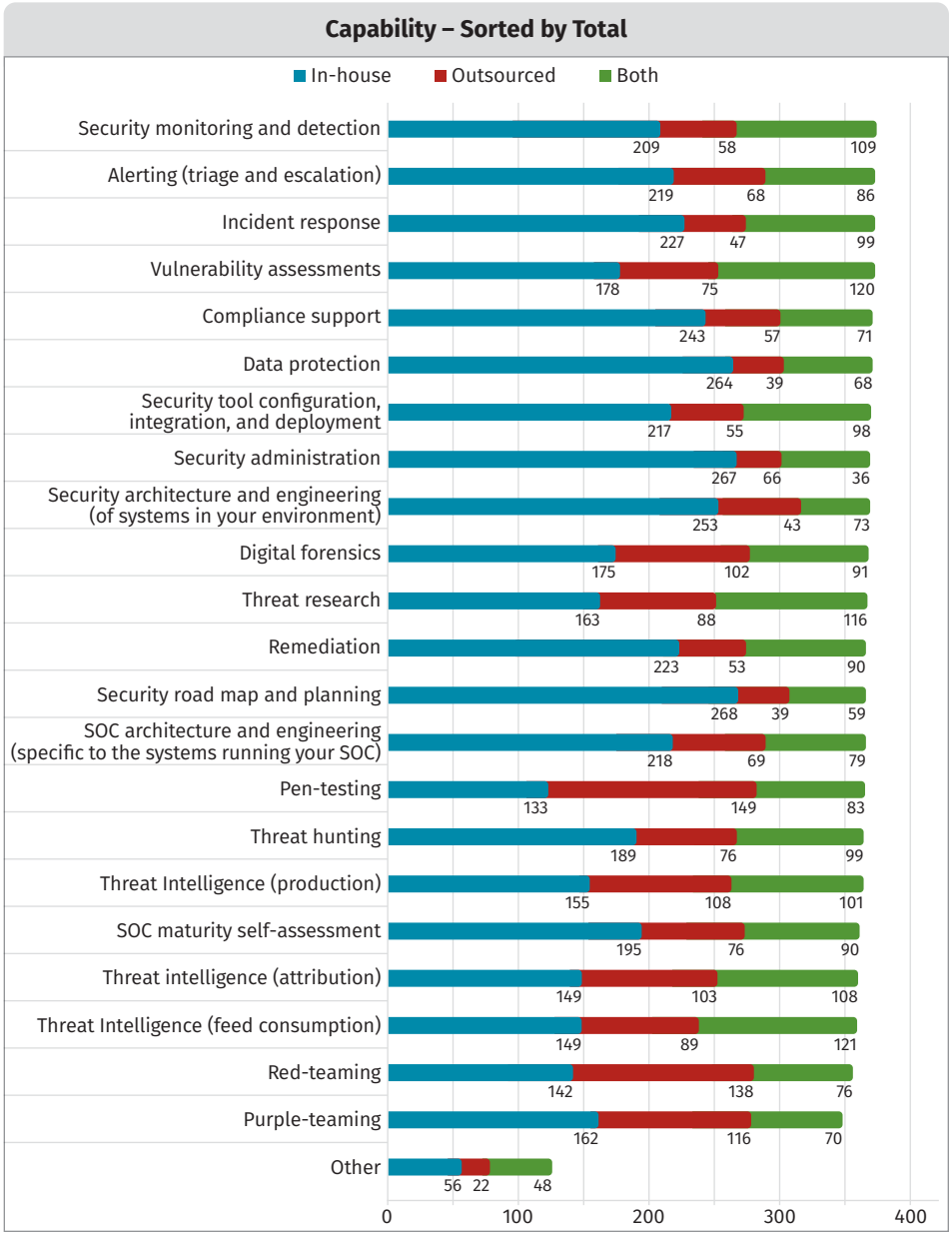

Figure 16. Capabilities Ranked on Total Reporting (Q3.10: n=383)

What's interesting to the author (Crowley) is how much consensus exists in this response set. If "Other" is excluded *(112)*, then the range is 348–376 from 383 respondents. There were only 20 other text responses, and 14 of these were none or N/A. A couple were comments about the question. There were three relevant other responses: business review, research, and NIST framework management. The research we'd put with "threat research" and the NIST framework we would expect to group with "compliance support."

While you might have good reasons to retain pen testing and its variants, threat intelligence, and forensics internally, many of your peers continue to outsource these capabilities, probably for two basic reasons. Retaining this expertise on staff can be cost-prohibitive, because talented specialized staff are rare. An added complexity is the requirement for training specialized staff, because keeping up to date with constantly changing technology and techniques, such as in pen testing (and related) and threat intelligence, can be difficult. Finally, budgeting for a full-time individual specialist in a small team usually doesn't make financial sense, as general-purpose analysts are usually internal staff. So, focused expertise is procured in an outsourced fashion. In larger teams, calculating the value proposition of outsourcing usually directs the outsource action.

