SANS

Analyst Program

Survey

A SANS 2021 Survey: Security Operations Center (SOC)

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

October 2021

Executive Summary

For the last five years, SANS has conducted the security operations center (SOC) Survey, and this year's report continues to provide insight to SOC leaders and other professionals. For 2021, we conducted a long questionnaire and then followed up with respondents for more details about their responses to some of the questions. The motivation for this report is to provide SOC managers, team leads, vendors, and industry analysts with an opportunity to peer into what others in the industry are doing.

The SANS Institute is uniquely positioned with trusted relationships throughout the world. We endeavor to provide transparent analysis and include qualitative insights, where appropriate. Because we asked follow-on questions of individuals who took the survey, this report also includes the explanations shared in those responses.

This report is organized into several sections, beginning with this executive summary, detailed demographics, and key findings. We then cover SOC capabilities, staffing, technology, funding, and deployment strategies, before concluding the report with survey challenges and a summary.

How to Use This Report

Throughout this report, you will find references to this year's survey questions and the response set. These references, which appear in italics, correspond with a full, de-identified version of the response set, accessible at https://soc-survey.com/2021. We encourage you to use this resource to investigate any additional questions you might have about the responses.

Let's start off by looking at a question we asked survey takers about their experience in this past year: **Has your organization suffered an incident or intrusion in the past 12 months?** *(Q3)* Of the 319 respondents who answered this question, 104 (33%) indicated that, yes, there was an incident or intrusion in the protected environment in the last year. Eighty-nine respondents were unsure (12%) or declined to answer (16%), and 126 (40%) indicated that they didn't suffer any incidents. The responses are illustrated in Figure 1.

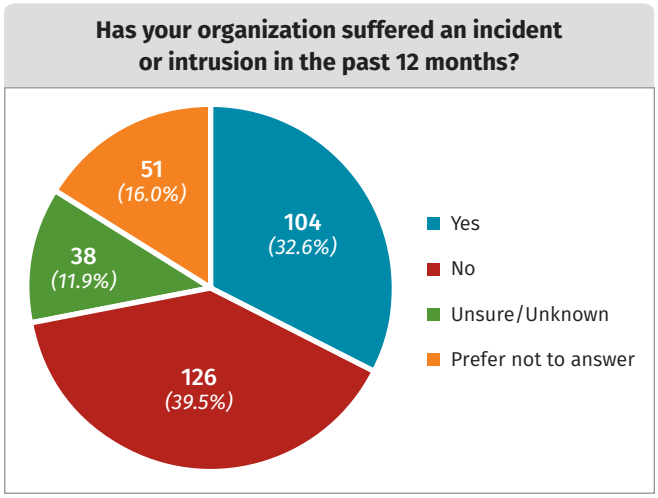


Figure 1. Number of Incidents or Intrusions (Q3 n=319)

In defining the strategic vision for the SOC in the coming year, respondents identified their biggest challenge. We asked them to select the best option when answering: **What is the greatest challenge (barrier) with regard to full utilization of your SOC capabilities by the entire organization?** *(Q55)* The most frequently cited challenge is the lack of skilled staff in the SOC *(n=24)*; however, it had only one more response than the lack of automation and orchestration *(n=23)*. It seems that the solution to these challenges is having skilled people and being able to automate the mundane tasks. In the 2020 SOC Survey, lack of skilled staff *(2020, column 79: n=23)* was the top challenge. But last year more people cited lack of management support *(2020, column 79: n=22)* than automation and orchestration *(2020, column 79: n=)*.[1] See Figure 2 on the next page for the full breakdown of this year's responses.

[1] "2020 SOC-Survey: A Tale of Two SOCs," https://soc-survey.com/2020-SOC-Survey-Tale-of-Two-SOCs.pdf, p. 9

When we followed up on this question in subsequent email conversations, we found that most respondents indicated a need for both more staff and additional skills for existing staff. However, most of the focus was on the missing skills. A common thread was that deep technical knowledge is the bigger need. While many analysts understand the cybersecurity issues, without deeper network, operating system internals, and overall IT architecture and operations technical knowledge, they were not productive in the SOC. Also mentioned frequently were soft skills—in particular, critical, analytical thinking and customer service. Threat hunting skills were the top lack in direct cybersecurity skills.

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

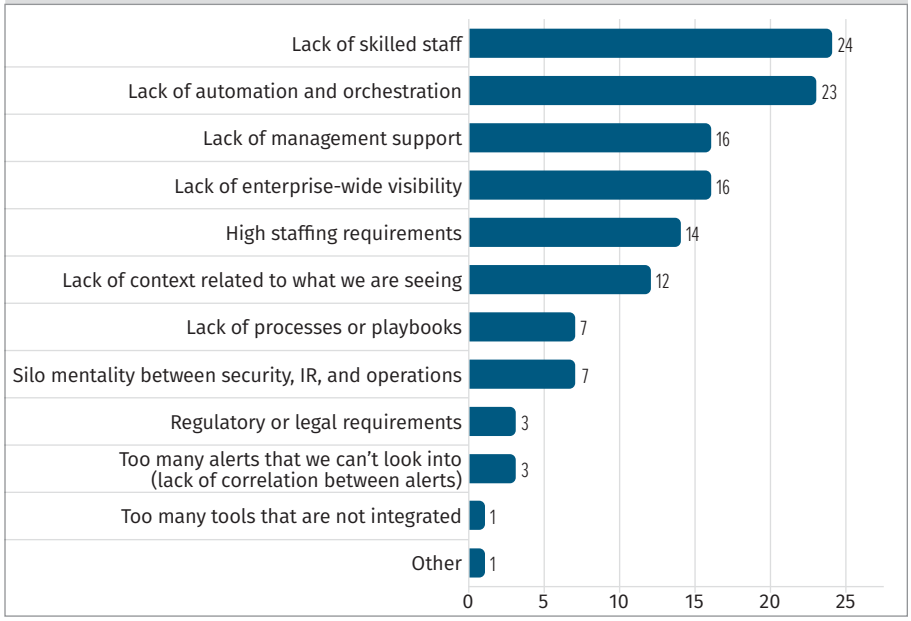


Figure 2. Greatest Challenge to Full Use of SOC Capabilities (Q55 n=127)

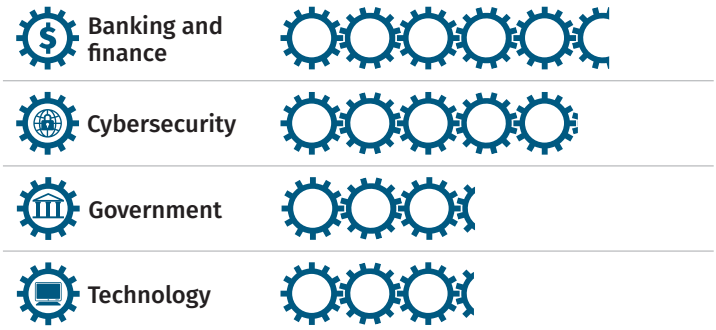
Automation was seen as needed primarily to reduce time to detect and respond. This recovered time enables existing staff to better handle the load of events and alerts, as well as meet security metrics used to judge performance objectives. An example from a follow-up message was a simple integration of dozens of data sources that were used to identify data into a portal. This portal served to consolidate information across multiple company divisions. The portal reduced Level 0 to Level 2 response times by 25%.

Detailed Demographics

The respondents who answered the survey provide insights from their personal experiences. In the opinion of the authors, we don't yet have a representative sample of the global consortium of cybersecurity operations centers.

We do have a broad spectrum of respondents across the globe and industry sectors, and we work hard to get as diverse of a population as possible. From respondents' self-characterizations, we find that they usually work in a smaller organization, from financial, government, or high tech. Their companies are primarily based in North America and Europe. Their work roles tend to be Security analyst/Administrator or Security manager/Director. These are the people who are either doing the work or managing the team doing the work. See Figure 3 on the next page.

Top 4 Industries Represented

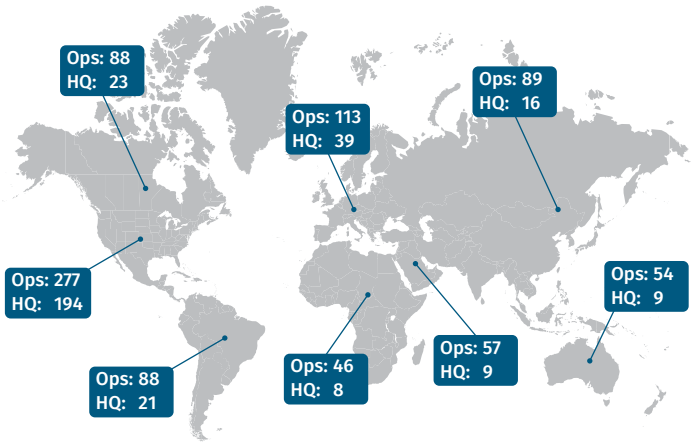


Each gear represents 10 respondents.

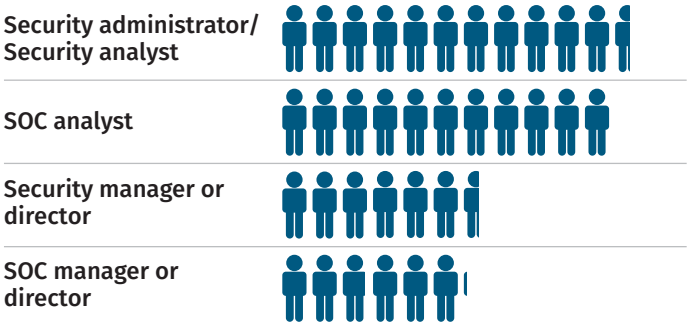
Organizational Size

Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 5 respondents.

Figure 3. Demographics of Respondents

Key Findings

Metrics

In our follow-up conversations, the most common issue was the lack of existing metrics. The most commonly required metrics mentioned were time to respond, percent of coverage of endpoints by required security agents, and SOC analyst performance metrics.

To determine if metrics are being reported, the survey asked: **Does your SOC provide metrics that can be used in your reports and dashboards to gauge the ongoing status of and effectiveness of your SOC's capabilities?** *(Q33)* Of the 144 responses, 111 (77%) indicated yes. Compared to last year, more metrics are being reported (77% this year vs. 70% in the 2020 Survey).[2] This year, however, only about 67% (49+21 out of 105) were very satisfied or satisfied with the metrics used, according to this question: **How satisfied are you with current SOC metrics used in reports and dashboards to help gauge the ongoing status and effectiveness of your SOC's capabilities?** *(Q34)* Among respondents, 33 said that they are not satisfied and their metrics need serious improvement.

[2] "2020 SOC-Survey: A Tale of Two SOCs," https://soc-survey.com/2020-SOC-Survey-Tale-of-Two-SOCs.pdf

The next question asked how these metrics were produced: **If you are providing metrics to your constituents, select the option that best describes the methods employed in your environment to collate and present that data.** *(Q34)* Of the 130 respondents who answered the question, 26 (20%) indicated that they are fully automated, and 52 of them (40%) said that the metrics are produced in a partially automated fashion with substantial manual effort required.

Work from Home

We asked if an organization allowed SOC staff analysts to work from home: **Do you allow SOC staff analysts to work remotely?** *(Q13)* Not surprisingly, 210 (87%) of the 241 who answered this question said yes.

We asked a follow-on question of those who said yes to ask about various criteria in considering who gets to work from home: **What factors are considered in determining whether a SOC staff analyst can work remotely?** *(Q14)* Figure 4 illustrates those responses.

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

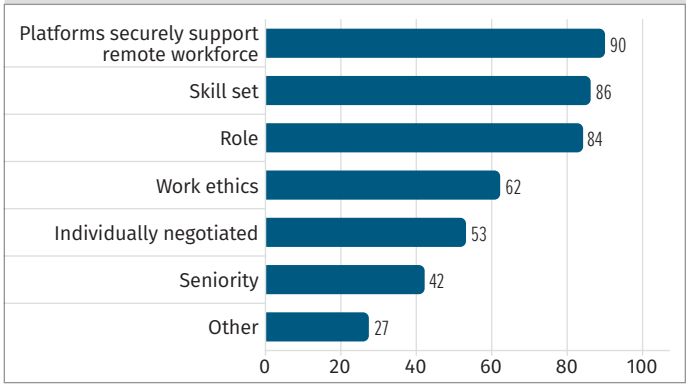


Figure 4. Factors in Allowing Remote Work (Q14 n=187)

In Question 14, most open text responses contained a reference to COVID-19, health concerns, or pandemic *(12 responses)*. Another commonly repeated element of the other responses was essentially that "SOC work is all remote" *(8 responses)*.

One interesting outlier in the open text was "System classification." While there's not a lot to go on with such a terse response, it might indicate that those analysts who work on less-sensitive data can work from home, while more sensitive systems still require onsite monitoring. It's interesting to the authors that this was the only mention of data sensitivity. (We peer into how organizations are assessing responsibility for systems later in the survey, in Figure 12.)

Staff Size

The wording of our question about staffing levels was intentionally long because we wanted respondents to count staff in a consistent way. We asked: **What is the total internal staffing level (i.e., all related positions) for your SOC, expressed in terms of full-time equivalents (FTEs)? What is the number of FTEs specifically assigned to the management of your SOC systems, not just to analysis of the data from your SOC systems?** ***Note: Include both employees and in-house, dedicated 1099 contractors who function as employees in your SOC. If responsibilities are shared across a team, estimate the equivalent FTE amount of time spent among the team.*** *(Q42)* The most commonly cited SOC size was from 2 to 10 people *(44 responses)*. See Figure 5 for the breakdown of non–size-adjusted counts of the responses. The same question asked how many of the staff working were dedicated to managing the technology, depicted in red in Figure 5.

What is the total internal staffing level (i.e., all related positions) for your SOC, expressed in terms of full-time equivalents (FTEs)? What is the number of FTEs specifically assigned to the management of your SOC systems, not just to analysis of the data from your SOC systems? ***Note: Include both employees and in-house, dedicated 1099 contractors who function as employees in your SOC. If responsibilities are shared across a team, estimate the equivalent FTE amount of time spent among the team.***

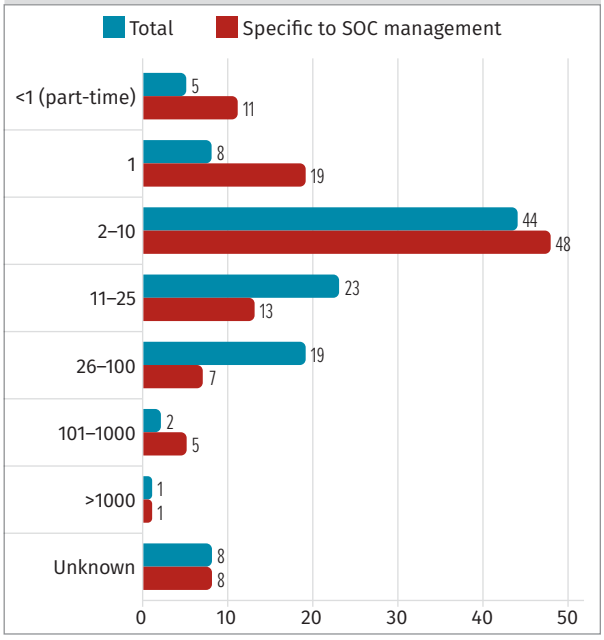


Figure 5. SOC Staff Size Total and SOC Tech Administration (Q42 n=110/112 total/management)

SOC Capabilities

Capability Depiction

Most of the responses received are from people who work within a SOC, and we presume they know what elements should be in a SOC. Having a basis for capability reference is an important method for assuring adequate operations as well as forming a basis for maturity and development trajectory, so we asked how people are assessing what needs to be done.

Figure 6 depicts the capabilities we asked about: **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 as a result of hosting in the cloud?** *Mark N/A those that do not apply.* *(Q10)* The chart suggests consensus among respondents about what a SOC does. It also depicts where capabilities are internal or outsourced, a topic we'll revisit in more detail. Incident handling, protection of assets, monitoring for issues, vulnerability management, and the management of the systems to do all of this are the top capabilities cited.

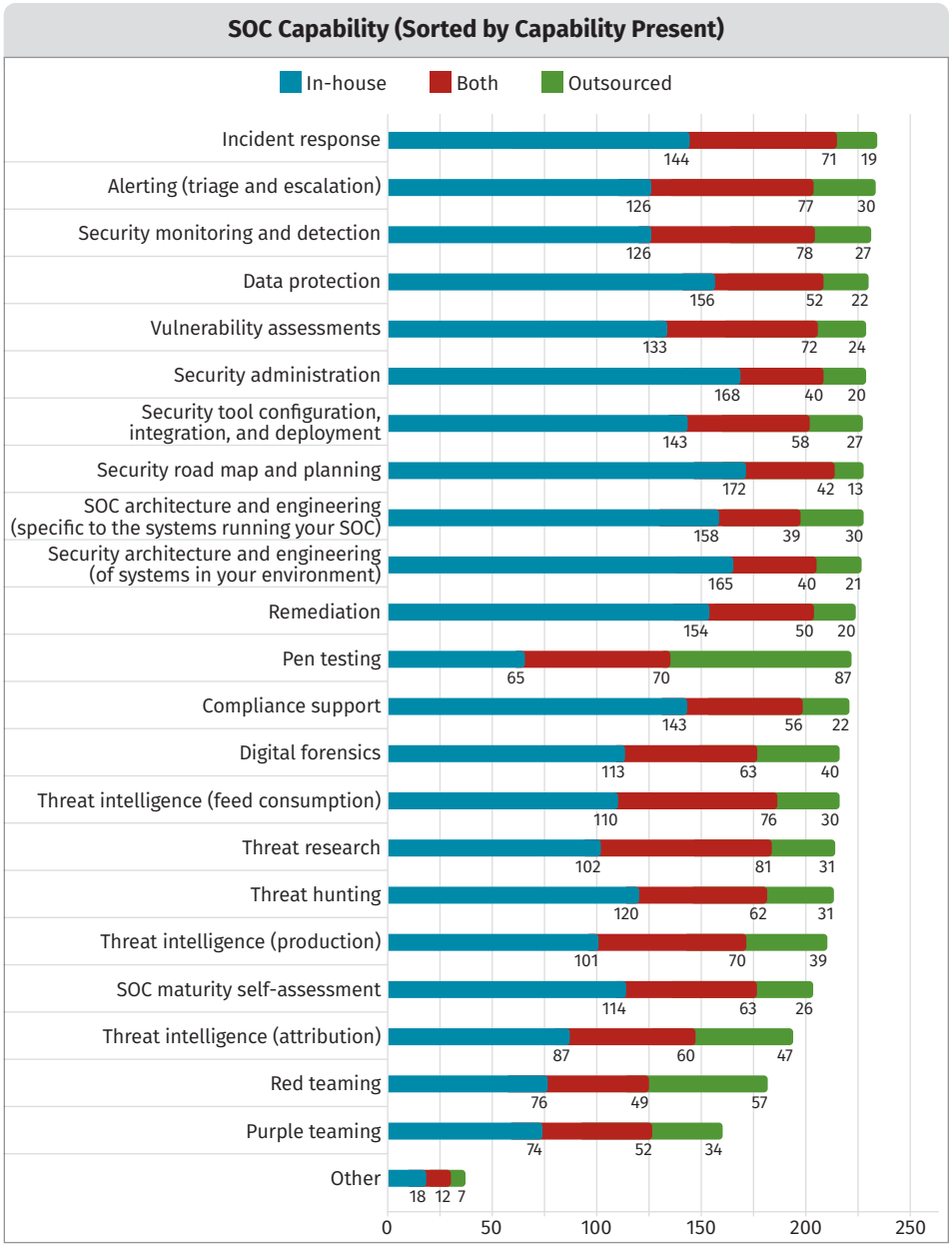


Figure 6. SOC Capabilities—Internal Only, Both Internal and External, and Outsourced Only—Ranked on the Capability Being Reported as Done (Q10 n=244)

Looking at this same data via a 100% bar chart, another angle emerges. Foremost in the recharting of Question 10 (shown in Figure 7), we see that for those who are doing it, some of the items are far more likely to be outsourced. The outsourced capabilities above 50% (combining outsourced and both) are: pen testing, red teaming, purple teaming, threat intelligence (attribution), threat intelligence (production), threat research, and other. If you look back at Figure 6, you'll notice that those are less likely to be done at all. (You can also flip forward to Figure 14, where we take one more look at this.) Pen testing and red teaming are reported as the highest outsourced-only percentages.