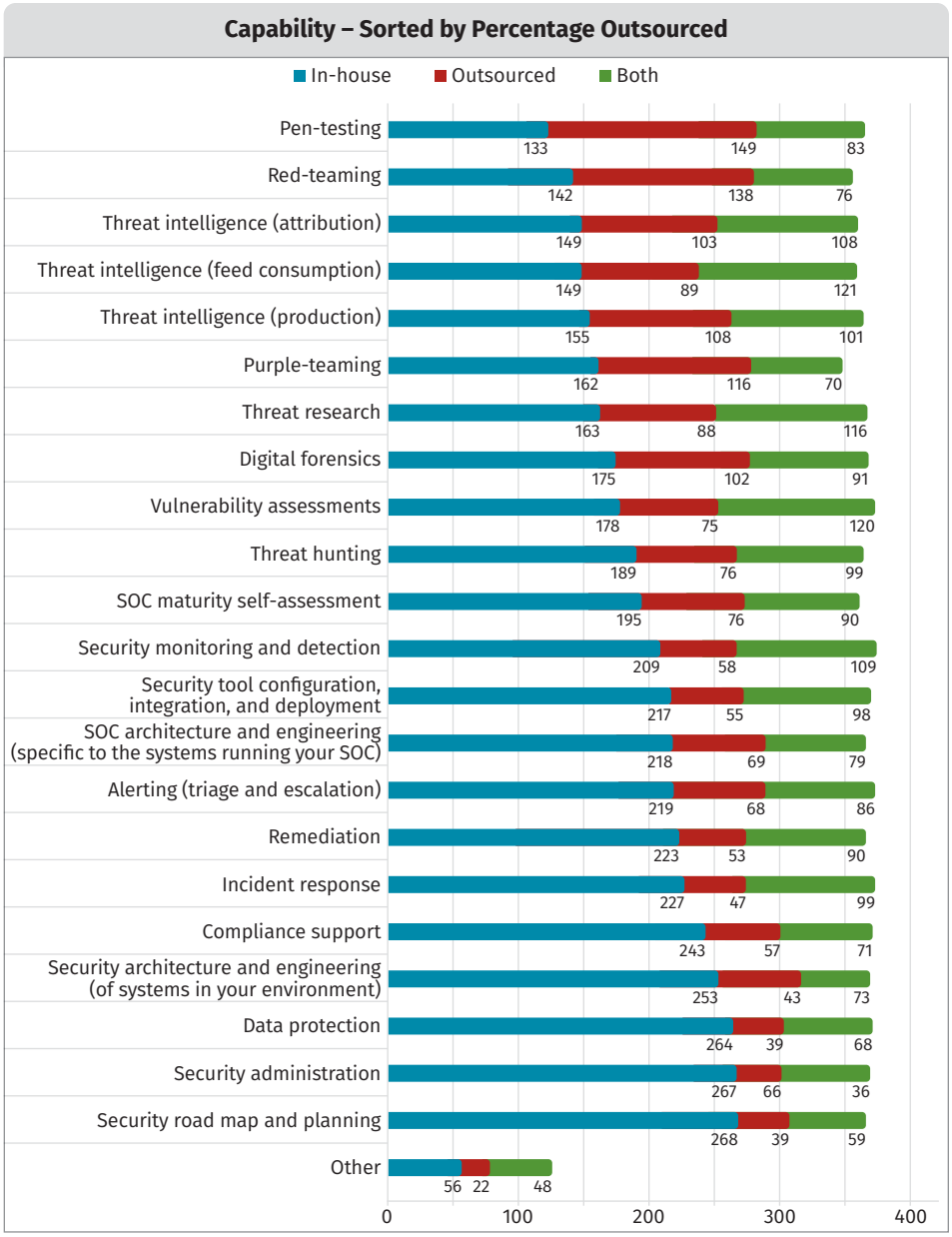

Figure 17. Capability Ranked Greatest to Lowest for Outsourcing (Q3.10: n=383)

So, what compels retention of staff internally? The rationale for capabilities which tend to be performed internally are those which require tailoring to the organization. The institutional knowledge to perform the tailoring is necessary for this work as the work tends to stay internal (also, the perceived need of of data control and privacy for these capabilities and the data handled therein). Defensible or not, this is the stance that many organizations use to keep the activity internal rather than outsourced.

Technology: What Is Getting a Passing Grade?

From a technology perspective, we discussed technology deployed and how far along it is in the deployment. Of course, we also asked what technologies people like and don't like. The two questions we asked to discover this information included long lists of choices and took at least 10 minutes to answer, so we allowed people to skip them, but 53% *(Q3.26, n=308)* agreed to answer them.

A perennial problem for IT environments is the "partial deployment" of systems. In the authors' experience, many SOCs' maturity, efficiency, and improvement efforts are pending completion of some technology deployment. Figure 18 indicates where the respondents' organizations are in their deployment efforts.

Category: Question	Production (All Systems)	Production (Partial Systems)	Implementing	Purchased Not Implemented	Planned
Host: Vulnerability remediation	58	42	24	5	14
Host: Malware protection system (MPS)	60	43	22	6	12
Host: Behavioral analysis and detection	51	29	27	9	24
Host: Data loss prevention	42	35	27	13	26
Host: Ransomware prevention	56	27	26	11	19
Host: User behavior and entity monitoring	39	34	23	10	30
Host: Endpoint or extended detection and response (EDR/XDR)	59	28	26	5	19
Host: Application whitelisting	46	34	23	11	24
Host: Continuous monitoring and assessment	61	37	18	11	16
Log: Endpoint OS monitoring and logging	57	38	18	12	17
Log: Endpoint application log monitoring	54	33	27	10	15
Log: Log management	56	40	23	10	13
Log: DNS log monitoring	47	43	25	6	20
Net :Network segmentation	64	41	15	10	9
Net: Email security (SWG and SEG)	72	33	15	8	12
Net: DNS security/DNS firewall	70	33	21	4	13
Net: Asset discovery and inventory	47	39	26	12	17
Net: VPN (access protection and control)	79	30	17	9	7
Net: Full packet capture	32	35	26	9	32
Net: Packet analysis (other than full PCAP)	41	33	23	10	26
Net: DoS and DDoS protection	51	48	15	13	15
Net: Network traffic monitoring	52	42	21	11	15
Net: Web application firewall (WAF)	53	52	16	11	10
Net: Next-generation firewall (NGF)	73	30	15	11	13
Net: Egress filtering	53	42	22	5	18
Net: Deception technologies such as honey potting	33	29	22	11	39
Net: Web proxy	58	36	19	6	16
Net: Network access control (NAC)	46	31	23	14	25
Net: NetFlow analysis	32	33	23	16	30
Net: Malware detonation device (inline malware destruction)	33	31	23	11	36
Net: Network intrusion detection system (IDS)/intrusion prevention system (IPS)	67	41	19	7	7
Net: SSL/TLS traffic inspection	40	39	23	6	24
Net: Ingress filtering	56	39	18	10	15
Analysis: Risk analysis and assessment	53	38	27	9	11
Analysis: SIEM (security information and event manager)	63	34	25	6	12
Analysis: Customized or tailored SIEM use-case monitoring	53	32	22	13	19
Analysis: AI or machine learning	36	26	20	6	42
Analysis: Frequency analysis for network connections	38	33	25	7	27
Analysis: External threat intelligence (for online precursors)	44	32	23	12	22
Analysis: Threat hunting	38	36	28	9	23
Analysis: Threat intelligence platform (TIP)	40	28	27	8	33
Analysis: Threat intelligence (open source, vendor provided)	42	29	29	14	22
Analysis: E-discovery (support legal requests for specific information collection)	36	29	22	5	40
Analysis: SOAR (security orchestration, automation, and response)	39	30	19	9	37
Other	13	10	11	5	12

Figure 18. Technology in Use and Deployment Status (Q3.26: n=150)

This view is useful, but it might also be beneficial to consider this in terms of accomplishing "all systems" deployment. To this end, Figure 19 shows a sorted view of the data shown in Figure 18. It loses the categorical grouping as a result. But this figure might be used as a guide on the likelihood of getting your intended technology fully deployed.

Category: Question	Percentage (All Systems)	Production (All Systems)	Production (Partial Systems)	Implementing	Purchased Not Implemented	Planned
Net: VPN (access protection and control)	55.6%	79	30	17	9	7
Net: Next-generation firewall (NGF)	51.4%	73	30	15	11	13
Net: Email security (SWG and SEG)	51.4%	72	33	15	8	12
Net: DNS security/DNS firewall	49.6%	70	33	21	4	13
Net: Network intrusion detection system (IDS)/intrusion prevention system (IPS)	47.5%	67	41	19	7	7
Net :Network segmentation	46.0%	64	41	15	10	9
Analysis: SIEM (security information & event manager)	45.0%	63	34	25	6	12
Host: Continuous monitoring and assessment	42.7%	61	37	18	11	16
Host: Malware protection system (MPS)	42.0%	60	43	22	6	12
Host: Endpoint or extended detection and response (EDR/XDR)	43.1%	59	28	26	5	19
Host: Vulnerability remediation	40.6%	58	42	24	5	14
Net: Web proxy	43.0%	58	36	19	6	16
Log: Endpoint OS monitoring and logging	40.1%	57	38	18	12	17
Log: Log management	39.4%	56	40	23	10	13
Host: Ransomware prevention	40.3%	56	27	26	11	19
Net: Ingress filtering	40.6%	56	39	18	10	15
Log: Endpoint application log monitoring	38.8%	54	33	27	10	15
Net: Web application firewall (WAF)	37.3%	53	52	16	11	10
Net: Egress filtering	37.9%	53	42	22	5	18
Analysis: Customized or tailored SIEM use-case monitoring	38.1%	53	32	22	13	19
Analysis: Risk analysis and assessment	38.4%	53	38	27	9	11
Net: Network traffic monitoring	36.9%	52	42	21	11	15
Net: DoS and DDoS protection	35.9%	51	48	15	13	15
Host: Behavioral analysis and detection	36.4%	51	29	27	9	24
Log: DNS log monitoring	33.3%	47	43	25	6	20
Net: Asset discovery and inventory	33.3%	47	39	26	12	17
Net: Network access control (NAC)	33.1%	46	31	23	14	25
Host: Application whitelisting	33.3%	46	34	23	11	24
Analysis: External threat intelligence (for online precursors)	33.1%	44	32	23	12	22
Host: Data loss prevention	29.4%	42	35	27	13	26
Analysis: Threat intelligence (open source, vendor provided)	30.9%	42	29	29	14	22
Net: Packet analysis (other than full PCAP)	30.8%	41	33	23	10	26
Analysis: Threat intelligence platform (TIP)	29.4%	40	28	27	8	33
Net: SSL/TLS traffic inspection	30.3%	40	39	23	6	24
Host: User behavior and entity monitoring	28.7%	39	34	23	10	30
Analysis: SOAR (security orchestration, automation, and response)	29.1%	39	30	19	9	37
Analysis: Threat hunting	28.4%	38	36	28	9	23
Analysis: Frequency analysis for network connections	29.2%	38	33	25	7	27
Analysis: E-discovery (support legal requests for specific information collection)	27.3%	36	29	22	5	40
Analysis: AI or machine learning	27.7%	36	26	20	6	42
Net: Deception technologies such as honey potting	24.6%	33	29	22	11	39
Net: Malware detonation device (inline malware destruction)	24.6%	33	31	23	11	36
Net: Full packet capture	23.9%	32	35	26	9	32
Net: NetFlow analysis	23.9%	32	33	23	16	30
Other	25.5%	13	10	11	5	12

Figure 19. Technology in Use and Deployment Status, Sorted by Percentage "All Systems" (Q3.26: n=150)

While each organization has distinct challenges, there is some benefit to projecting based on this chart. The author's (Crowley) speculation on why the projects at the top of the list of all systems have gotten there is that network security controls have been in place for many years. A network-implemented solution represents the older paradigm of perimeter protection. These solutions can be deployed with the IT teams as networks are updated. While users are affected by VPN solutions in a way that requires changes in behavior, the rest of the technologies topping the list have no requirement of user behavior change. Related, a VPN forces users through a new channel to access data, but once configured, it is minimally impactful on the user.

Technology, regardless of deployment status, is a source of strong opinions from most cybersecurity professionals. To assess the reasons why some technology scored well, such as VPN (Grade=+79), which is the highest-ranked technology in Figure 20, will require speculation.

The highest-ranking tools score at the top because they do something well and the tools are likely in the enlightenment or productivity phase of the hype cycle.[4] In this continued speculation, the lowest scorers are relatively new or fail to do the task for which they were purchased. That may be no fault of the technology (full-PCAP not allowed to capture due to legal restrictions) or failure of the technology to adapt (full-PCAP being outmaneuvered by advancing encryption protocols).

Finally, the middle of the pack looks like the technology that works well only when you've applied the appropriate customization and tailoring for your environment. This takes time, dedicated staff, and cooperation with the protected systems' owners and IT administrators. Cooperation and time are often an unnecessarily scarce commodity in the cybersecurity space.

Figure 20 (shown on the next page) represents the GPA for each technology based on the grades respondents assigned to that technology. The GPA is calculated on a 4-point scale, where A is 4 and F is 0, divided by the number of responses per technology.

To be fair, the GPA is based on the respondent's opinion, and we do not have a fully developed assessment rubric for this. Take this respondent's opinion-based GPA scoring as anecdotal opinions on a product category, not specific products.

[4] "Gartner Hype Cycle," www.gartner.com/en/research/methodologies/gartner-hype-cycle

Category: Question	A	B	C	D	F	GPA
Net: VPN (access protection and control)	53	52	16	11	2	3.11
Analysis: SIEM (security information and event manager)	49	44	25	7	5	3.08
Log: Endpoint OS monitoring and logging	47	42	29	7	9	3.03
Net: Next-generation firewall (NGF)	45	44	30	8	6	2.99
Host: Endpoint or extended detection and response (EDR/XDR)	45	37	27	10	7	2.98
Net: Web application firewall (WAF)	43	47	25	11	6	2.97
Host: Ransomware prevention	46	36	25	13	8	2.96
Log: Endpoint application log monitoring	38	41	37	3	9	2.96
Host: Vulnerability remediation	44	42	38	6	3	2.95
Net :Network segmentation	44	36	28	11	7	2.95
Analysis: Customized or tailored SIEM use-case monitoring	39	45	28	10	7	2.93
Host: Malware protection system (MPS)	40	50	30	11	3	2.91
Net: Ingress filtering	40	41	34	9	3	2.90
Net: DNS security/DNS firewall	38	47	29	11	8	2.90
Net: Egress filtering	39	34	39	7	8	2.88
Net: DoS and DDoS protection	45	33	38	11	7	2.88
Net: Email security (SWG and SEG)	44	35	29	15	9	2.88
Log: DNS log monitoring	38	45	28	13	8	2.87
Net: Web proxy	38	33	35	9	14	2.87
Host: Continuous monitoring and assessment	39	38	37	10	6	2.85
Analysis: Risk analysis and assessment	31	45	34	7	8	2.85
Net: Network intrusion detection system (IDS)/intrusion prevention system (IPS)	41	38	32	14	5	2.85
Other	10	7	11	2	7	2.83
Log: Log management	36	49	28	15	5	2.83
Net: Network access control (NAC)	36	36	30	13	13	2.83
Host: Behavioral analysis and detection	39	39	36	13	5	2.82
Net: Network traffic monitoring	33	40	41	9	6	2.79
Analysis: Threat intelligence platform (TIP)	32	36	30	13	13	2.78
Host: Application whitelisting	30	41	30	13	13	2.77
Analysis: Frequency analysis for network connections	31	28	34	11	21	2.76
Analysis: External threat intelligence (for online precursors)	32	36	29	16	10	2.74
Net: Deception technologies such as honey potting	31	26	33	13	22	2.73
Analysis: Threat intelligence (open source, vendor provided)	28	37	43	10	9	2.70
Analysis: E-discovery (support legal requests for specific information collection)	24	39	30	14	14	2.68
Net: SSL/TLS traffic inspection	29	32	37	14	14	2.68
Analysis: Threat hunting	32	30	36	17	10	2.67
Net: Packet analysis (other than full PCAP)	24	40	30	16	15	2.65
Analysis: AI or machine learning	27	26	37	13	20	2.65
Host: User behavior and entity monitoring	27	41	34	18	7	2.64
Net: Malware detonation device (inline malware destruction)	25	27	37	13	23	2.63
Host: Data loss prevention	30	32	35	20	15	2.62
Net: Full packet capture	27	30	36	17	17	2.61
Net: Asset discovery and inventory	31	27	46	16	10	2.61
Net: NetFlow analysis	27	24	43	13	12	2.61
Analysis: SOAR (security orchestration, automation, and response)	23	26	38	12	17	2.61

Figure 20. GPA Rating (Q3.27: n=132)

If you want to see these two charts combined (like we did), see Figure 21.