Respondents who participated in the follow-on emails indicated that they are generally happy with the mix of outsourcing. Threat hunting and threat intelligence mentioned as outsourced functions would be much more effective with detailed business and corporate IT knowledge. This becomes a challenge with outsourcing, because the outsourced company doesn't have internal insight. Keeping these capabilities in-house would require hiring more people with those skills, likely adding to head count.

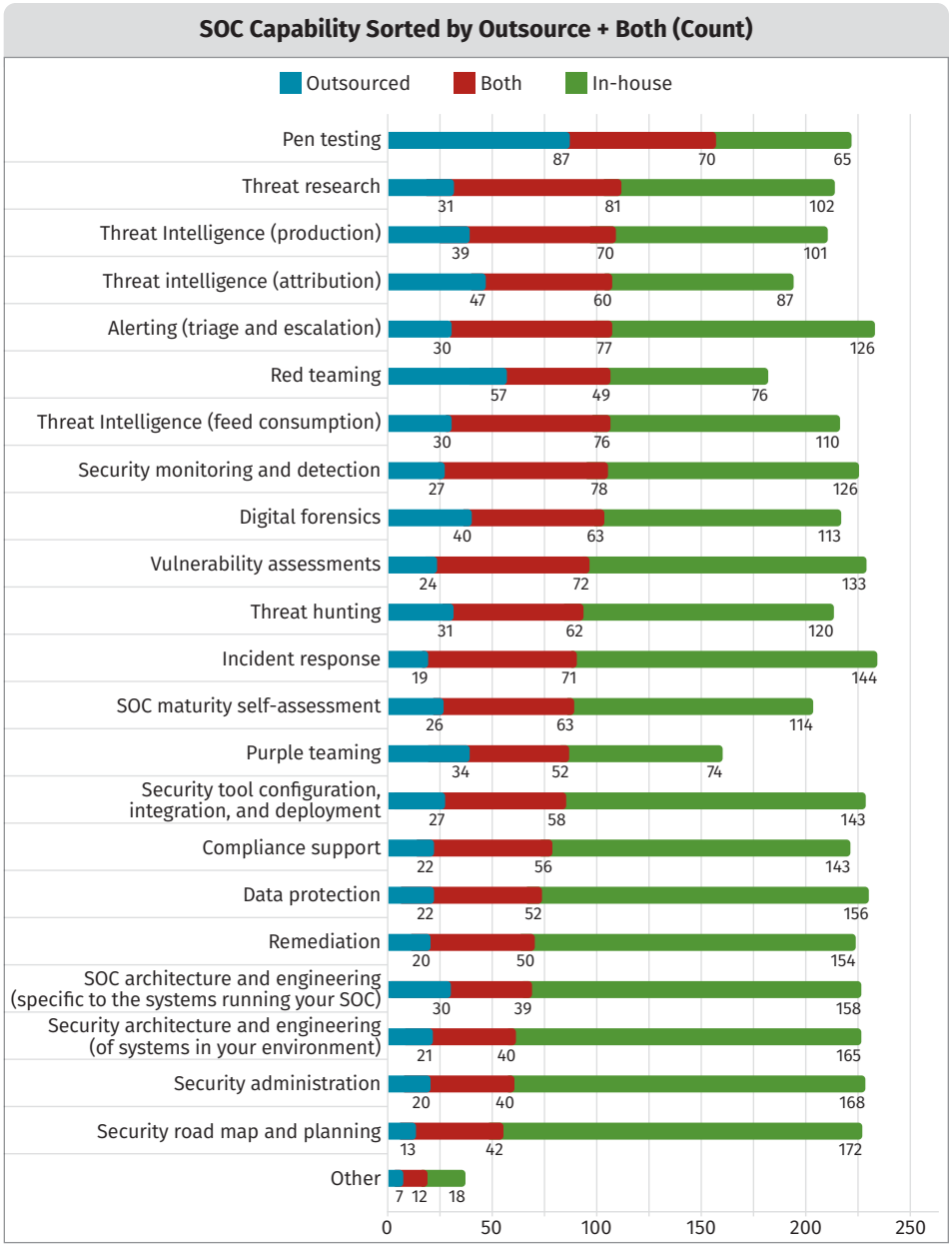


Figure 7. SOC Capabilities—Outsourced Only, Both Internal and External, and Internal Only—Sorted on the Capability Being Outsourced (Q10 n=205, Q10 n=244)

Because monitoring is a critical capability, we investigated further by asking a detailed question about the form the SOC monitoring capability takes: **What is included in your security monitoring activities?** ***Select all that apply.*** *(Q11)* The most popular answer is detection of threats—that is, looking for signs of attack within the environment. The second-most popular is tracking access and usage, or the inspection of activity to attempt to differentiate authorized from unwanted. Figure 8 shows the breakdown.

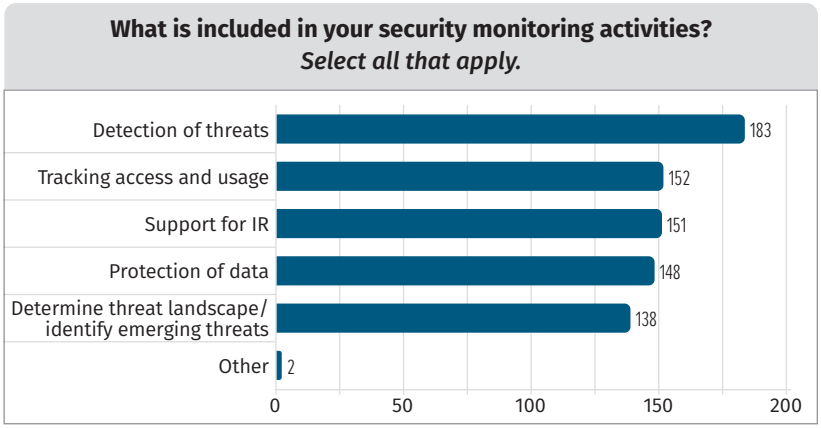


Figure 8. Monitoring Capability Details (Q11 n=205)

Because computers rarely sleep, we asked if the SOCs ever stop operating. The authors presume that the SOC needs to be 24/7, but we posed the question if it actually is (or is not) operating 24/7 because this is something for the business to decide to fund. We asked: **Does your SOC operate 24/7?** *(Q12)* The response options include variations on whether these operations are accomplished with in-house staff or if an MSSP helps deliver this non-stop monitoring. Figure 9 captures the results in a chart, showing that most 24-hour-a-day operations are an internal only capability. The second-most popular response is a mix of internal and external (via MSSP) monitoring to deliver 24-hour-a-day coverage. Noteworthy in Figure 9 is that more responses indicated that 24-hour operations are not sustained than outsourcing exclusively. Outsourced-only operations for 24-hour coverage are not very popular.

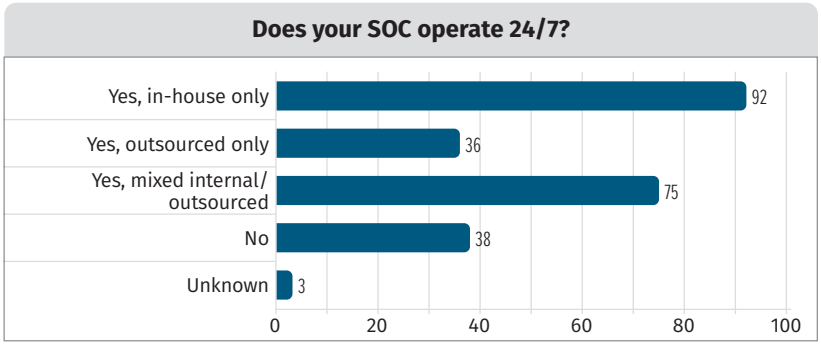


Figure 9. 24/7 Operations (Q12 n=244)

To the MSSPs: Your customers (and prospective customers) seem to prefer a mixed model to deliver 24/7 coverage, so plan for effective data and alert interchange.

To the customers of MSSPs: If you are asking the MSSPs for effective coordination to accomplish a mixed model of 24/7 coverage, prepare to pay for the customization or adjust your operational capability to match what the MSSP offers.

Because the vision of SOC capability is rarely a singular vision, SOCs usually look to a reference model to define their SOC capabilities. We asked: **What model(s) are you using to determine what capabilities your SOC needs?** ***Select all that apply.*** *(Q15)* Note that respondents could select multiple models.

We speculate that the models may be used for different purposes within the SOC. For example, NIST CSF is an extensive framework, and the SOC-CMM asks questions to assess maturity versus the NIST CSF. MITRE ATT&CK® is especially good at assessing visibility issues and helping with detection engineering. ATT&CK can also be used to guide hunting, response, and investigations. SOC-Class addresses the functional architecture of the SOC to optimize internal and outsource arrangements. These could be used to assess and direct growth for different aspects of the SOC. The most popular models, as indicated by survey respondents, are NIST CSF and ATT&CK, as shown in Figure 10.

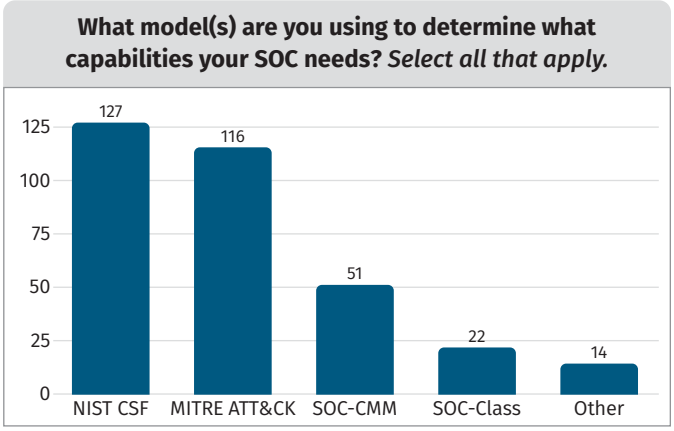


Figure 10. Capability Model in Use (Q15 n=241)

Related to the idea of capability for the SOC is the notion of visibility. We asked: **Estimate the percentage of endpoints that your SOC has asset-type knowledge including endpoint asset type, hardware address or asset identifier, and responsible party/owner.** *(Q27)* A fundamental concept in information assurance/defense is understanding the topography of what is to be defended because it assists in the formulation of defensive strategy and capability.