Category: Question	SUM Prod (Full + Partial)	GPA	Total
Net: VPN (access protection and control)	109	3.11	132
Net: Network intrusion detection system (IDS)/intrusion prevention system (IPS)	108	2.85	125
Net: Web application firewall (WAF)	105	2.97	126
Net :Network segmentation	105	2.95	119
Net: Email security (SWG and SEG)	105	2.88	123
Net: Next-generation firewall (NGF)	103	2.99	127
Host: Malware protection system (MPS)	103	2.91	131
Net: DNS security/DNS firewall	103	2.90	125
Host: Vulnerability remediation	100	2.95	130
Net: DoS and DDoS protection	99	2.88	127
Host: Continuous monitoring and assessment	98	2.85	124
Analysis: SIEM (security information and event manager)	97	3.08	125
Log: Log management	96	2.83	128
Log: Endpoint OS monitoring and logging	95	3.03	125
Net: Ingress filtering	95	2.90	124
Net: Egress filtering	95	2.88	119
Net: Web proxy	94	2.87	115
Net: Network traffic monitoring	94	2.79	123
Analysis: Risk analysis and assessment	91	2.85	117
Log: DNS log monitoring	90	2.87	124
Host: Endpoint or extended detection and response (EDR/XDR)	87	2.98	119
Log: Endpoint application log monitoring	87	2.96	119
Net: Asset discovery and inventory	86	2.61	120
Analysis: Customized or tailored SIEM use-case monitoring	85	2.93	122
Host: Ransomware prevention	83	2.96	120
Host: Behavioral analysis and detection	80	2.82	127
Host: Application whitelisting	80	2.77	114
Net: SSL/TLS traffic inspection	79	2.68	112
Net: Network Access Control (NAC)	77	2.83	115
Host: Data loss prevention	77	2.62	117
Analysis: External threat intelligence (for online precursors)	76	2.74	113
Analysis: Threat hunting	74	2.67	115
Net: Packet analysis (other than full PCAP)	74	2.65	110
Host: User behavior and entity monitoring	73	2.64	120
Analysis: Frequency analysis for network connections	71	2.76	104
Analysis: Threat intelligence (open source, vendor provided)	71	2.70	118
Analysis: SOAR (Security Orchestration, Automation, Response)	69	2.61	99
Analysis: Threat intelligence platform (TIP)	68	2.78	111
Net: Full packet capture	67	2.61	110
Analysis: E-discovery (support legal requests for specific information collection)	65	2.68	107
Net: NetFlow analysis	65	2.61	107
Net: Malware detonation device (inline malware destruction)	64	2.63	102
Net: Deception technologies such as honey potting	62	2.73	103
Analysis: AI or machine learning	62	2.65	103
Other	23	2.83	30

Figure 21. Deployment State and GPA Rating (Q3.26 and Q3.27: n=142,132)

Tying Pieces Together

The equation for successful SOC operation is additive: people (staff) plus capabilities (process) plus technology. Our survey addressed several instances that tie these elements together.

Monitoring

Drilling down into the monitoring capability, we asked exactly what this entailed. (This question is new this year.) Detection of threats is at the top. But in many cases, it seems that the monitoring team doesn't support incident handling, at 47% *(174/368)*. This is an area of improvement the authors think warrants focus: better integration between monitoring and incident handling. See Figure 22.

Figure 22. Security Monitoring Details (Q3.11: n=368)

Because most computer networks never shut down, the SOC should probably monitor 24 hours a day, every day. We asked if this is the case, and it is in most cases (details are in Figure 23). Only 62 respondents (17%) indicated that the SOC doesn't operate 24 hours per day. The "Yes" contingent answered that a purely in-house *(144, 38%)* 24-hour operation is the most popular approach to this, trailed substantially by mixed *(89, 24%)*. See Figure 23.

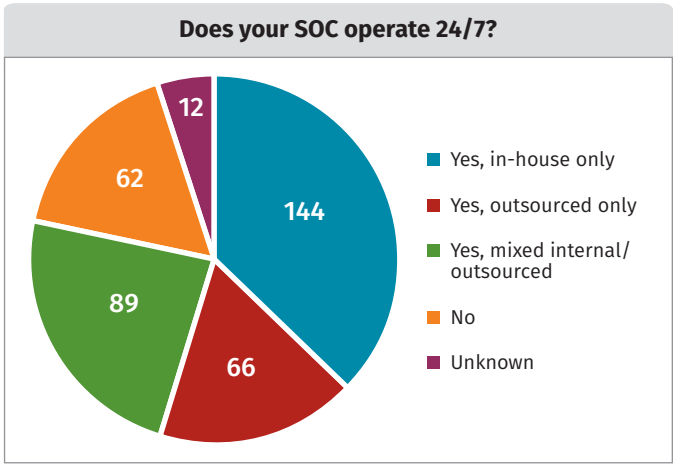

Figure 23. 24/7 Operations or Not? (Q3.12: n=373)

While running 24/7 operations, the primary task is identification of issues (see Figure 24). We have a section later about technology, but capability is integrally connected to the technology used to perform it. So, we asked how the data correlation of event data for identification of issues is performed. To the authors, the top answer "through our SIEM" *(151, 47%)* is no surprise. Our projection is that this obvious dominance changes soon, as more SOCs shift this effort into SOAR *(36, 11%)*, XDR *(35, 11%)*, and MDR *(24, 7%)* platforms. See Figure 24.

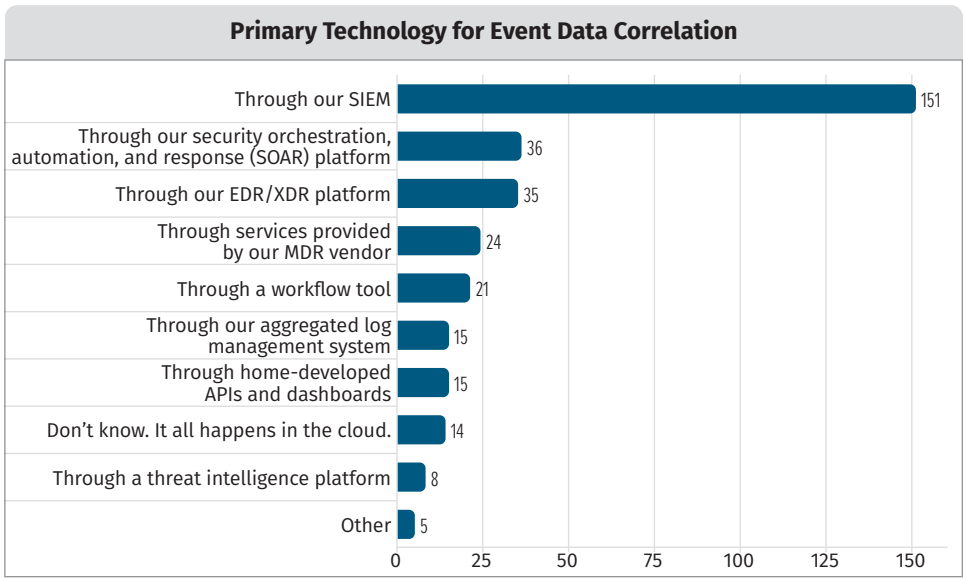

Figure 24. Event Correlation Technology (Q3.20: n=324)

The author (Crowley) isn't suggesting this is necessary or necessarily advantageous based on the technologies involved. But rather, his opinion is that the staff's assessments of performance of the tool drives replacement of the tool rather than reconsidering the implementation and programmatic elements surrounding the technology. This opinion is not derived directly from survey responses. It is a fusion of assessment and observation of SOCs, the marketing pressures within the technology market, and generalizations around human behavior when faced with criticism over SOC performance. The tools don't usually speak up to defend themselves and point out the deficiencies of implementation or tool operator.

Visibility Across Systems

As these SOCs are correlating events, there are varying categories of systems into which they provide visibility. This occurs to a greater degree on different types of systems, so we include smart devices in Figure 25 and mobile devices in Figure 26.

Does your SOC support nontraditional computing devices such as smart sensors, building devices, building monitoring, manufacturing, industrial control systems, OT (operations technologies), and system assets considered as part of the IoT?

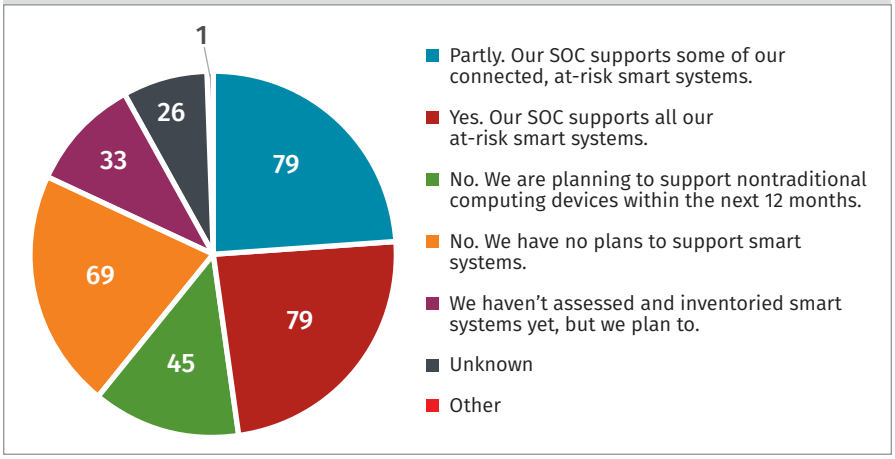

Figure 25. Smart Device Support (Q3.16: n=332)

Most respondents *(158, 48%)* indicated that they either partially or fully support smart devices.

When asking what is being used for this, the MDM is clearly ahead, but not by enough to call it a certain choice if there are new deployments. Importantly, this question (Q3.18) asked respondents to include all that apply for monitoring technology for multiple items, and some respondents answered multiple items. MDM, EDR, and XDR are specifically intended for this type of nontraditional compute device monitoring. The authors see continued development of this technology, in addition to the use of cloud-provider-native monitoring tools.

What are you using to monitor your mobile devices, extranet, and cloud partner (AWS, Azure, etc.) resources? ***Select all that apply.***

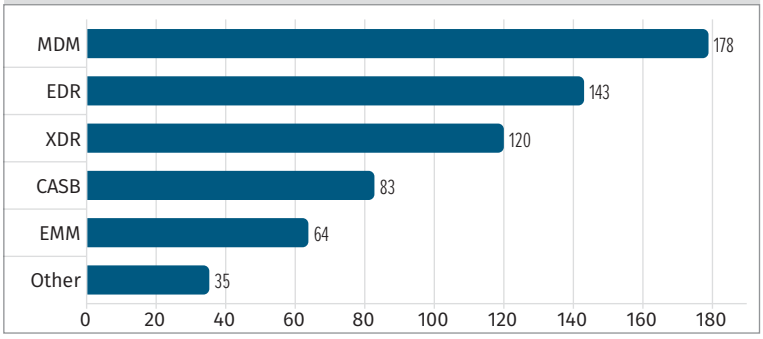

Figure 26. Monitoring Technology (Q3.18: n=311)

Also, on the topic of nontraditional arrangements, we inquired into the techniques for monitoring OT networks. Of the respondents who monitor OT as part of their SOC, most *(103, 32%)* do so converged with IT systems. This is closely followed by separately *(80, 25%)* as the next most common. Another technique is to use separate technology but the same staff for monitoring, and if these two groups are considered together (because physical separation of the visibility and protection instrumentation is consistent for both groups), then that grouping *(127, 39%)* exceeds the "together" responses (see Figure 27). This is important because there appears to be a strong urge for compartmentalization of these resources onto their own network, and the conceptual boundary appears to be extended to the defensive monitoring systems as well. This compartmentalization approach has strong advocates on both sides of the subject in the OT cybersecurity community. From this survey, it's about evenly split in terms of how the SOCs monitor OT.

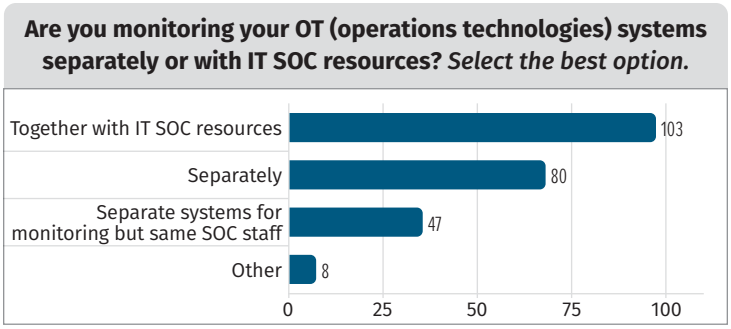

Figure 27. OT Monitoring Strategy (Q3.17: n=326 but n=88 excluded from chart because there's no OT)

Relationships

In discussing OT/IT convergence, it's apropos to also highlight the SOC to IT operational monitoring. It is the opinion of the author (Crowley) that there are opportunities for tool reuse, converged visibility, collaboration, and coordinated hunting activities if these teams are empowered to share data and ideas.

In Figure 28, it looks like a lot of the SOCs agree. The strongly segmented responses "very little direct communication" *(54)* and "there is no relationship" *(27)* are 19% *(81)* of responses, whereas the strongly positive "integral part … not technically integrated" *(119)* and "…integrative dashboards…" *(77)* are 45% of the responses *(196)*. This is a call to action to leverage your scarce resources to further the collaboration or integration of two core operational capabilities: SOC and IT.

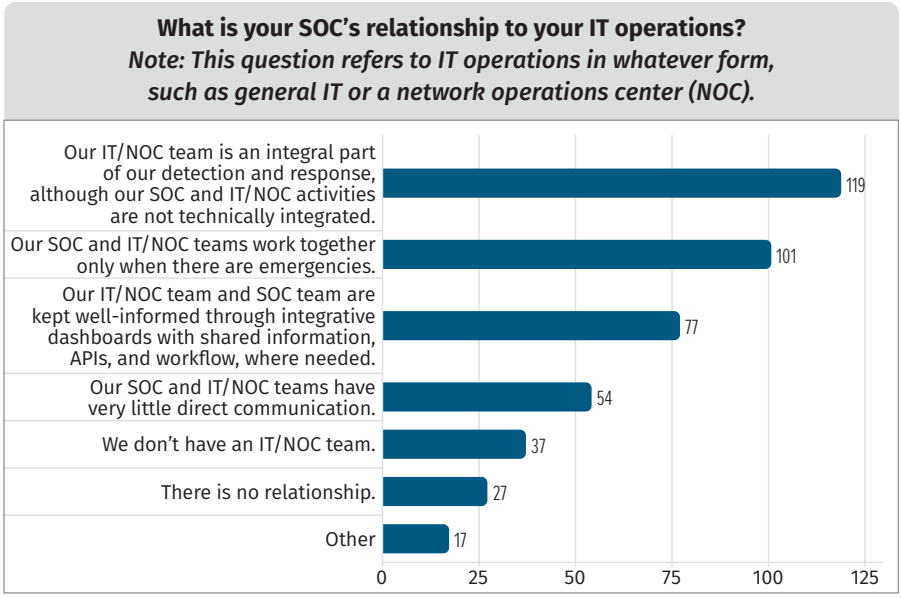

Figure 28. SOC to IT Relationship (Q3.8: n=432)

The only likely counter-indication the authors see in this situation would be that the SOC might lose some oversight capability of potentially malicious or negligent system administrators; the IT admin could also see what the SOC sees about his or her (insider/malicious) activity and adjust to avoid detections. The value of the visibility as a deterrent likely outweighs the risk of a crafty insider threat intentionally evading monitoring.