Figure 11 shows how well SOCs are doing in gaining "full coverage" of the assets to defend. The most popular answer was 76–99%. We converted this into the A–F grading scale, which we asked respondents to use for assessing technology, so it seems fair to do later in this paper (see Tables 1 and 2).

It is the opinion of the authors that collection and visibility are not adequate to accomplish the overall objective of a SOC. They're prerequisite tasks to the more complicated responsibility of analysis.

When the monitoring detects an issue and a SOC starts to handle the issue with its incident handling capability, it is standard practice to notify the affected system owner of the potential for trouble. We asked if asset correlation is performed: **Do you correlate your assets to the responsible system owner or user in your environment?** *(Q28)* Figure 12 shows that most respondents (80%, or 121 of 152) said yes.

Of course, we followed up with an inquiry as to how this correlation is performed: **Select the option that most accurately represents your method of correlating assets to responsible system owner or user for servers and user endpoints in your environment.** *(Q29)* Figure 13 depicts the responses both for servers and endpoints. Automation is the most common method. The authors would rather not be an analyst in the SOC where "manual effort each time" is the prevailing method for correlation.

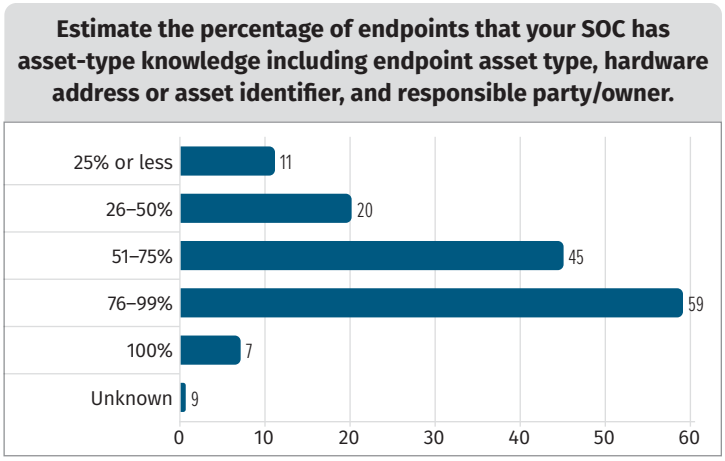


Figure 11. Asset Knowledge According to Self-Assessed Coverage (Q27 n=151)

This is an area where many SOCs need to improve if they want to be effective against attacks. More respondents *(45+20+11=76)* self-assessed visibility into assets as below 75% of endpoints having full coverage than self-assessed *(59+7=66)* as greater than 76%. Not knowing what is to be defended is the pathway to not being able to defend it.

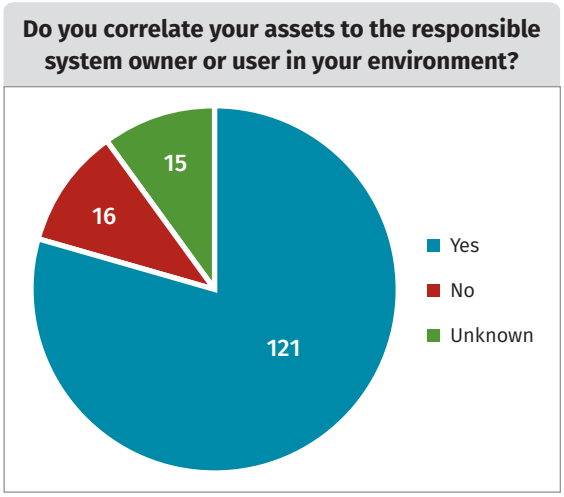


Figure 12. Asset Correlation to Responsible Owner (Q28 n=152)

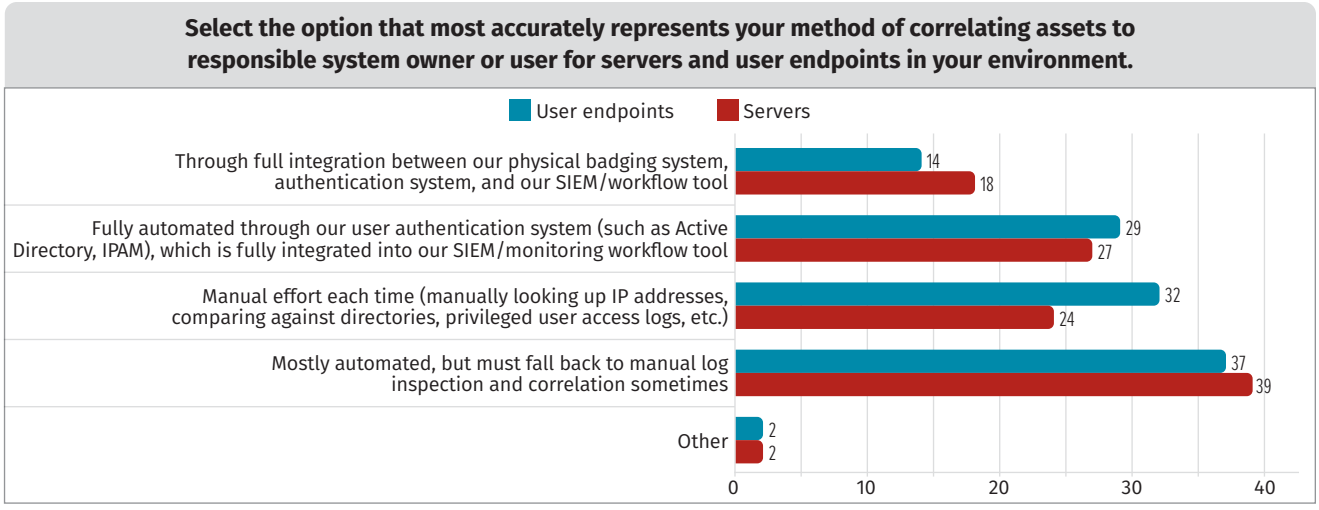


Figure 13. Method of Correlating Assets (Q29 n=114)

Outsourcing

Most SOCs use outsourced capability in some form. Let's look at what's most popular to outsource. Figure 14 shows this, ordered by the most commonly outsourced, again using the data from Question 10: **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 as a result of hosting in the cloud?** *Mark N/A those that do not apply.* (You can look back at Figure 7 to see this in a 100% bar chart in the same order.)

Now that we have some insight into staff capabilities, the next section addresses what staff role composition is present in the surveyed SOCs.

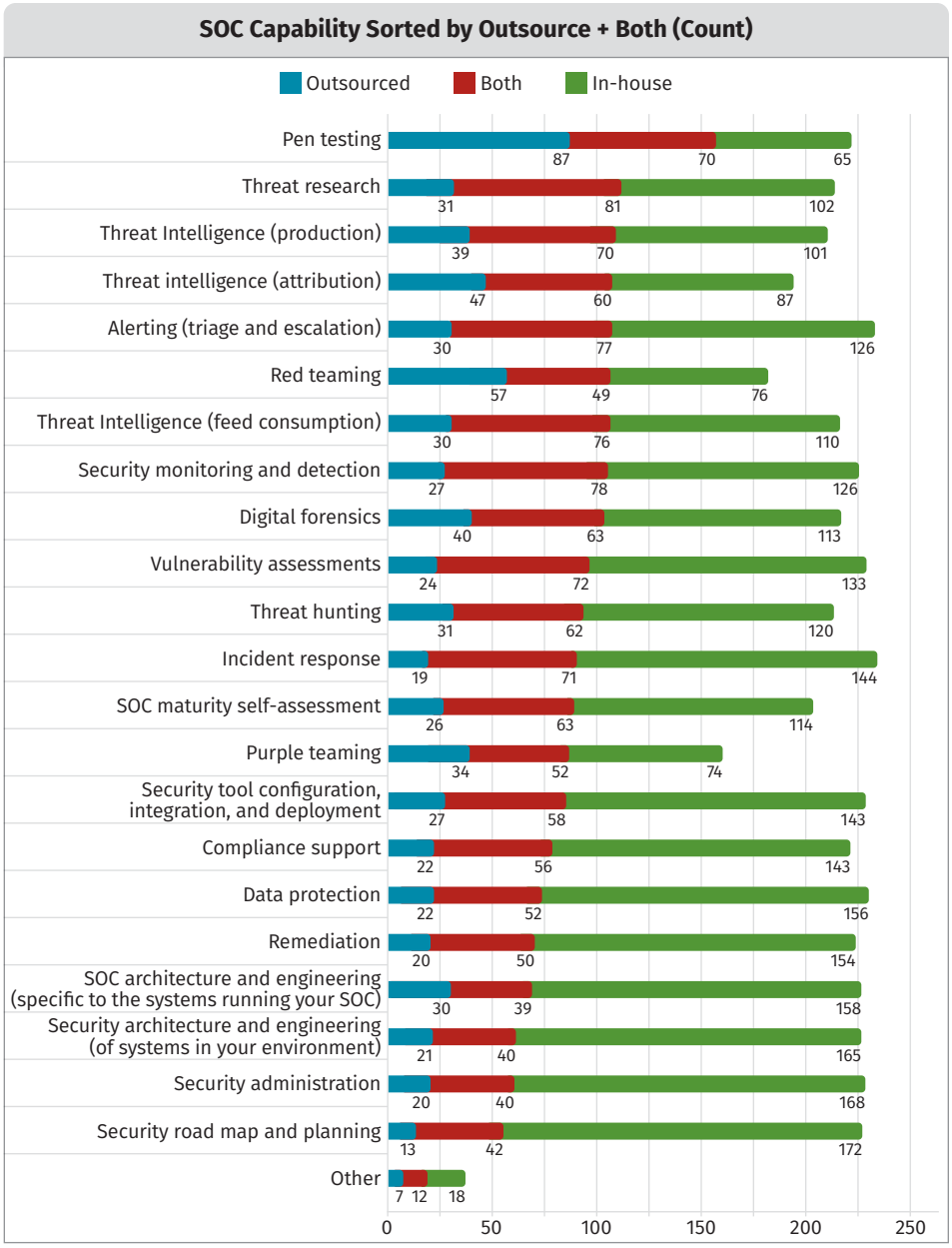


Figure 14. SOC Capabilities—Outsourced Only, Both Internal and External, and Internal Only—Sorted on the Capability Being Outsourced (Q10 n=244)

The skillsets in pen testing (and related red teaming, etc.), as well as forensics and threat intelligence, are reported as being outsourced more frequently. It's the opinion of the authors that this is a result of the way the SOC leverages these disciplines. Unless the SOC covers a very large set of assets, these specialized activities probably don't provide enough work to keep a dedicated specialist busy all the time. These specializations require ongoing dedicated practice, and most organizations resist asking staff who are generalists to jump into dedicated specializations infrequently. Hiring and retaining those specialists becomes a niche plan for consulting firms, which sell the capability as an outsourced offering.

SOC Staffing

Staff Roles and Corresponding Size

Because the staff count doesn't necessarily indicate what roles the staff performs, we asked specifically about staff roles: **To your best estimate, how many of the following positions do you have on staff?** *(Q43)* Figure 15 shows the role count responses, keyed by the answer to Question 42 about the reported overall size (shown earlier in Figure 5).

Training/Retention/Issues Resolution

A perennially reported issue for security operations is the lack of skilled staff. (See Figure 2, where it's the top-cited challenge, for example.) Hiring skilled staff is a challenge when there aren't enough qualified applicants to go around, so the presumption is that the SOCs would try to retain already hired staff. We asked about the duration of staff retention: **What is the average employment duration for an employee in your SOC environment (how quickly does staff turnover)?** *(Q44)* Figure 16 shows the rest of the responses, but the most popularly cited response duration was from one to three years *(47 of 129 responses)*.

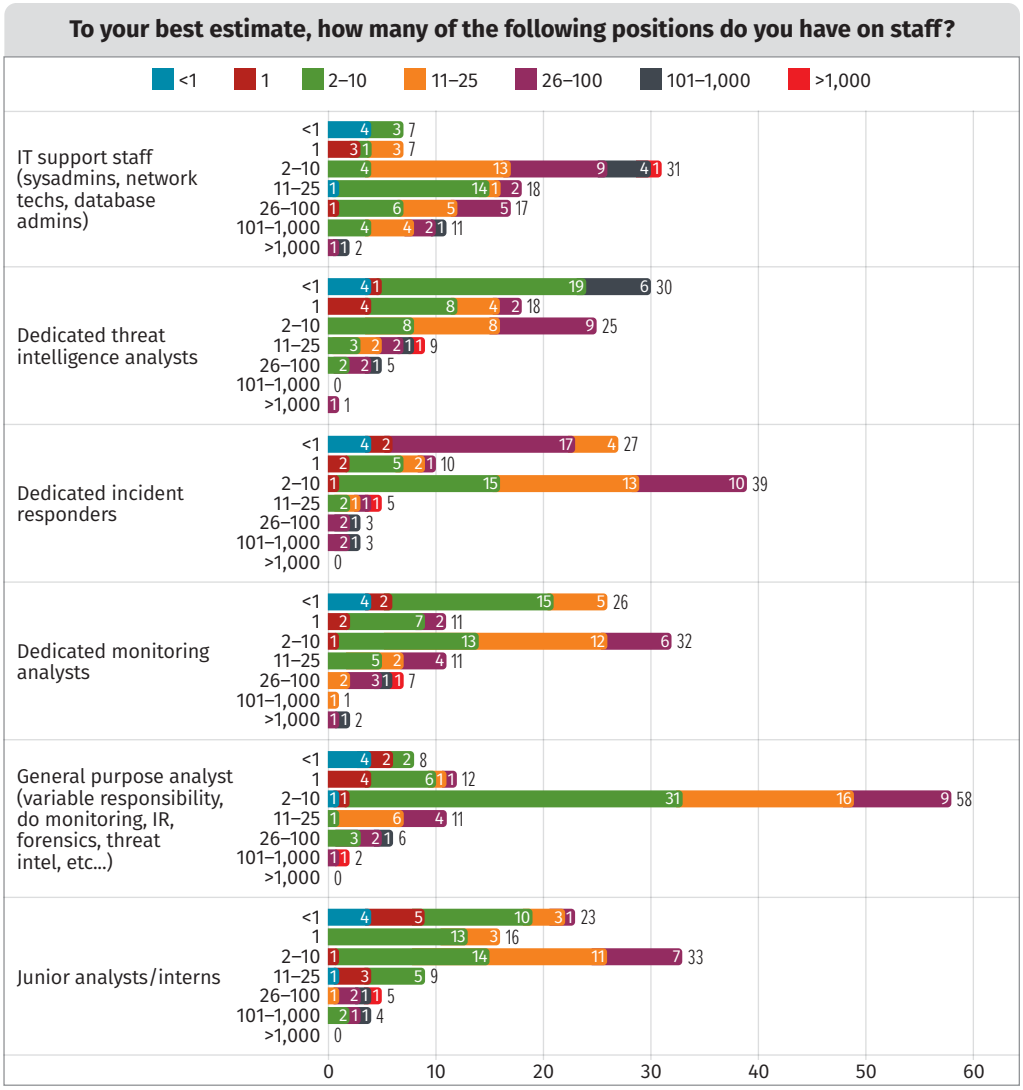


Figure 15. Positions per Reported Staff Size (Q42 and Q43 n=124)

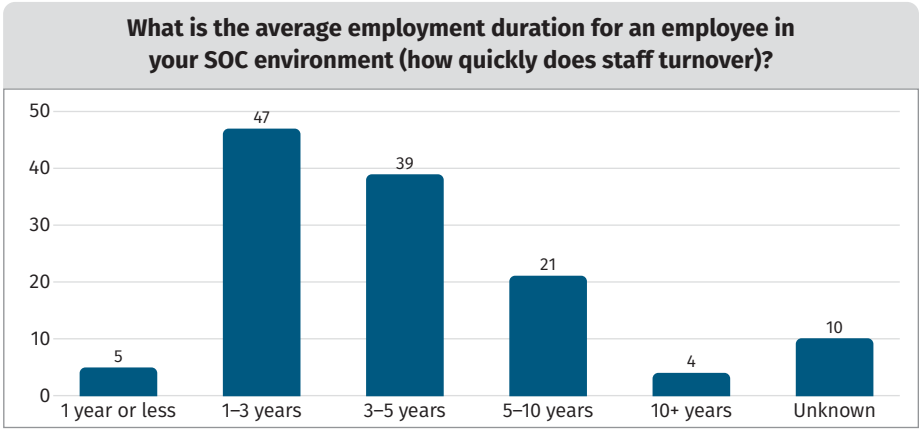


Figure 16. Average Duration of Employment (Q44 n=129)

To retain staff in the SOC, look for ways to keep people energized and engaged. Sending someone to training once a year won't diminish the daily grind enough to retain the person for the long term. Career advancement opportunities also include rotating job roles, which works especially well in smaller teams composed of generalists where there are no vertical progression opportunities. The opportunity to master a new domain of knowledge (e.g., threat intelligence, forensic analysis) is adequate incentive to stay in many cases.

The other strategy for retention that always seems to work is being the only SOC within commuting distance. That's not a joke. Being the only game in town is a solid retention strategy often cited by SOC managers who have that advantage. Recruiting in those circumstances is its own challenge. The move to work from home is extending the geographic hiring range, reducing the lock-in of a single employer by geographic region.

Because there's no one strategy for retention, we used a free format entry field to capture the knowledge from the brain trust who generously participated in the survey: **What is the most effective method you have found to retain employees?** *(Q45)* We're including a word cloud in Figure 17 for visualizing the rest of the comments, but we can summarize it in three words: training, money, mission.

Figure 17. Word Cloud of Most Effective Retention Methods (Q45 n=58)

Per-Analyst Workload

Another perennial problem we're trying to ask in an answerable way is how to decide what is the right count of staff. We posed an open text question: **How do you calculate per-analyst workload?** *(Q38)* Figure 18 shows the frequency response weighted depiction of the words in respondents' answers. It is mostly a negative explanation that, "They don't calculate it." The second-most popular response is primarily using time-per-ticket as a calculation.

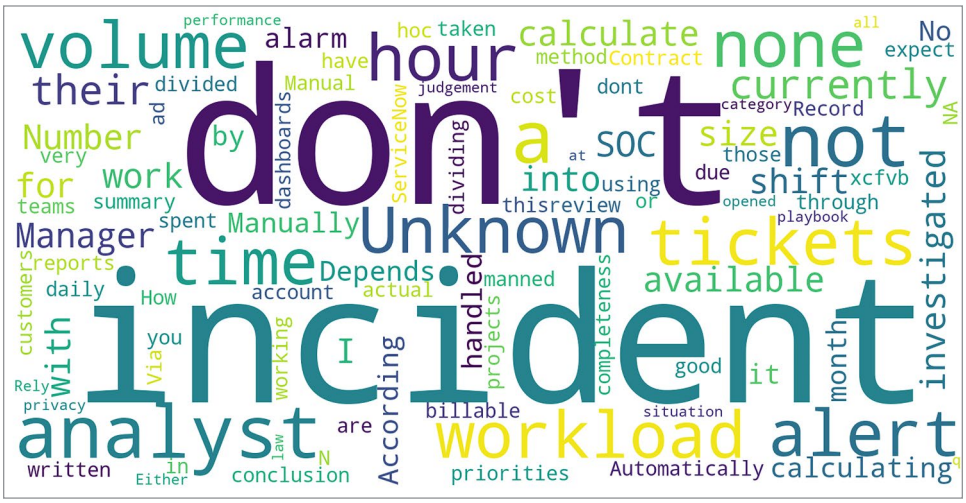


Figure 18. Word Cloud: How to Calculate Per-Analyst Workload (Q38, n=60)

Most Commonly Owned or Planned to Implement

The technology that a SOC uses is a core pillar of its capability. We asked: **Please indicate which technologies are in use to secure the IT systems in your environment.** *(Q23)* We asked for a phased-based status for each technology because we've heard that some companies buy technology but then never successfully complete implementation. We used the status of implementation to determine how far along people are. The phase options were: Production (all systems), Production (partial systems), Implementing, Purchased not Implemented, and Planned. The detailed chart of responses is shown in Table 1. Hopefully the bar charts help identify the most common answers, because we left them in the categories ordered as asked. The top five products (combining phases) in use are: Host: Endpoint or host-based detection and response *(158)*, Analysis: SIEM (security information and event manager) *(156)*, Net: VPN (access protection and control) *(155)*, Net: Email security (SWG and SEG) *(154)*, and Net: Network segmentation *(152)*.

Table 1. Technology in Use per Deployment Phase *(Q23 n=166)*

Category: Question	Production (all systems)	Production (partial systems)	Implementing	Purchased not Implemented	Planned
Host: Vulnerability remediation	73	47	20	2	6
Host: Malware protection system (MPS)	87	47	9	2	6
Host: Behavioral analysis and detection	58	52	15	10	11
Host: Data loss prevention	42	53	19	10	13
Host: Ransomware prevention	60	42	17	10	15
Host: User behavior and entity monitoring	41	54	18	6	16
Host: Endpoint or host-based detection and response	76	57	13	5	7
Host: Application whitelisting	39	39	11	9	20
Host: Continuous monitoring and assessment	62	42	19	9	14
Log: Endpoint OS monitoring and logging	64	52	14	6	14
Log: Endpoint application log monitoring	52	57	17	3	15
Log: Log management	63	50	20	8	9
Log: DNS log monitoring	62	39	22	4	19
Net: Network segmentation	54	59	19	9	11
Net: Email security (SWG and SEG)	94	30	17	6	7
Net: DNS security/DNS firewall	69	28	14	7	18
Net: Asset discovery and inventory	49	48	23	7	20
Net: VPN (access protection and control)	101	29	9	6	10
Net: Full packet capture	30	48	18	3	13
Net: Packet analysis (other than full PCAP)	31	49	15	9	17
Net: DoS and DDoS protection	68	40	13	9	7
Net: Network traffic monitoring	67	50	13	6	13
Net: Web application firewall (WAF)	55	54	20	7	6
Net: Next-generation firewall (NGFW)	77	39	13	13	7
Net: Egress filtering	59	37	20	8	12
Net: Deception technologies such as honey potting	24	32	22	11	15
Net: Web proxy	65	37	16	6	7
Net: Network Access Control (NAC)	48	37	24	6	20
Net: NetFlow analysis	35	47	19	15	13
Net: Malware detonation device (inline malware destruction)	40	44	17	10	9
Net: Network intrusion detection system (IDS)/intrusion prevention system (IPS)	75	43	16	8	8
Net: SSL/TLS traffic inspection	45	53	17	9	13
Net: Ingress filtering	73	37	14	8	14

This table is continued on the next page. ▶

Table 1. Technology in Use per Deployment Phase *(Q23 n=166)* *(CONTINUED)*

Category: Question	Production (all systems)	Production (partial systems)	Implementing	Purchased not implemented	Planned
Analysis: Risk analysis and assessment	60	48	15	8	11
Analysis: SIEM (security information and event manager)	85	36	17	9	9
Analysis: Customized or tailored SIEM use-case monitoring	63	39	17	11	9
Analysis: AI or machine learning	29	41	26	9	15
Analysis: Frequency analysis for network connections	33	35	22	11	11
Analysis: External threat intelligence (for online precursors)	56	34	21	8	17
Analysis: Threat hunting	48	47	26	4	15
Analysis: Threat intelligence platform (TIP)	41	35	23	9	19
Analysis: Threat intelligence (open source, vendor provided)	58	44	17	9	13
Analysis: E-discovery (support legal requests for specific information collection)	50	47	17	7	13

Best and Worst

To identify what the implementation looks like, we asked respondents to give the technology a grade of A, B, C, D, or F. In a technique which some may not agree with, we then summed the As and Bs as positive and subtracted the Cs, Ds, and Fs. This gave a popularity-based assessment of satisfaction with the technology. You can see the positive and negative scores in Table 2. The short story is, our respondents love their next-gen firewalls the most and are most dissatisfied with deception technology.

Table 2. Technology Satisfaction Ratings per Type *(Q24 n=166)*

Category: Question	A	B	C	D	F	(A+B) – (C+D+F)
Host: Vulnerability remediation	30	52	38	8	6	30
Host: Malware protection system (MPS)	40	54	23	10	6	55
Host: Behavioral analysis and detection	34	45	32	5	14	28
Host: Data loss prevention	22	36	40	13	18	-13
Host: Ransomware prevention	37	48	28	8	10	39
Host: User behavior and entity monitoring	29	34	32	13	19	-1
Host: Endpoint or host-based detection and response	56	40	20	10	10	56
Host: Application whitelisting	26	25	29	20	31	-29
Host: Continuous monitoring and assessment	33	44	28	11	12	26
Log: Endpoint OS monitoring and logging	42	47	24	8	9	48
Log: Endpoint application log monitoring	32	41	30	11	12	20
Log: Log management	38	43	31	12	9	29
Log: DNS log monitoring	28	42	34	14	15	7

This table is continued on the next page. ▶

Table 2. Technology Satisfaction Ratings per Type *(Q24 n=166)* *(CONTINUED)*

Category: Question	A	B	C	D	F	(A+B) – (C+D+F)
Net: Network segmentation	40	37	29	14	12	22
Net: Email security (SWG and SEG)	48	45	21	11	8	53
Net: DNS security/DNS firewall	39	32	28	14	15	14
Net: Asset discovery and inventory	26	39	26	26	15	-2
Net: VPN (access protection and control)	49	49	20	11	7	60
Net: Full packet capture	25	31	33	11	25	-13
Net: Packet analysis (other than full PCAP)	26	39	31	12	20	2
Net: DoS and DDoS protection	31	45	25	12	14	25
Net: Network traffic monitoring	34	37	34	15	11	11
Net: Web application firewall (WAF)	32	48	29	9	13	29
Net: Next-generation firewall (NGFW)	52	45	22	6	7	62
Net: Egress filtering	35	40	27	8	16	24
Net: Deception technologies such as honey potting	24	18	41	12	31	-42
Net: Web proxy	34	31	32	14	17	2
Net: Network Access Control (NAC)	34	32	30	15	19	2
Net: NetFlow analysis	27	39	32	7	21	6
Net: Malware detonation device (inline malware destruction)	29	36	33	11	19	2
Net: Network intrusion detection system (IDS)/intrusion prevention system (IPS)	34	45	29	13	11	26
Net: SSL/TLS traffic inspection	30	38	35	15	13	5
Net: Ingress filtering	33	40	32	12	8	21
Analysis: Risk analysis and assessment	31	36	34	13	10	10
Analysis: SIEM (security information and event manager)	39	43	24	15	13	30
Analysis: Customized or tailored SIEM use-case monitoring	38	34	27	16	15	14
Analysis: AI or machine learning	18	30	33	21	23	-29
Analysis: Frequency analysis for network connections	20	31	37	14	21	-21
Analysis: External threat intelligence (for online precursors)	28	34	37	13	18	-6
Analysis: Threat hunting	28	36	38	11	16	-1
Analysis: Threat intelligence platform (TIP)	22	30	40	11	21	-20
Analysis: Threat intelligence (open source, vendor provided)	27	41	34	11	14	9
Analysis: E-discovery (support legal requests for specific information collection)	23	36	36	12	13	-2

Further Thoughts on Technology

We spent time looking at the grades and the varying degrees of implementation. Then we assessed whether technology gets a higher grade at the planning phase than if it is fully implemented. We selected the SIEM as a deep-dive technology for the next analysis. It is among the top five technologies deployed and has a highly positive score, but it isn't the most positive score, having been beaten by the next-gen firewall and EDR. (Look back at Tables 1 and 2 to compare these three items.) By looking at satisfaction by phase, we see that the SOCs that indicated they had fully implemented across all systems were more likely to rate the product with an A grade *(n=42)* than a B grade *(n=28)*. But that was reversed in production if the SIEM was only partially implemented—only 7 A grades *(n=7)* to 42 B grades *(n=42)*. Figure 19 shows these results in a chart. A clear takeaway: If you want to be most satisfied with your SIEM, finish the implementation to full coverage.

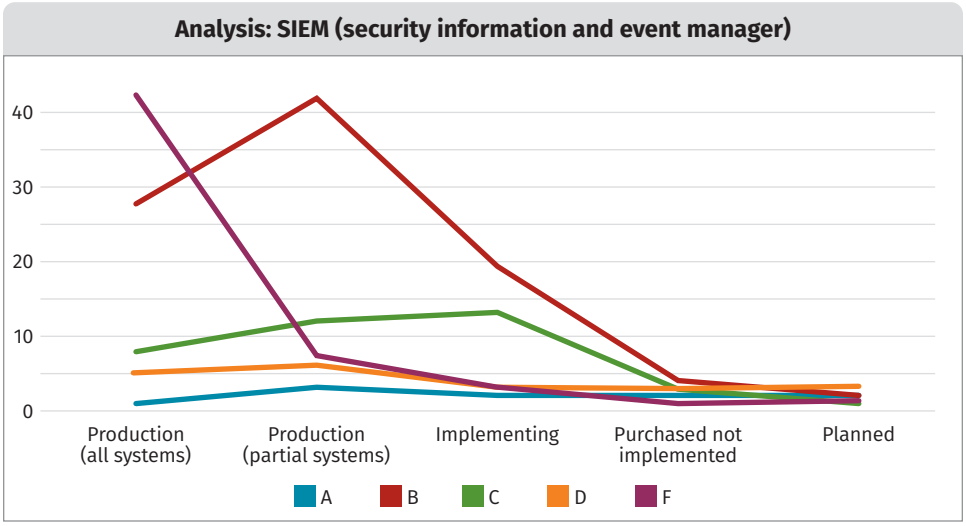


Figure 19. SIEM Phase and Grade (Q23 and Q24 n=216)

The Rest

"The cloud" is an oft-repeated term. Because we presume most SOCs take a trust-but-verify stance for resources they're protecting and outsourcing, we asked: **What are you using to monitor your mobile devices, extranet, and cloud partner (AWS, Azure, etc.) resources?** ***Select all that apply.*** *(Q25)* In Figure 20, we see that MDM is the most common response by far. Maybe the bucket of mobile devices and cloud devices is too encompassing. We think this is a technology problem for many organizations because they're not sure how to adapt to the new reality of *the extranet*, or assets outside of the traditional perimeter.

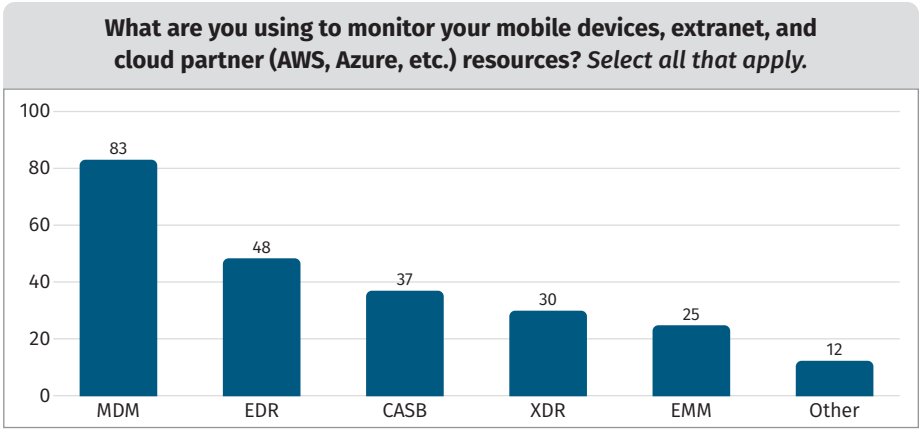


Figure 20. External Resources Monitoring Technology (Q25 n=139)

Visibility is important for cybersecurity analysis, yet encryption of network communications has increased steadily in the last several years. We asked how SOCs were peering inside of the encrypted connections: **How are you using TLS interception to review HTTPS and other encrypted communication?** *(Q31)* This capability provides insight for analysts at the cost of potential reduction in personal privacy. So, it's frustrating to see that people have implemented it but aren't doing anything with it. Next year the SOC Survey plans to ask how SOCs are replacing DNS logging with DNS over HTTPS and DNS over TLS logging. See Figure 21.

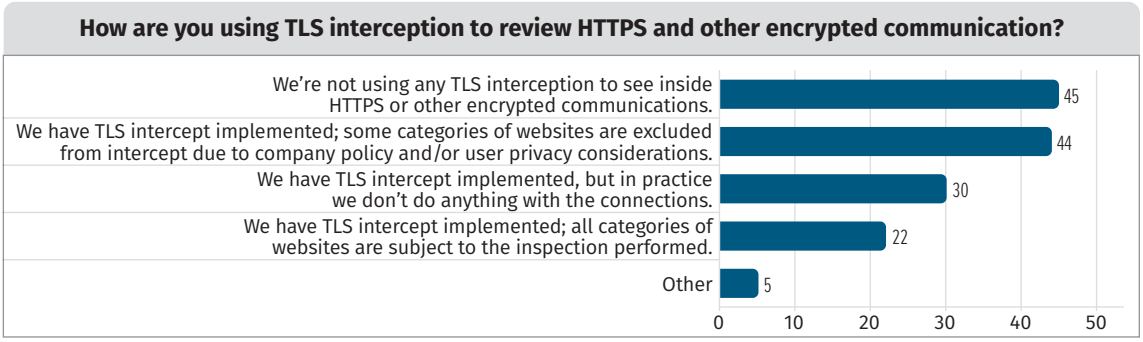


Figure 21. TLS Interception Implementation Descriptions (Q31 n=146)

In our follow-on questioning, we heard that the most common reason for not using TLS intercept is corporate concern over regulations and privacy. However, no one using TLS intercept reported running into legal issues. One respondent pointed out the need for management education in this area. On the technology side, however, performance issues with inline TLS decryption were mentioned.

SOC Funding

Financial Considerations

A question often posed is how to assess the right level of funding for the SOC. A method for calculation we offer is to look at costs per record as a start of a more complicated loss prevention calculation. To see how many are implementing something along this line, we asked: **Have you calculated a "cost per record" from an actual incident?** *(Q39)* Of the 130 respondents, 42 (32%) said yes. Candidly, that's higher than expected. There were 67 "No" responses, and 21 survey takers indicated that they do not know if cost per record is calculated.

The survey also inquired about a more complicated dimension of the challenge: **Do you have an estimated or calculated "incident with a SOC vs. incident without a SOC" value?** *(Q40)* We asked to see whether there was a calculation in use that allowed for determining the loss prevention value of the SOC. Inured to the difficulty of deploying this operationally, we were not surprised to see that 9 of the 130 who answered the question (7%) said "Yes" as to whether there was an estimated or calculated "incident with a SOC vs. incident without a SOC" value? To that question, 27 answered that they did not know, and 94 of the survey takers (72%) selected "No."

Speculating loss prevented is complicated and involved. One method is to assign estimated figures for each phase of intrusion along the ATT&CK phases. If you have actual numbers based on calculation of loss incurred, use them. The next best option is using industry averages for loss incurred. Estimates of loss that would occur are the last option. You'll produce excessive numbers if you multiply all the firewall blocks and phishing messages dropped prior to delivery. A very complicated scheme for calculation would use adjusted values along the ATT&CK phases.

SOC Funding

We asked respondents several questions about how they deal with funding the SOC within their organization. Here, we'll focus on two questions, the first of which asked: **Does management in your organization consult SOC leads/managers to discuss funding levels and deficiencies in the environment?** *(Q51)* Figure 22 shows that 65% (84 of 130 responses) say the funding is discussed with the SOC's management.

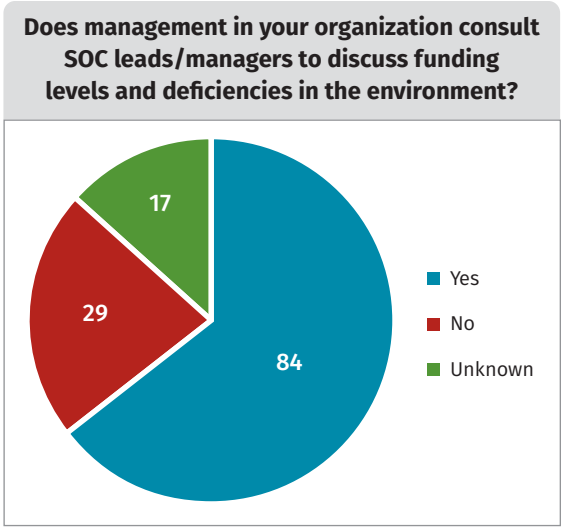


Figure 22. Funding Levels for SOC Addressed (Q51 n=130)

Of course, funding is a complicated and sensitive topic. There were several other ways we asked about this, including a free format response to describe the way this is addressed. We asked for open text answers in the next question: **Do you provide metrics to your senior management to justify requests for increased funding for resources for cybersecurity? If so, how do you approach budgetary concerns when it comes time to discuss funding for the next year?** *(Q52)* Several comments echoed the frustration one survey taker stated, "I do provide metrics, they are summarily dismissed or disregarded entirely. We will need a full disaster here to get their attention."

SOC Deployment Strategies, Architecture, and Coverage

IT/OT

General-purpose compute systems are usually deployed to perform business processes. We often call this *information technology (IT)*. Physical processes are usually managed by more specialized deployments, often referred to as *operational technology (OT)*. We wanted to determine whether there was a blending of IT monitoring with OT monitoring, so we asked: **Are you monitoring your OT (operations technologies) systems separately or with IT SOC resources? Select the best option.** *(Q17)* Of the 214 respondents, 64 indicated that this isn't a concern because there's no OT to monitor. Seventy-five people indicated that they use the same SOC systems, blending IT and OT resources, whereas 45 said it is totally separate. The remaining 29 respondents said that they use separate monitoring technology but the same staff to look after it. See Figure 23.

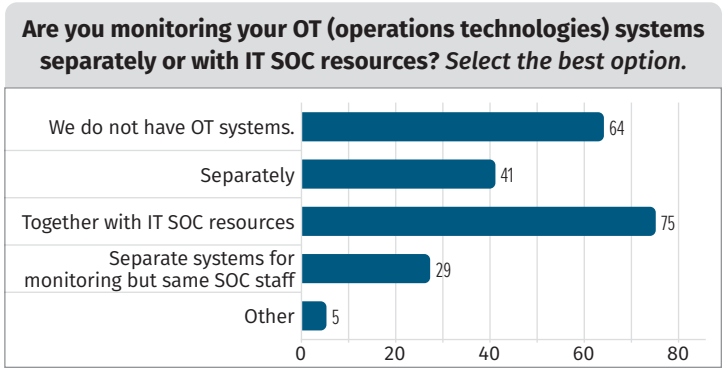


Figure 23. OT/IT Strategy (Q17 n=214)

There's something distinct in OT from many other information systems in use. OT is an operationally focused capability, and there are usually tangible work products that can be observed or inspected for verification that the operations are proceeding. This is a mixed advantage. If there are experts who are monitoring the operational capability, they can quickly detect erroneous values or diminished information system performance with a cross-reference to expected physical properties. On the other hand, if experts aren't available for that cross-reference, serious damage might occur before the problem is noticed.

SOC/IT Administration

There is usually separation of duties between the administration of the information systems (we no longer preserved an IT/OT distinction for Question 8) and the management of security of those systems. In Question 8 we asked: **What is your SOC's relationship to your network operations center (NOC)?** Not surprisingly, there is a dearth of integration between these teams. Of the 280 respondents to this question, 85 (30%) of them indicated that interaction takes place only during emergencies, compared to 54 (19%) who indicated that there is strong integration between the teams. See Figure 24.

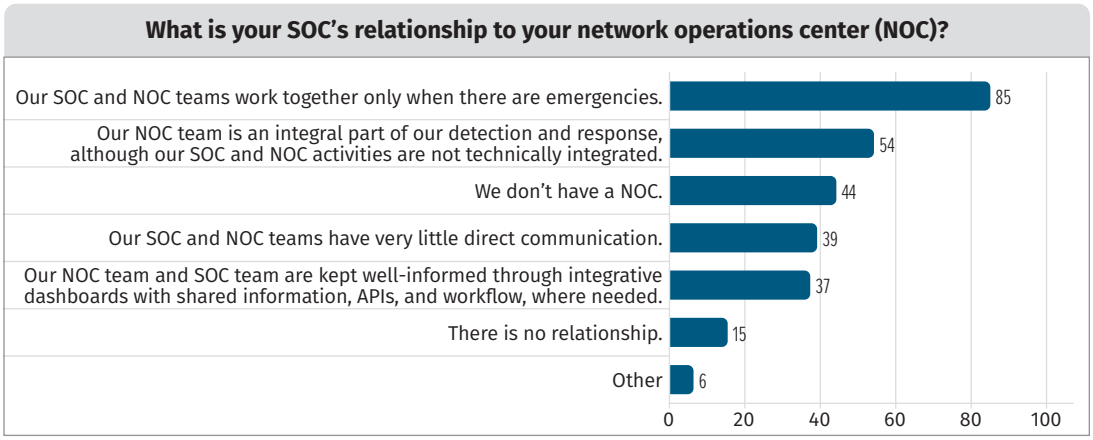


Figure 24. SOC/NOC Relationship (Q8 n=280)

Surprisingly, the top two detailed responses from our follow-up messaging were: "We don't have a formal NOC" and "Our NOC and SOC do work together very well." All the responses in-between highlighted that network operation and security operation priorities were very different and integrating them would require management and organizational changes.

IoT Approach

OT comprises the industrial systems that control physical operations such as assembly lines and refineries. But there's an additional class of systems known as the *internet of things (IoT)*. These systems are networked devices that traditionally have some durable goods type of role but are now enhanced with IP-based networking to provide monitoring and control. Examples include thermostats, lights, refrigerators, and dishwashers. But the uniquity of these networked devices is extended through mesh networks for Bluetooth and Zigbee, designed for low-power, short-range-proximity communications, but may ultimately link to an internet-connected control point.

We asked about this IoT approach: **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?** *(Q16)* The short version of this is that most SOCs aren't fully monitoring these systems, haven't considered it, or have considered it and dismissed it. Only 50 of the 220 respondents said that they support all the at-risk smart systems. See Figure 25.

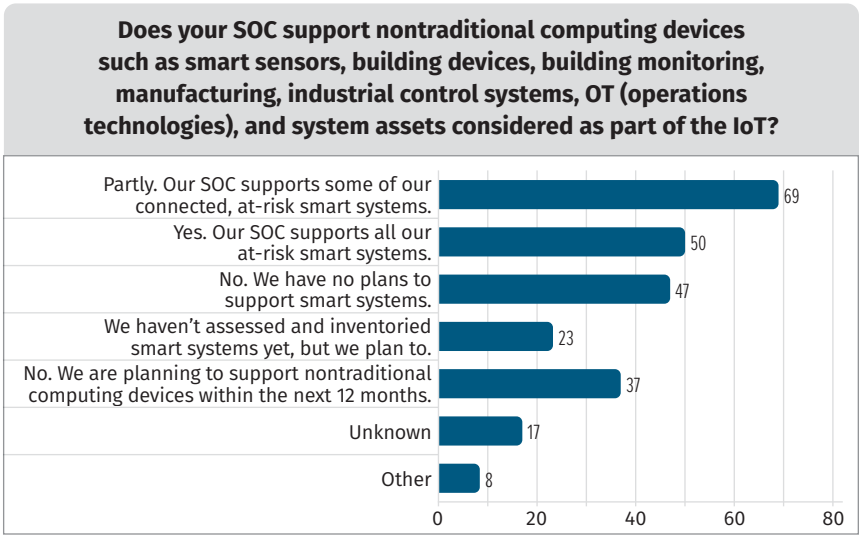


Figure 25. Support of IoT (Q16 n=220)

IoT then becomes a potential soft target for persistence and durable access. It's not usually the initial point of entry, but the recent high-visibility supply chain attacks may compel attackers to attempt to piggyback into the network over a third-party software or hardware provider. For example, how would the SOC know if the HVAC system is supposed to connect to a server every month or so? We envision a scenario where the initial installation has a firewall in place to protect the furnace (or any other IoT device) and eventually a persistent rogue device figures out a way to tunnel network connections out.

Architecture

There are many techniques for arranging a SOC to cover the systems deployed. In discussing deployment, we felt it appropriate to ask how the SOC is arranged: **How is your SOC infrastructure (i.e., your SOC architecture) deployed today, and how might it change over the next 12 months? Select the best choice for each. If you select the same answer for Present and Future, SANS will assume no change.** *(Q6)* We also asked what the plans were for changing. Note that in Figure 26 the current/next twelve months don't necessarily mean that the person who responded selected the same answer. They're simply counts. As expected, the single, central SOC dominates with 84 responses (31%) of the current deployments. However, the trend to cloud-based SOC in the next 12 months, with 65 responses (24% compared to its current 35 responses of 13%), must be acknowledged as an obvious continued march to the cloud, hastened by IT changes in response to COVID-19 and more people working from home.

How is your SOC infrastructure (i.e., your SOC architecture) deployed today, and how might it change over the next 12 months? Select the best choice for each. If you select the same answer for Present and Future, SANS will assume no change.

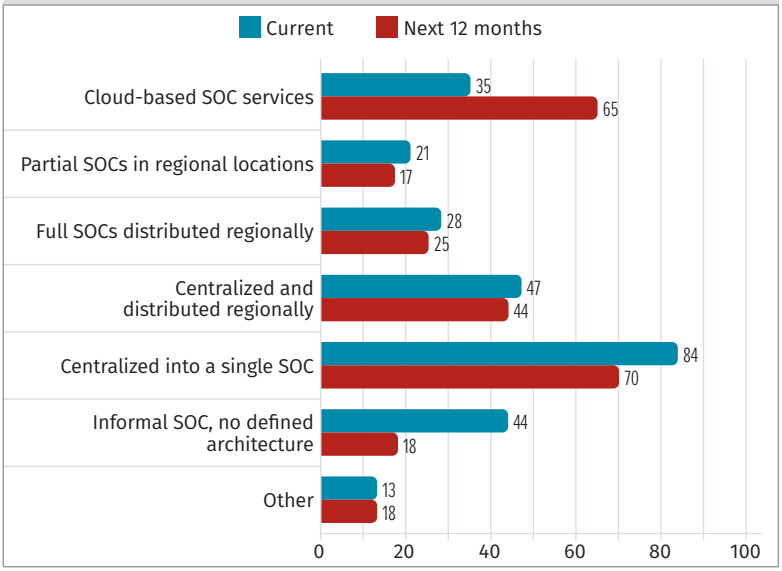


Figure 26. SOC Infrastructure Today and One Year from Now (Q6 n=272/266 current/future)

2021 SOC Survey Response Dataset and Analysis

The unanswered question of who's changing to what is buried in the data of the responses. Starting with the 2020 SOC Survey, SANS released the full dataset, and this year we continue that trend. There will be follow-on releases of analysis capability in the form of a Jupyter notebook and instructional guidance for analysis from the SOC Survey's author, Christopher Crowley.

We're optimistic that by releasing the data from the survey, there will be additional community analysis performed by and shared with the cybersecurity community. We do this to help everyone SOC better. We'd like you to be able to investigate and answer additional questions you might have. We have shared a de-identified version of dataset at https://soc-survey.com/2021 so that you can access this resource. If you perform analysis and would like to add it to the repository for others to see, contact Chris Crowley, the author of the paper (soc@montance.com).

If you perform some analysis with the response dataset we shared, please provide a link so that we can share it with the community.

Survey Challenges and Summary

Throughout this report we have elaborated on several SOC-related topics. Here, we'd like to end by repeating several key findings to keep in mind as you move forward:

- Metrics help in understanding and communicating the performance of the SOC. In the question about metrics *(Q33)*, a large portion *(77%, n=111)* of respondents indicated that, yes, they do provide metrics. This is an increase from the equivalent question in the 2020 Survey, where 70% responded yes.
- The most commonly reported SOC size (not adjusted for organization size) was 2 to 10 people *(44 responses to Question 42)*.
- In the work-from-home question *(Q13)*, 87% *(210 of 241 responses)* said work from home is allowed. We're looking forward to finding out from the 2022 Survey results if this change is here to stay.
- Other interesting data elements include the occurrence of incidents or intrusions. The responses are distributed among yes (33%), no (40%), don't know (12%), and decline to answer (16%), per Question 3. A large portion of the SOC-protected organizations are not experiencing serious issues.
- The solutions most desperately needed (Question 55: "What is the greatest challenge (barrier) with regard to full utilization of your SOC capabilities by the entire organization?") are to have skilled staff *(24 responses)* and automation *(23 responses)*. To help you address this challenge, we formulated an opinion by synthesizing the responses from multiple questions and follow-up conversations: metrics *(Q33/Q34)*, staff retention *(Q45)*, SOC funding *(Q51)*, tech satisfaction *(Q23/Q24)*, and work from home *(Q13)*. It is our opinion that the pathway to high performance is to automate metrics, complete the implementation of the technology you buy, develop an ongoing program for moving repetitive tasks into automation technology, and promote ongoing analytical excellence and technical mastery in the SOC staff. That mastery and excellence will come from training and programmatic peer review of work.

If you read this report and found it valuable, we're happy to hear that. If you work in or manage a SOC and can contribute to the response set in the future, please do so! Also, we offer a final "thank you" to those who contributed this year!

About the Authors

Christopher Crowley

Christopher Crowley, a SANS Senior Instructor, has 15 years of industry experience managing and securing networks. He has authored numerous courses and is considered a leading expert in building an effective SOC. He currently works as an independent consultant in the Washington, DC area focusing on effective computer network defense. His work experience includes penetration testing, security operations, incident response, and forensic analysis.

John Pescatore

John Pescatore joined SANS as DIrector of Emerging Security Trends in January 2013 with 35 years of experience in computer, network and information security. He was Gartner's Lead Security Analyst for 13 years, working with global 5000 corporations and major technology and service providers. Prior to joining Gartner Inc. in 1999, Pescatore was Senior Consultant for Entrust Technologies and Trusted Information Systems. Prior to that, Pescatore spent 11 years with GTE developing secure computing systems. Pescatore began his career at the National Security Agency, where he designed secure voice systems and at the United States Secret Service, where he developed secure communications and surveillance systems. He holds a BSEE from the University of Connecticut and is an NSA Certified Cryptologic Engineer.

Sponsors

SANS would like to thank this paper's sponsors:

ANOMALI®
ARCTIC WOLF
cisco Cisco Umbrella
CyberProof® A UST Global Company
ExtraHop
Infoblox NEXT LEVEL NETWORKING
paloalto® NETWORKS
Siemplify
sumo logic | aws
THREATQUOTIENT