Our advice? Monitor IT admin access by using a behavioral monitoring strategy to identify patterns that could be attributable to malicious insider activity. This would cover the other common fear of sharing the security visibility data with IT peers, if an attacker seizes credentials and is using your tools to see what you see about the attacks. This scenario of loss of control and use would likely represent a behavioral change from the normal baseline of that account, giving you a potential alert late in the phase of an attacker intrusion.

Investment: The Determining Factor

Looking at SOC budgets reveals some interesting observations. First, 30% of respondents *(71/240)* are not aware of the overall SOC budget. (See Figure 29.) This may be indicative of respondent role according to Q2.5 where 270 (52%) were analyst, administrator, or architect roles.

However, the next most popular funding amounts in Figure 29 indicate budgets of less than $500,000: $100,000 *(39)*, $100,001–$250,000 *(28)*, and $250,001–$500,000 *(21)*. While regional staff salary variation could certainly play a part here, this doesn't represent a realistic view of the investment to run a SOC, especially if there's a 24/7 performance expectation.

In short, a realistic model of required investment should be developed, specifically around the SOC team size of 2 to 10 members.

Most respondents *(56%, n=133/236)* follow a formal budget process. (See Figure 30.) But there may be issues in actually determining funding.

We asked how the funding was determined, and Figure 31 shows the breakdown. Most respondents *(n=93)* indicated that the SOC management and organization management work closely on this. However, the majority still believe that management does not heed recommendations from SOC leaders in allocating funds *(n=83+25+25)*.

What is your estimated annual budget for new hardware, software licensing and support, human capital, and any additional costs?

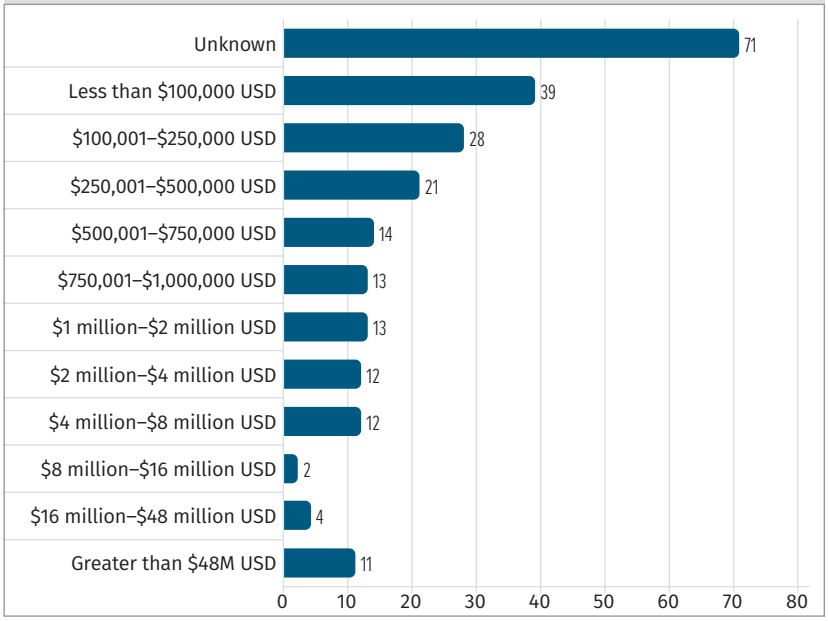

Figure 29. Overall Budget (Q3.51: n=240)

How would you characterize your process for establishing IT/security budget for next-year funding?

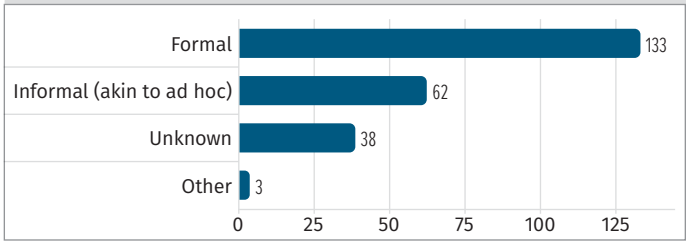

Figure 30. Budgeting Method (Q3.56: n=236)

How is funding allocated in your organization? ***Select the best option.***

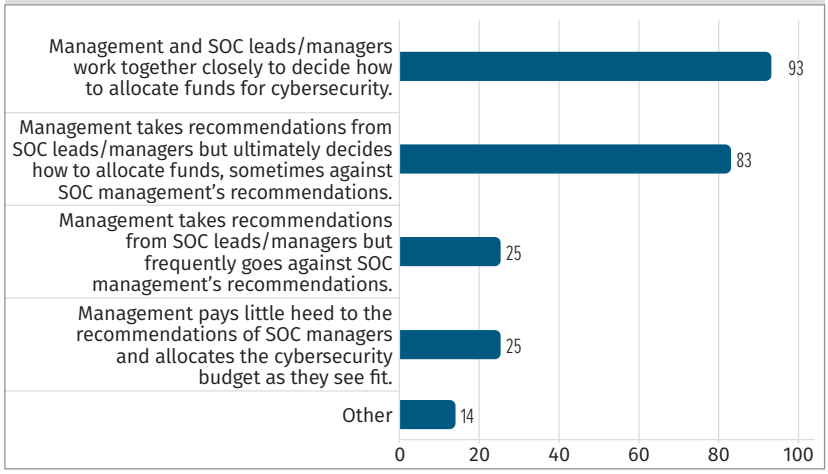

Figure 31. Funding Allocation (Q3.52: n=240)

While there seems to be more cooperation and less frustration expressed with organizational management not heeding SOC management advice on funding, a problem may still remain, suggesting that a formal budgeting method should be derived from metrics showing the need for the work. So, we checked to see if the respondents who said they provided metrics tended to operate in an environment with a formal budgeting process. Figure 32 shows that there is a clear difference, where formal budgeting is more present where metrics are delivered. We suggest taking this as an attribute of maturity for your SOC.

Measuring for Success

Metrics are a critical component of the SOC's interaction with the organization, in the authors' opinion. Yet, most of the metrics used fail to effectively characterize the value the SOC provides to the business. Admittedly, we're taking the optimistic view that the SOC does provide value and could calculate it.

Among respondents, 70% *(193/274)* indicated that they provide metrics to accomplish this communication. See Figure 33.

We asked about satisfaction with these metrics, and of those who answered, 78% *(136/187)* are either satisfied *(92)* or very satisfied *(54)* with the metrics. See Figure 34.

We have been conducting this survey for several years, so we looked back to see what the responses from previous years said about metrics and metrics satisfaction. We are using percentages to compare because the numbers varied in each year. In 2019, 57% said they provided metrics, but the survey didn't include questions on metrics satisfaction. In 2021, 77% provided metrics, of which 67% were satisfied. This year's survey shows a 7% drop from 2021 in providing metrics but an overall increase in satisfaction of about 12% on how these metrics help gauge the effectiveness of the SOC.

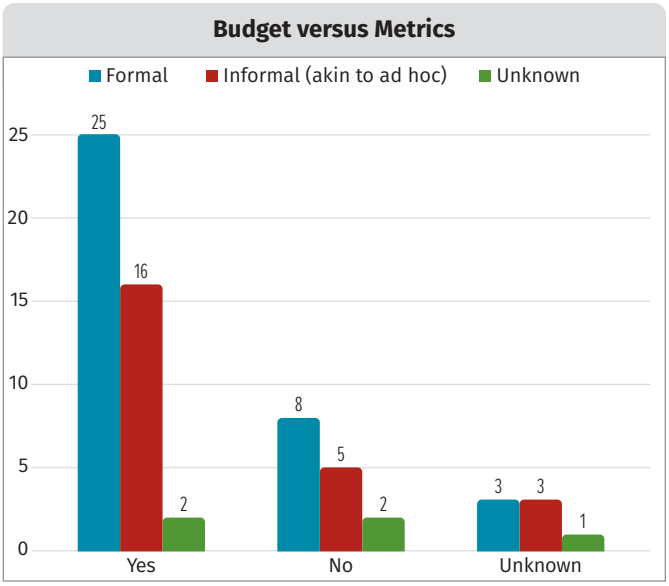

Figure 32. Budget Method and Metrics (Q3.35 and Q.56: n=240)

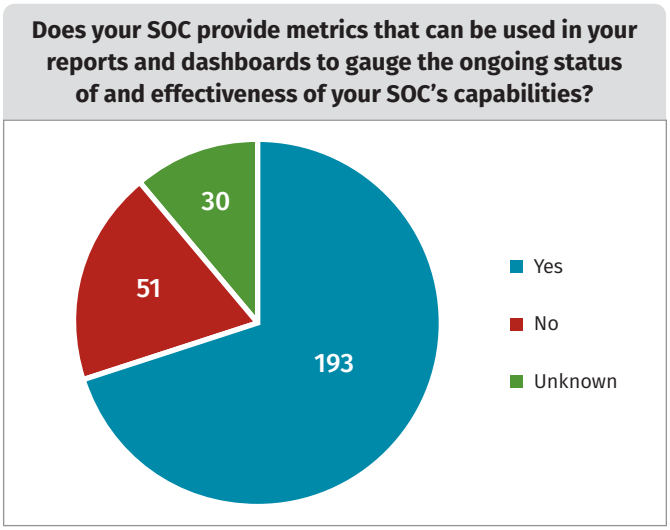

Figure 33. Metrics Provided (Q3.35: n=274)

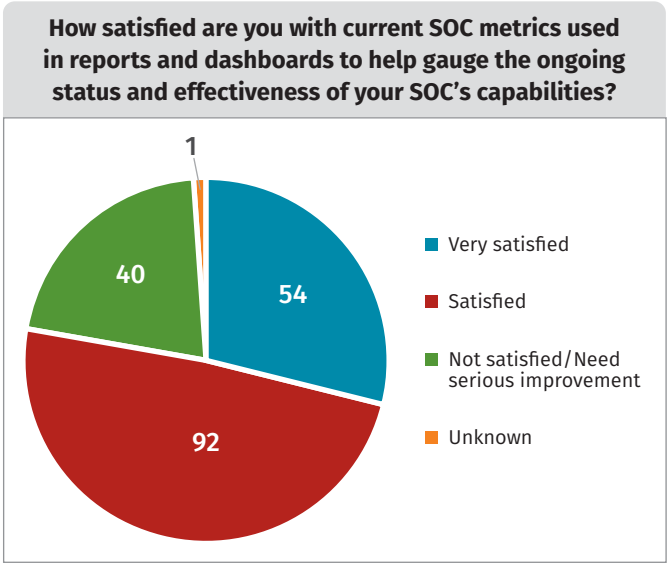

Figure 34. Metrics Satisfaction (Q3.36: n=187)

Looking at Metrics That Tie Value to Effectiveness

But how to tie funding to metrics that ascertain how SOC value is determined? Questions 41 to 44 aimed to determine this by first investigating cost-per-record values related to cybersecurity incidents and then exploring potential methods of calculating loss prevention provided by the SOC. Ultimately, it is the promise of loss prevention that compels organizations to fund SOCs. Let's trace out what the respondents said.

It seems like most respondents are not calculating cost-per-record values. Figure 35 shows that 58% answered that they don't calculate this. The author's recommendation to these respondents and the readers of this report: Start this effort. It will be imprecise at first, so be patient and nurturing. But this tactical operational value should be correlated to funding to secure the right amount of funding to protect the organization's information.

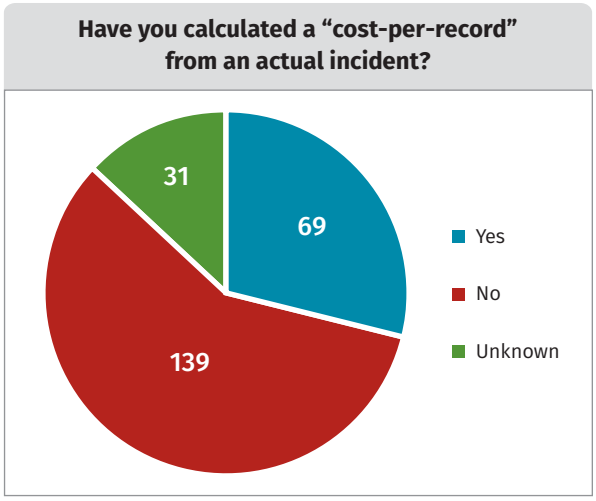

Figure 35. Cost-per-Record Calculation Percentage (Q3.41: n=239)

Where they have been calculated, the numbers are all over the map, with no clear consensus, as is displayed in Figure 36.

Consolidating this to eliminate the distinction between the record types, there's still no clarity on which is the most common value, as shown in Figure 37. This suggests that the calculations aren't consistent and that the conditions of intrusions aren't consistent among the respondents. A per-record cost should be consistent between organizations for the same record type. The takeaway here is that this measurement isn't done often enough and has yet to achieve consistency across various organizations. But there's still value to the effort. As one example, your insurers are using an estimated value for their calculations of your insurance premiums related to this. You should have an idea of handling costs and impact costs.

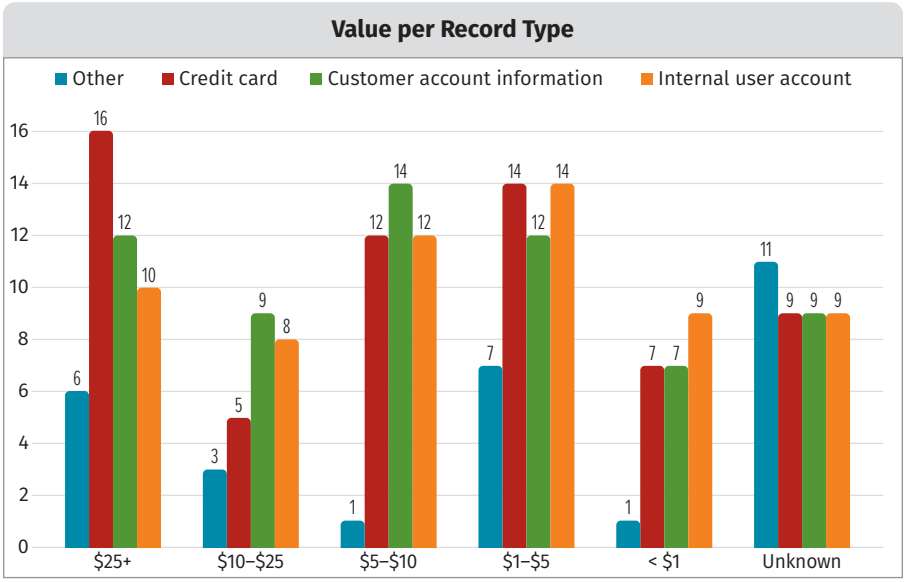

Figure 36. Cost-per-Record by Type (Q3.42: n=42)

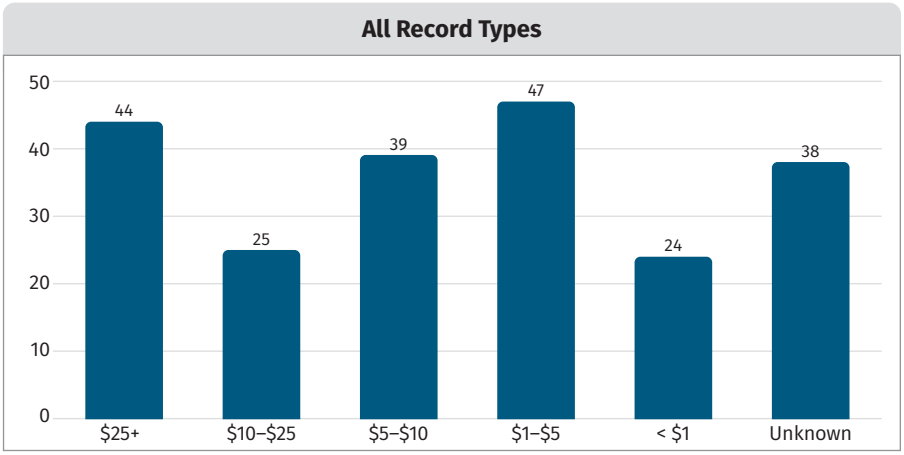

Figure 37. User Account Cost-per Record (Q3.42: n=42)

Of course, we went on to ask the next obvious question (in the authors' manner of thinking): whether respondents are calculating the value of the SOC by using some form of comparison between the SOC intervening and the SOC not intervening. Like cost-per-record shown in Figure 37, most *(58%, n=140/244)* said that they don't calculate this, as shown in Figure 38.

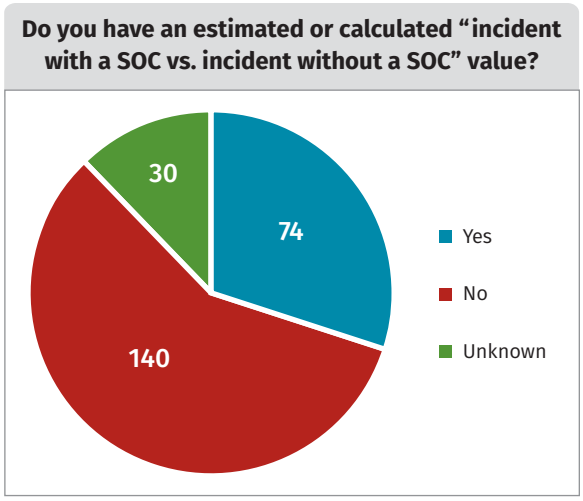

Figure 38. Estimated or Calculated Value Provided by the SOC (Q3.43: n=244)

You can see where this is going. If the respondent is calculating it, we wanted to know. So, the next question asked is what help the SOC is (if it is, in fact, helping). Only a small number said the SOC's existence made the handling effort more costly than without the SOC *(n=7)*, and the impact more costly *(n=4)*. But many more saw 10% handling *(n=19)* and impact *(n=24)* reduction. The most popular response for handling reduction was 50% reduction *(n=22)*, with the incident impact reduction of 50% for *(n=18)* respondents (see Figure 39). This provides a compelling story to show value to management when you go into that formal budget to try to assure the organization management works closely with you to allocate the SOC budget.

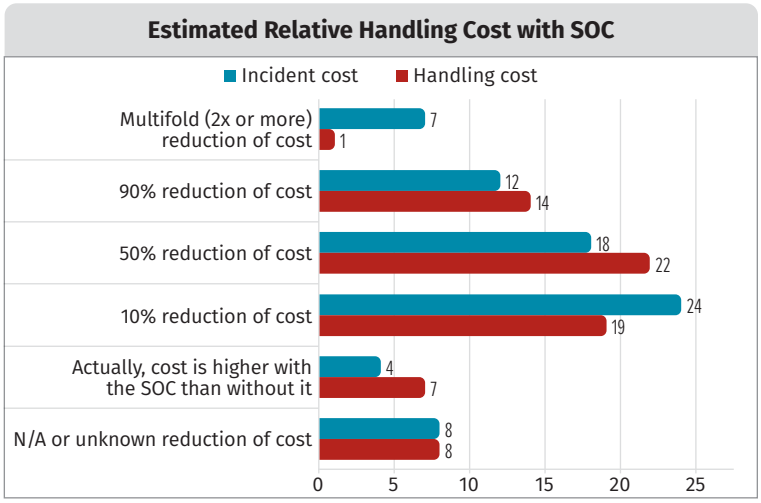

Figure 39. Estimated SOC Value (Q3.44: n=73)

Summary

We've covered a lot of territory with this survey. It represents a major expansion of our linguistic offering, and we're optimistic that we'll soon offer the survey natively in other languages.

We have taken a capabilities-based approach to the concept of a SOC. The way to use this survey is to assess your capabilities compared to your peers. In doing so, you'll see that most SOCs have the same capabilities but accomplish them through varying levels of internal performance and outsourcing. Most SOCs deliver metrics, and many are starting to deliver calculations on the value of the defense provided.

For SOCs with lesser maturity, adding missing capabilities is the next step. Doing so through outsourcing often provides speed and high-value proposition without the accompanying tailoring and customization. The next step would be assuring performance of metrics. For more mature SOCs, delivering calculations related to data protected and loss prevention provided is the step to take.

Follow These Calls to Action

- Match your organization against our demographics and related results.
  - ✔ Compare the size of your organization's workforce versus survey-reported workforce size.
  - ✔ Check SOC staffing levels in comparison to your business growth over time.
  - ✔ Evaluate the capabilities of your SOC against those reported in this survey as commonly present to develop what you lack.
  - ✔ Compare what survey respondents frequently outsource with what your organization outsources to evaluate whether there's an opportunity to outsource capabilities or bring them back in-house.
- Be sure that the trends which are important to your organization are going in the right direction!
  - ✔ Define and track the critical metrics to your organization.
  - ✔ Make sure you have at least one metric that depicts the value your SOC provides.
- Explore the "Technology: What Is Getting a Passing Grade?" section to see how your organization stacks up against the community.
  - ✔ Compare your implementation of technology with how other organizations have implemented it.
  - ✔ Ask the following hard questions:
    - Are you still just investing in technologies that most other organizations have successfully transitioned to production?
    - When you buy technology for your SOC, do you have a plan to get it deployed to full production?
- Are you considering the effectiveness of the SOC in budgeting for its resources?
  - ✔ Make sure your organizational management listens to SOC leadership where important!
  - ✔ Keep your metrices in mind!

Sponsor

SANS would like to thank this survey's sponsor: