



Research  
Program

## Survey

# SANS 2024 SOC Survey: Facing Top Challenges in Security Operations

Written by Christopher Crowley

May 2024

Abnormal

ANOMALI



CARDINALOPS



The bridge to possible

corelight

Dropzone AI

Google Cloud

infoblox

paloalto  
NETWORKS

RadiantSecurity

SWIMLANE

torq

©2024 SANS™ Institute

# Executive Summary

As we've seen in the past, security operations centers (SOCs) are a core component of an organization's cybersecurity practice. We're exploring what a SOC is, and hope that you use this survey to recalibrate your near term and longer-term plans. In the author's experience many organizations are currently looking for a basis to compare the SOC's performance with other SOC's. This includes capabilities, budget, staffing, and challenges. All of these are covered in this report.

In addition to the details covered here, there are a multitude of additional items we simply don't have space to address. To help you help yourself, the de-identified responses and a Jupyter notebook are available for you to do some additional analysis at: <https://soc-survey.com>.

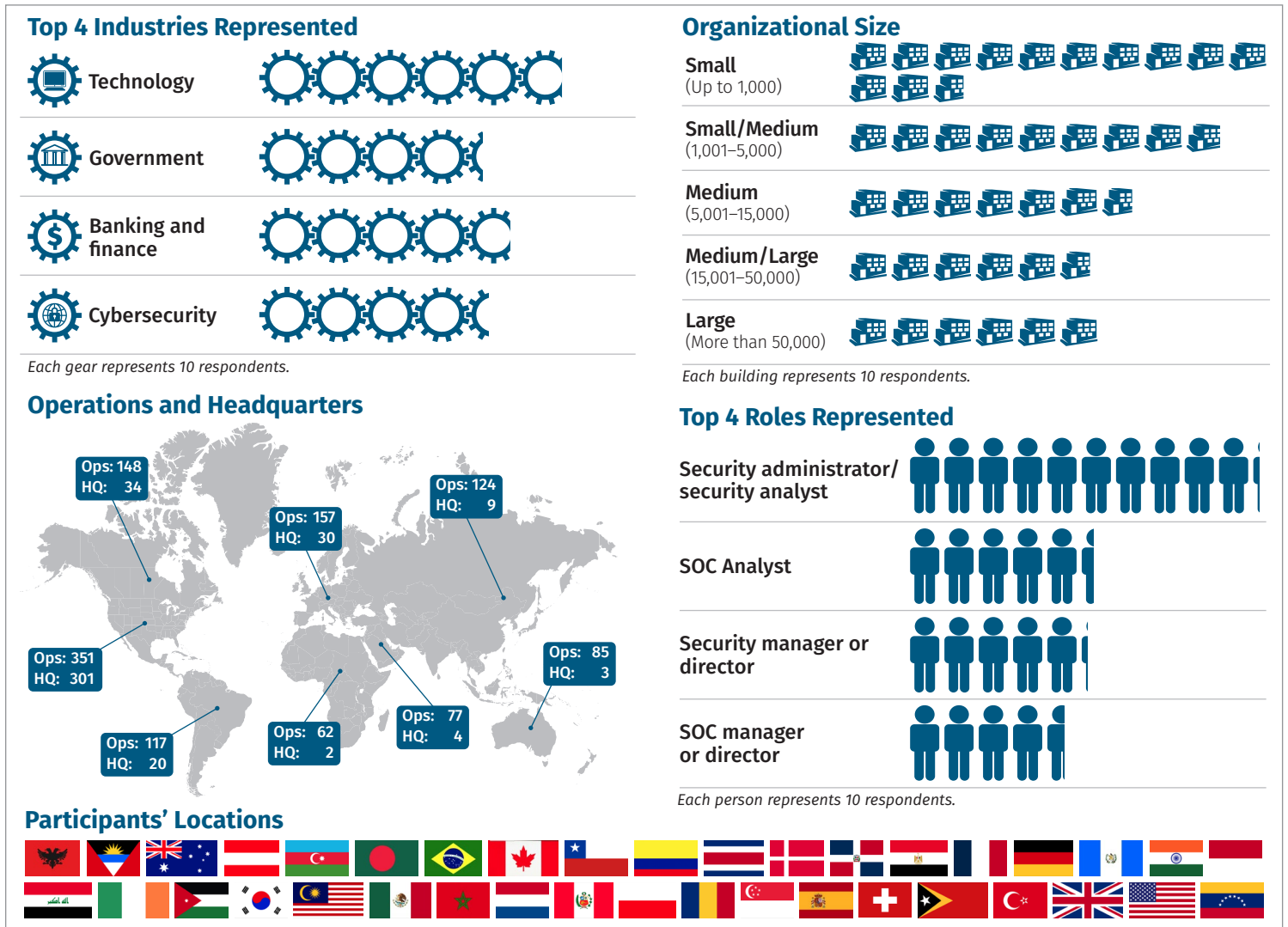


Figure 1. Survey Demographics

Figure 1 is dense with information. Some of the items expressed in it are that the top sectors represented by respondents were Technology, Government, Banking and finance, Cybersecurity, and Education. The respondents were a mix of technical and managerial: the top responses were: Security administrator/Security analyst, SOC Analyst, Security manager or director, and SOC manager or director. 334 out of 403 respondents were headquartered in North America, 301 of those were based in the United States of America. But there were responses from companies headquartered around the globe, including: Europe, Latin or South America, Asia, Middle East, Australia/New Zealand, and Africa.

What's your budget? "Unknown" is by far the most common response, answered by 151 people. This seems odd. It is the author's opinion that it is a result of a fundamental misalignment between the SOC staff/management and the organizational budget process. The author's interpretation of this response and others is that the SOC is misaligned with the organization it is intended to protect.

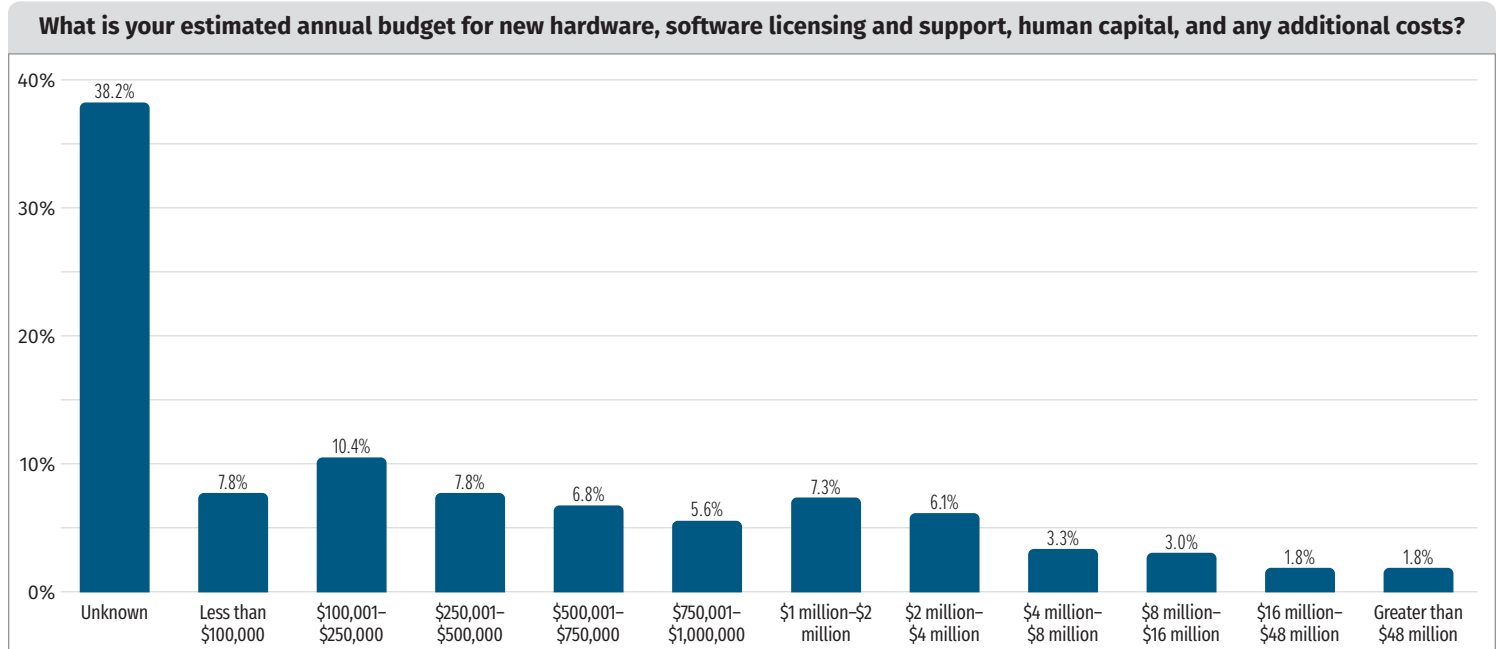


Figure 2. SOC Budget

You're reading this report to understand how it is going in other people's SOC's. To provide a consistent basis of comparison, we frequently use metrics. The survey asked if metrics are reported. 260 of 384 responses to Q3.77 said they provide metrics to senior management to justify resources for the SOC, representing 67% of the responses.

This is a relatively small increase from 2023 where 66% said they did the same. Both these last two years, however, are a fairly substantial drop from 2022 where 74% reported using metrics to senior management for justifying SOC resources. Prior to 2022, we asked the question as an open-ended response so the percentages aren't available.

What might cause such a change? We can only speculate—maybe a more mature approach to metrics. Regardless, we'll dig into specifics of metrics in a later section.

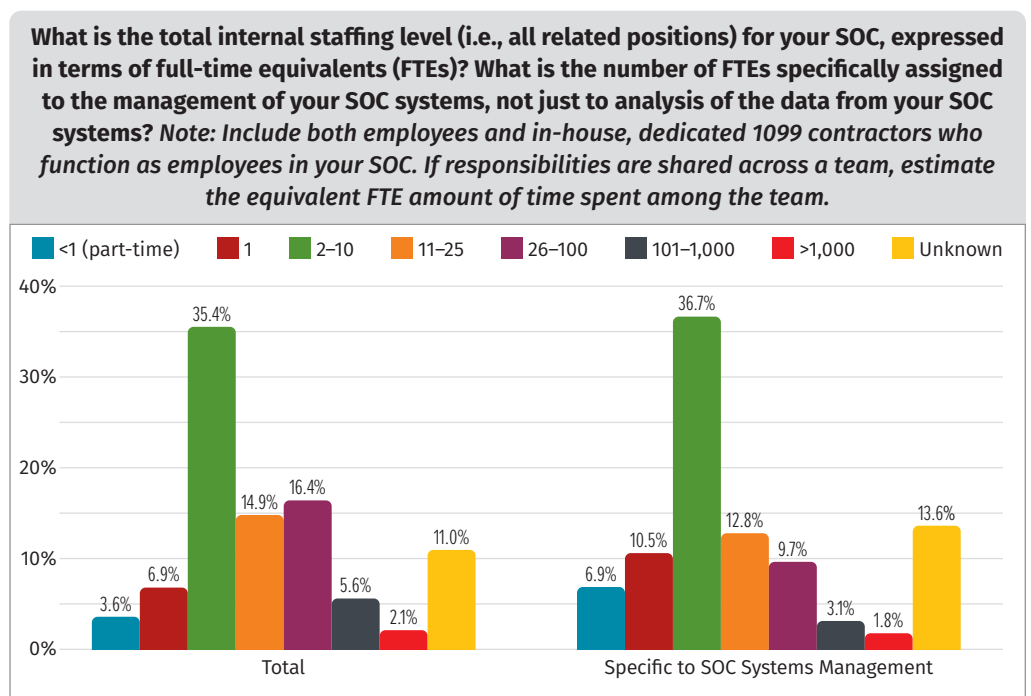


Figure 3. SOC Staffing

“How many people work in your SOC?” The figure for question Q3.61 shows that most respondents report 2–10 people. In a later section, we’ll dissect this into industry, organization size, and outsourcing. This has been the most common answer since the inception of the SOC survey in 2017. So, it’s no surprise that it is the same this year.

“What’s your biggest barrier in the SOC currently?” Lack of automation and orchestration is the single highest answer with 71 responses out of 388. But combining the next two answers which are directly related—“high staffing requirements” and “lack of skilled staff” (56+55=111) we see that staffing represents the greatest barrier. The third issue commonly cited is a lack of enterprise-wide visibility, with 50 responses.

“How does the SOC know there’s a problem?” EDR/XDR is the highest reported initial trigger for incident response by the SOC team in question Q3.32. The SIEM, user reports, other anomalous activity, and third-party intelligence represent the items that received over 200 responses out of 394 respondents to this “select all that apply” question. We’ll update the answer options in 2024, because “anomalous activity” doesn’t get to the heart of the question we asked, “How does the SOC know there’s a problem?”

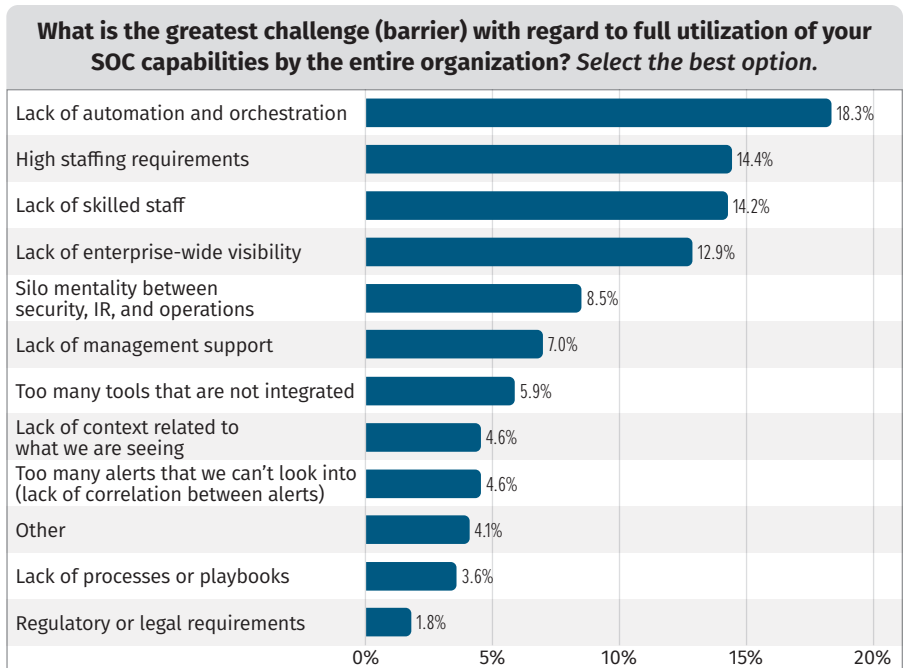


Figure 4. SOC Automation

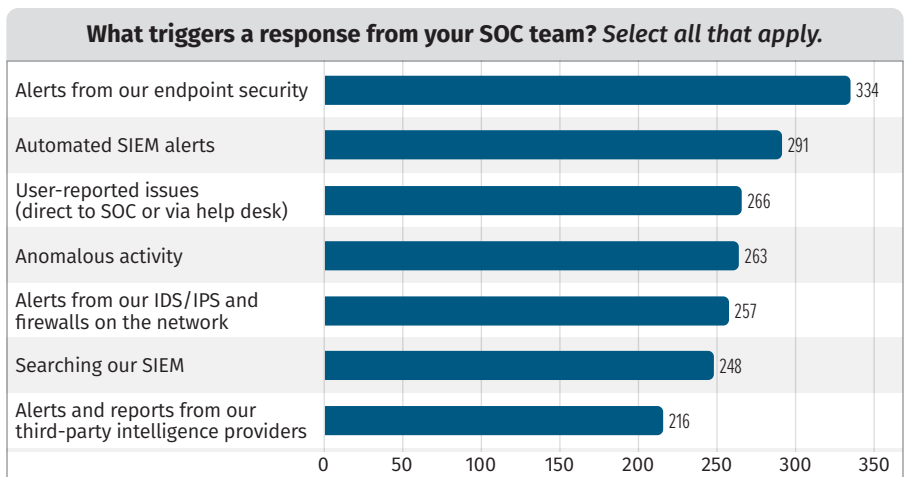


Figure 5. Response Triggers

## Commentary on Trend Analysis of Responses

An important note about identified change and consistency trends in the next sections is that we can’t guarantee the same population responds year over year. We don’t vet the identity of the respondent. Nonetheless, polling provides a reasonable insight into the state of things in the world. One way to measure quality of the respondents is how long people spent answering this extremely long survey! The mean time was 52 minutes and the median time was 33 minutes with a Qualtrics projected time to complete of 36 minutes. In fact, people frequently tell the author of the survey that answering the questions has substantial value as a thought exercise!

# Highlights of Changes and Trends in SOC Survey Responses

**Section Summary:** Changes: Cloud-based is new top structure; everything goes in SIEM is more common; single, central SOC is more common; vendor-tool based threat hunting is more common; fewer are planning on deploying AI/ML; people express lower grade for AI/ML than last year; TLS inspection is decreasing; employee duration of employment is increasing; career progression is more important for retention.

We hope you've been reading the SOC Survey since it was first created in 2017. Since you might not remember the charts from last year, let's look at a few things that changed from previous years.

## Cloud-Based Architecture

The first one we'll explore is a big one. That "cloud based" now exceed "single central" SOC as the most common architecture. The trend of moving to the cloud has been observed in IT for years and is now embedded in SOC architecture.

## SIEM Everything

We asked how people deal with the massive volume of data, and they seem to be exerting less effort filtering things and instead are dumping everything into the SIEM. This may seem counter-intuitive, but it may be more economical than exerting lots of engineering effort to figure out what is actually needed before collecting it. See Figure 6 for the answer of the question, "What is the primary approach you use to decide what data to ingest into your SOC?"

This represents an increase from 2023 when the percentage was 29% of 600 answers, this year it's 38% of 403 answers for the same question. We didn't ask the question prior to 2023.

## Single Central Architecture Greater Ratio

There are a few ways to build out your SOC. Having a single, centralized SOC is the most common way to do it, as shown in Figure 7 for 242 out of 403 or 60% of respondents. An increase from 2023 at 49% and 2022 when 53% answered single, central SOC.

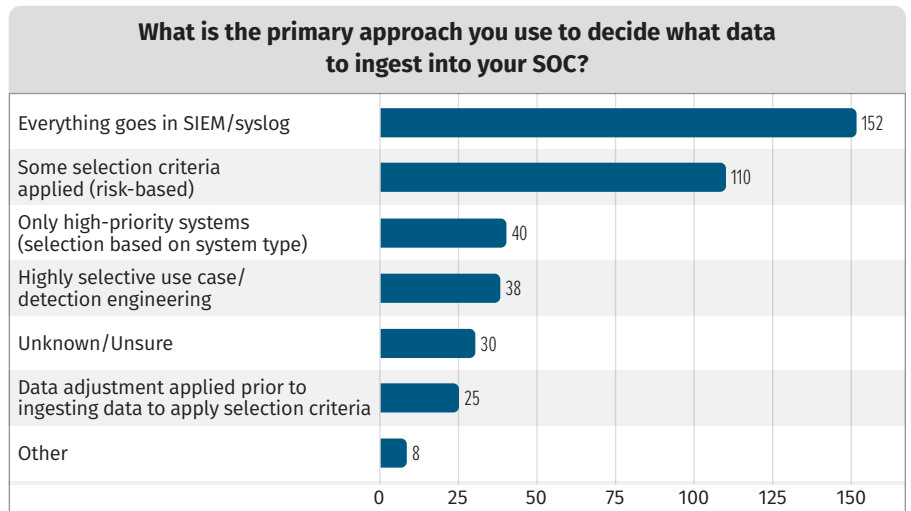


Figure 6. SOC SIEM

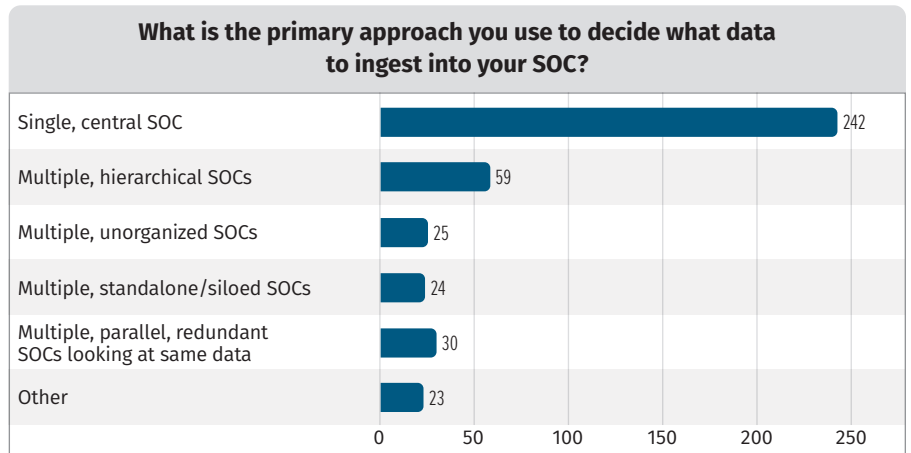


Figure 7. SOC Architecture

## Vendor Threat hunting automation on rise

Threat hunting has a primary objective of looking for compromise which wasn't detected by our alerting systems. One important but simple approach to this is applying newly discovered indicators to historical data repositories.

We asked if threat hunting activities were automated, and 179 out of 388 responses indicated they are at least partially automated using vendor provided tools, as visualized by figure hunting automation.

Last year, only 38% of 457 responses indicated the same "partially automated with vendor tools" response compared to this year's 46%.

It's the author's opinion that retroactive analysis using updated IOCs is just the bare minimum hunting and real hunting entails thoughtful seeking of the previously undiscovered. Our advice, keep automating the retroactive analysis, and strive to do sophisticated hunting.

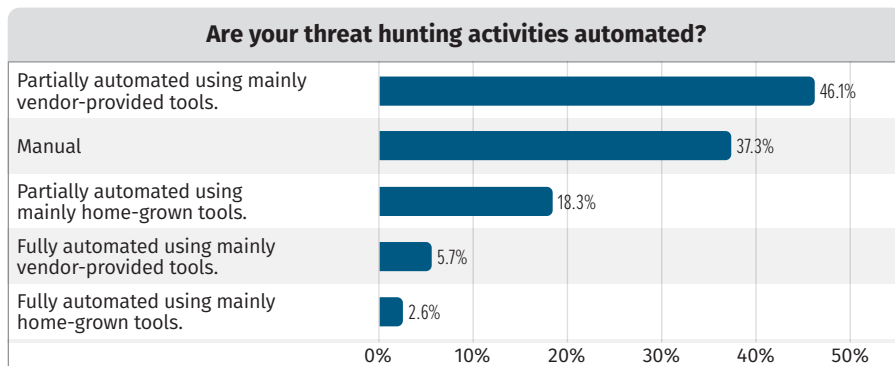


Figure 8. Hunting Automation

## AI/ML Tech and Satisfaction

Last year we quickly added AI/ML to our technology satisfaction list, and it was unsurprisingly at the very bottom. We'll show you the overall grade-based comparison again this year in a later section. But, let's look at some of the technology changes from 2023 to 2024.

From 2023 to 2024, the percentages of full or partial production or in the midst of implementing didn't change much. But look at the drop in planned implementations from 2023 when 21% said it was planned to 2024 when 11% said it is planned. From this picture it looks like the people who were going to do it have already done it, and the rest have decided to pass.

The other thought to explore is if people are having buyers' remorse. We provide a GPA based grading each year. In 2023 "Analysis: AI or machine learning" got a GPA of 2.17, beating only network packet analysis which scored the lowest GPA of 2.15. How did it do in 2024? It came in 2nd to last again, but with a lower GPA of 1.99.

We considered that the drop was due to respondents being harder graders in 2024. But there was a higher high than last year: EXDR kept the top spot. It got a 2.88 in 2023, and a 3.13 in 2024. So, our interpretation is Cybersecurity staff are more unhappy with AI/ML in 2024 than in 2023.

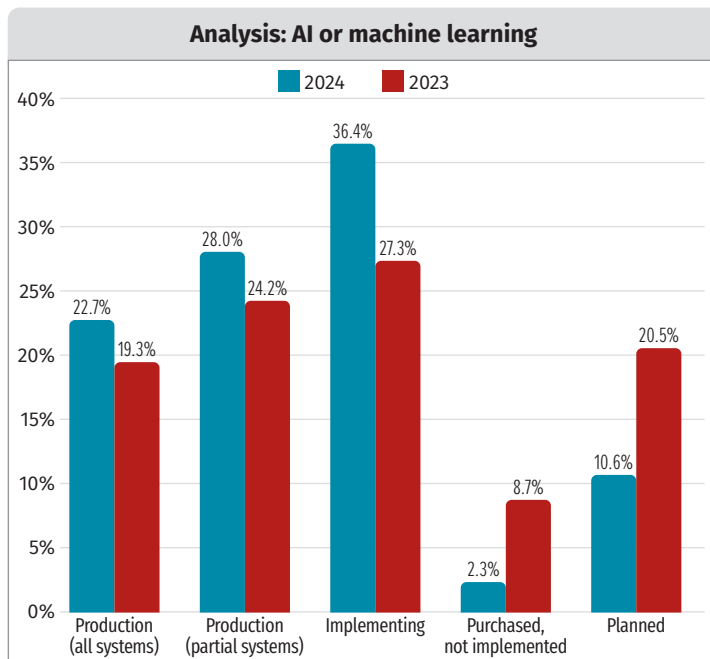


Figure 9. AI Implementation

But, the new lowest was a new addition to our list of technology. Are you ready for the new lowest? Making its debut at the bottom of the list is "Analysis: AI or machine learning-Generative (GPT)" at a GPA of 1.80. Let's look at it again in 2025. In 2025 we plan to have a more detailed list of AI/ML technology options because the products are proliferating.

## TLS Intercept

TLS intercept address blindness, or lack of visibility into data. With applaudable privacy advances come reduced enterprise visibility into network traffic. One approach to this is providing transport layer security (TLS) intercept technology to peer into encrypted communication. This is becoming harder to do, and the 2024 responses indicated a slight decrease from 2023.

In 2024 34% indicated “We’re not using any TLS interception to see inside HTTPS or other encrypted communications” whereas in 2023 only 25% indicated the same. In 2023 38% indicated “We have TLS intercept implemented, some categories of websites are excluded from intercept due to company policy and/or user privacy considerations.” In 2024 that percentage dropped to 34%.

SOCs are losing visibility into the traffic leaving the network, which likely means more reliance on the endpoint protection tools.

## Average Tenure Increasing

Staffing is always a concern for the SOC. It takes skilled analysts to perform well under high pressure for a long time. So, retention is a perennial challenge. The survey asks how long the average tenure is, and slightly longer tenures of three to five years are just barely eclipsing one to three-year tenures, but this is a positive trend for long term career-oriented staff and organizations looking to minimize the cost and uncertainty of constantly hiring and retraining. See Figure 10 depicting this inflection. We’ll keep an eye on it for 2025.

## Retention

What has been compelling people to stay? The survey asks how to retain employees. We don’t cover macro-economic conditions, but those could also play a factor. See Figure 11 to see that meaningful work took the top spot this year, but the reported differences have reduced.

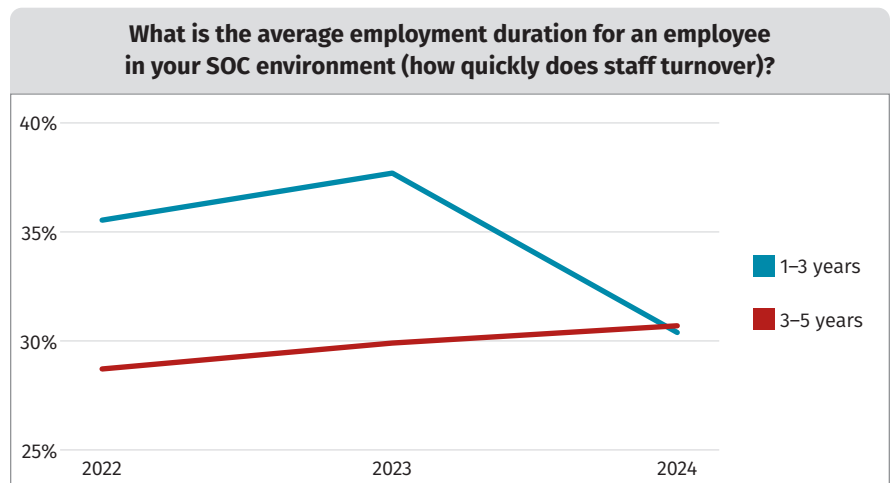


Figure 10. Employment Duration

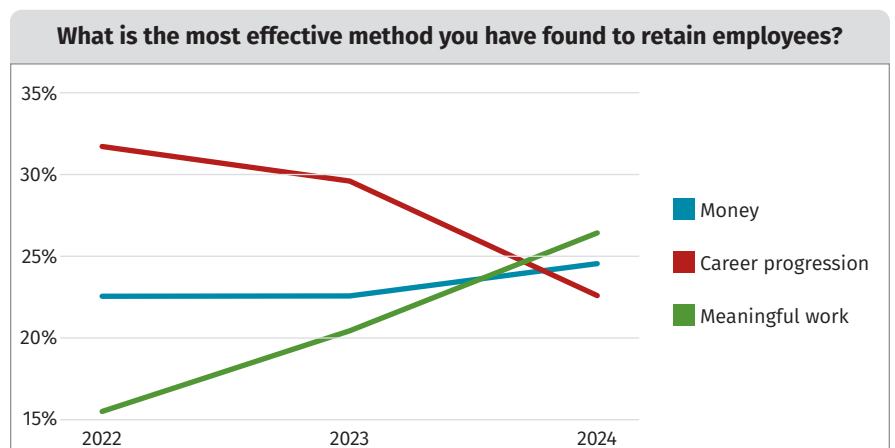


Figure 11. Retention

## More of the Same

**Section Summary:** Same old story: internal SOC is mandatory; NOC and SOC are not integrated but coordinate.

We've explored some of the changes observed for the past couple of years. What seems to be consistent?

### Internal SOC Mandatory

For one thing, most of the time use of the SOC is not an option, and this is consistent with all the years we've run the survey.

Q3.2 asked if internal SOC use was mandatory. Figure 12 indicates that the spread has changed slightly but the ratios are about the same with no major movement.

The NOC and SOC have about the same relationship year over year, as shown in Figure 13.

Next we deep dive into some other questions in the survey, leaving behind the year over year comparisons.

**Within your organization, is use of the internal SOC viewed as mandatory or is it acceptable for members of your organization to acquire services from external parties/providers?**

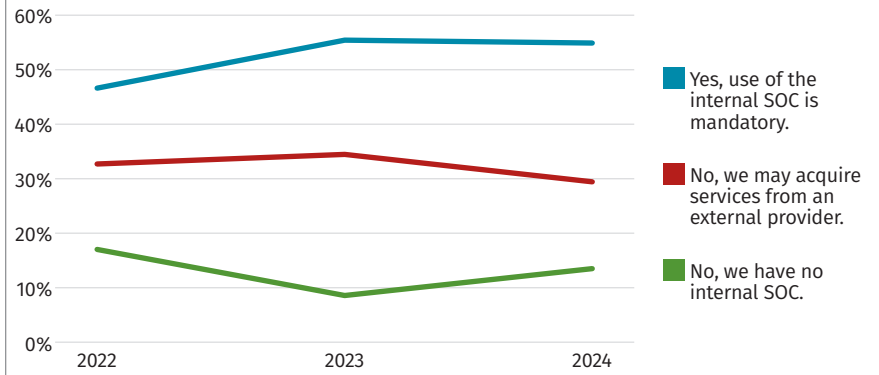


Figure 12. SOC Mandatory

**What resources does your organization utilize to collect malware samples and/or perform malware analysis?**

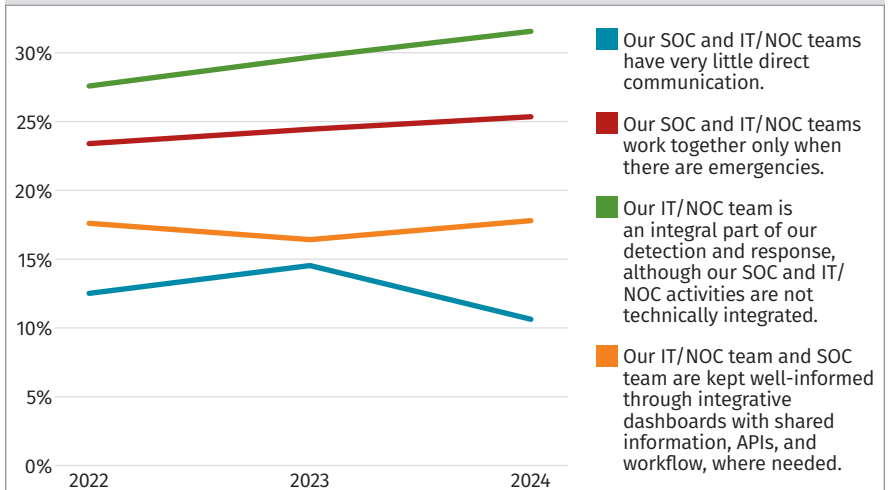


Figure 13. NOC/SOC Relation



# SOC Technology

**Section Summary:** 47 listed technologies graded; EXDR is top GPA technology still; AI/ML is lowest.

Since 2020, we've taken a GPA approach to the depiction of technology satisfaction. Surprise, this year one technology received an A! Barely in the A range of 3.1, EXDR tops the list. Figure 9 has the full list. It's worth noting that AI/ML occupy the bottom two spots in satisfaction. We added AI/ML Generative Transformer this year, since ChatGPT has captured the public imagination since Generative Pretrained Transformer (GPT) version 3 started spouting useful stuff. SOC staff don't seem impressed yet.

Figure 14 ranks the technology list by deployment phase and shows the corresponding GPA of that technology.

Another interesting way to look at this is to rank technology based on the top of each category. Let's take each in turn.

Production (all systems) has a top product of "Net: Email security (SWG and SEG)" with 111 out of 161 overall responses. This mature technology is easy to accomplish full coverage and is so commonplace and necessary that email would be unusable without it. Plus, it would likely be criminally negligent to run an email server with no filtering in place. Or maybe criminally profitable, but offering bulletproof hosting and no-trace mail servers is the other side of the cyber industry.

Production (partial systems) top technology is Analysis: Threat hunting with 61 responses. This is aligned with the aforementioned increase in threat hunting being driven by third party provided hunting tools. This is easy to deploy into production, but a challenge to accomplish full coverage because of visibility issues. These issues may stem from inadequate authorization or mandate. But it may also simply be a challenge to provide effective hunting across all systems. It's trivial to say, go look for a hash on a computer. Doing so across tens of thousands of globally deployed systems on commodity internet with varying bandwidth becomes a substantial challenge.

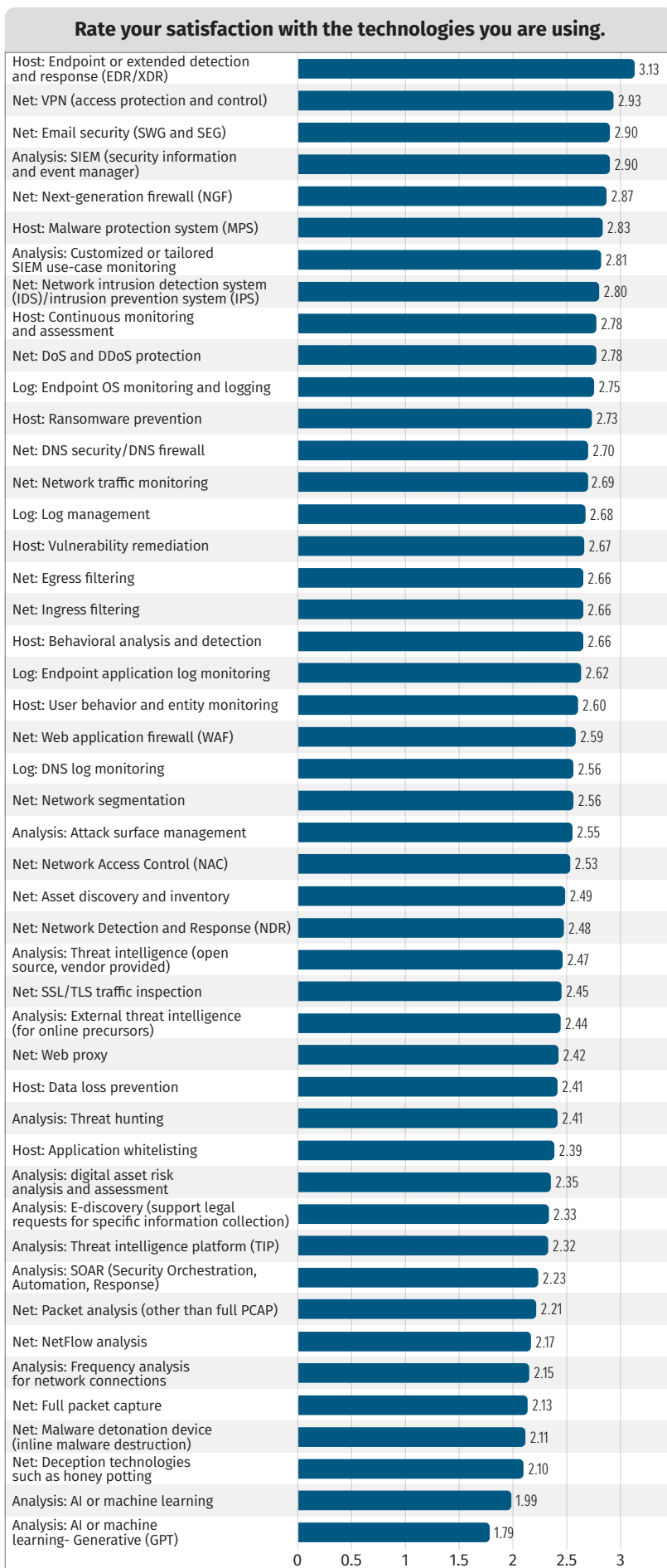


Figure 14. Grade Point Average

Implementing is topped by generative AI, “Analysis: AI or machine learning-Generative (GPT) with 51 responses. Funding is a challenge for SOCs, and the GPT products have rained out of the sky recently to try to optimize efforts within most businesses. It’s the author’s opinion that GPT can be a phenomenal enabler for better communication and analyst understanding of information, but it is not yet a replacement for analysts.

Purchased not implemented sees a tie for the top of the list, “Analysis: Threat intelligence platform (TIP)” and “Analysis: SOAR (Security Orchestration, Automation, Response)” with six responses. It is probably due to shifting priorities. It’s an oversimplification, but when a product is purchased but the implementation gets sidelined, there are usually two major parties to blame: us and them. We, the SOC, are to blame because we frequently underestimate the time to deploy items, and often don’t have a clear comprehension of how the technology will fit into our tech stack. Or the SOC finds it isn’t as easy to accomplish the original intention.

With respect to “Them,” the organization is to blame because there is often last-minute budgeting without allocation of resources from other teams, usually IT.

Finally, Planned has “Net: Deception technologies such as honey potting” with 20 responses. Deception has been slowly increasing in its deployment and satisfaction according to the SOC survey. But it hasn’t reached the production deployment levels of other technology.

## Incident Response Satisfaction

**Section Summary:** Most satisfied with endpoint-based incident response capability; visibility and asset correlation continues to be a challenge.

We asked about satisfaction with incident response capability. Figure 15 is sorted by the sum of very satisfied and satisfied. Endpoint and network detection and response are well regarded. Whereas deception and reverse engineering receive low rankings.

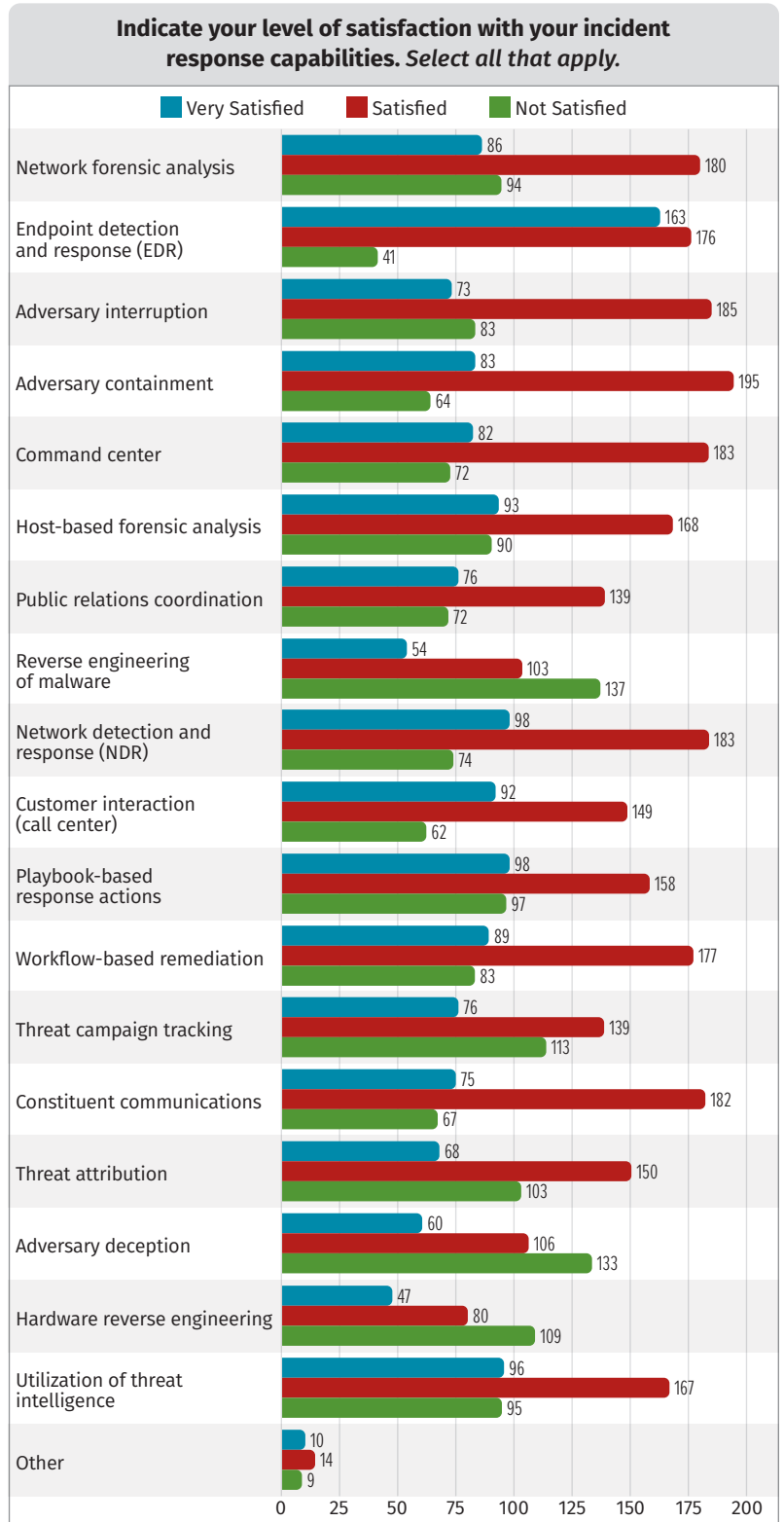


Figure 15. IR Satisfaction

## Visibility

Visibility into systems is important. Correlation to what the systems are doing and who is using them is important to contextualize systems. We asked, “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.” Figure 16 shows that the most common method is mostly automated augmented by manual efforts. A surprising number have a manual effort each time.

A surprising number have integration with physical badging systems and into the SIEM!

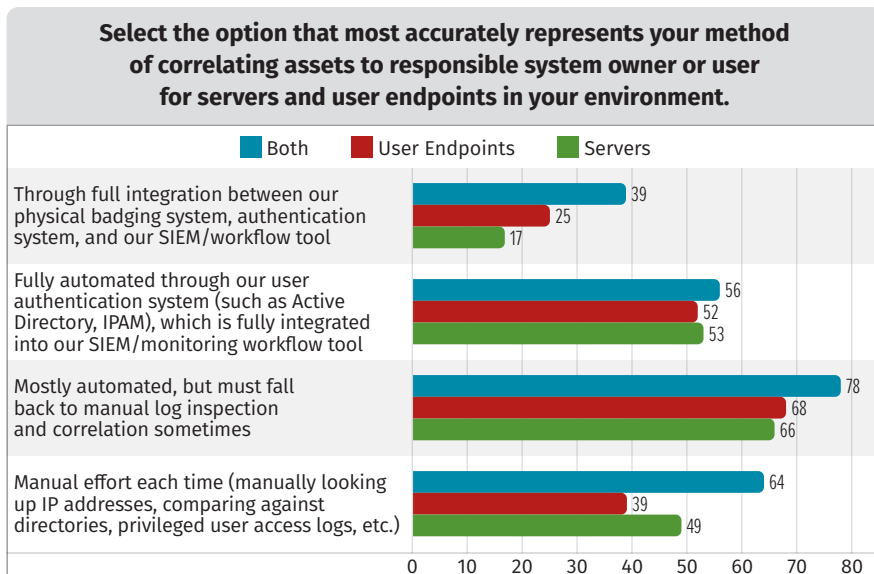


Figure 16. Correlation

## SOC Capabilities and Outsourcing

**Section Summary:** Capabilities are consistent across almost all respondents; frequently outsourced items are pen-testing, forensics, threat-intel, and alert triage.

About two-thirds of the way into the report, we define what we consider a SOC! We’ve reused the capabilities list for years since there’s a strong consensus on what people do in the SOC. Slightly more than 400 people answered the question as to it being done In-house, outsourced, or both. The highest total answer for an activity was 401 (alerting) and the lowest was 378 total (purple teaming). Basically, everyone answering performs all the capabilities in some way. For the lowest count capability, only 25 of the people, or about 6%, don’t perform it. To illustrate this, look at Figure 17.

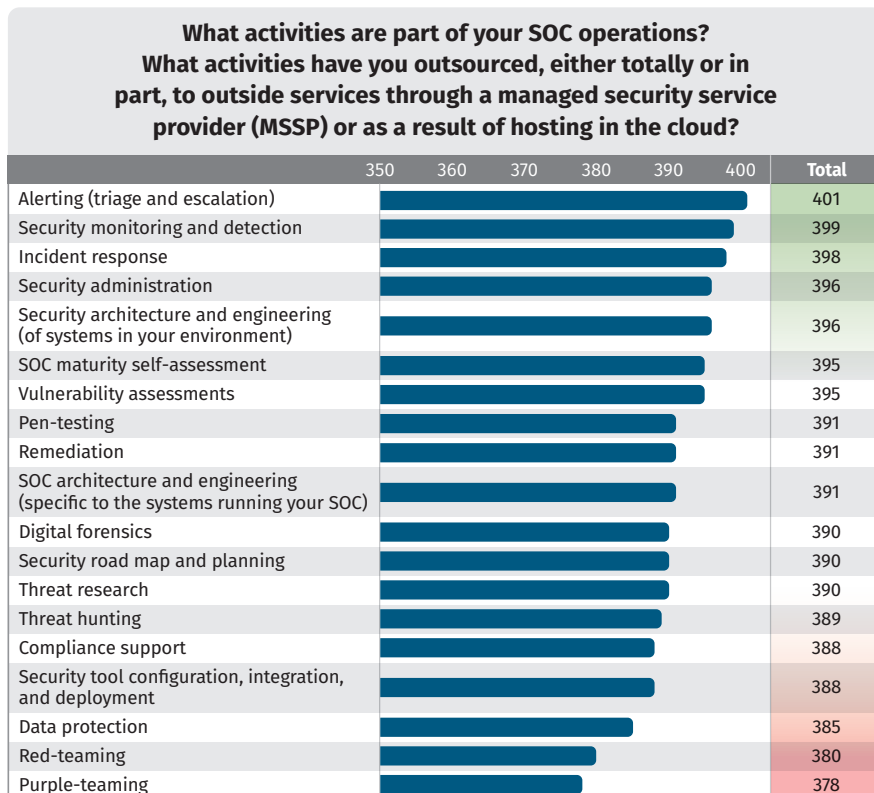


Figure 17. SOC Capabilities

Let's see alternate visualizations to depict the internal/outsourced variation within these responses. First, we'll focus on what's primarily done internally. If we sum "Inhouse" and "Both," we see that security administration, security planning, and architecture are at the top.

Flipping the combination, look in Figure 19 at the sum of purely outsourced and done both in and out. Here we see our typical outsourcing items of pen-test, forensics, threat intel, and initial alert triage are most commonly outsourced.

For measuring maturity of those capabilities, Figure 20 shows that NIST-CSF and MITRE ATT&CK are about equal in the capabilities assessment.

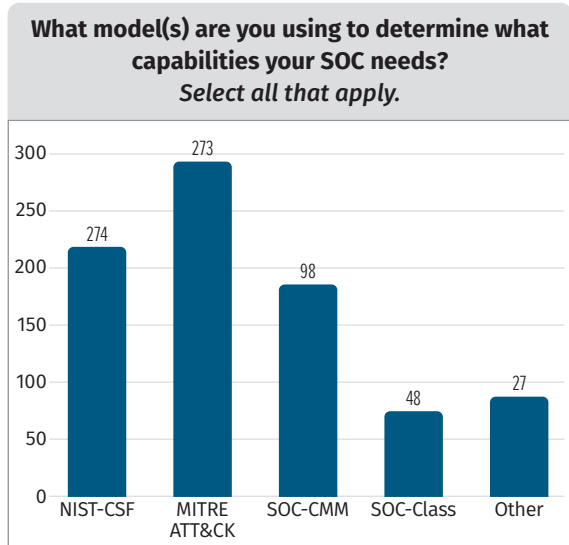


Figure 20. Capability Basis

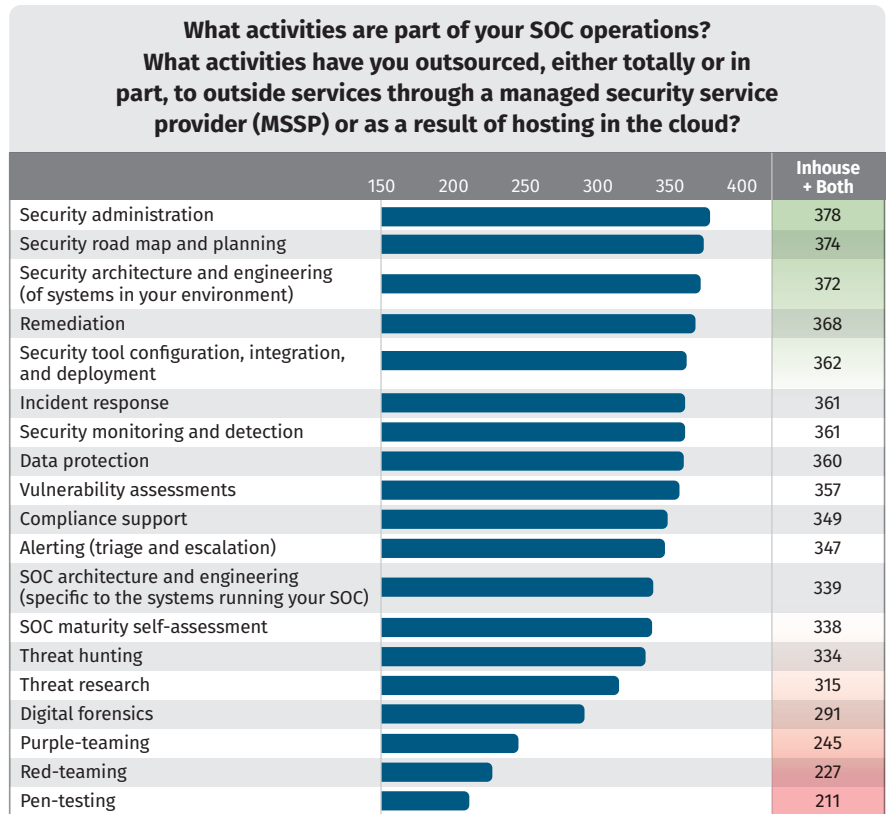


Figure 18. SOC Internal and Internal/Outsourced

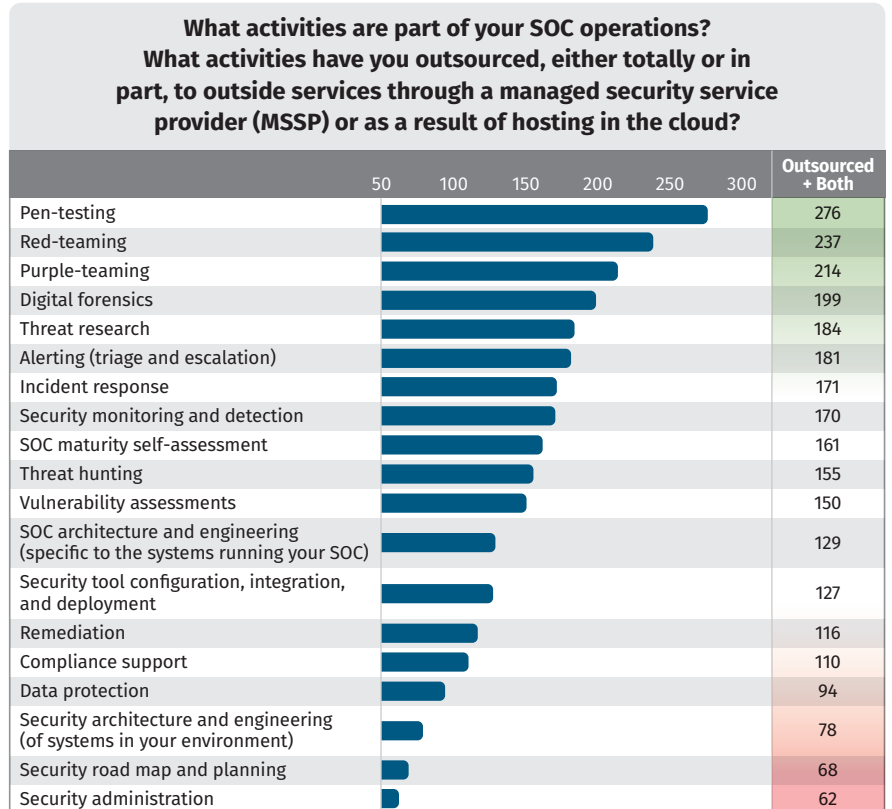


Figure 19. Outsourced + Both

# Architectures

**Section Summary:** Most SOCs run 24x7, and about half are follow-the-sun; most allow work-from-home; 68% have some OT component to monitor, with about equal portions monitoring IT/OT separately as converged.

Most SOCs are 24x7. Only 20% of 402 answered “No” to Q3.24, “Does your SOC operate 24/7?” Of the 314 operating 24x7, 36% are in-house only, 16% are outsourced only, and 26% are mixed internal and outsourced. Of these 314, 49% indicated there’s a “follow the sun” model in place.

Other interesting facts that affect architecture:

- 76% of 403 responses to Q3.26 indicated SOC staff can work remotely.
- Regarding the IT/OT split, 68% of 397 acknowledged there was some OT component. 10% of these said separate monitoring systems were used but the same staff was used. 29% said separately, and 30% said together with IT resources. This is from Q3.30 with 397 people answering the question

# SOC Staff

**Section Summary:** Staff with analytical skills on EDR and vulnerability remediation are in demand; workload calculation per analyst is typically based on historical ticketing or SIEM data.

We mentioned earlier that the most popular SOC staff size is a consistent 2-10. So, let’s dig in to some other details on staff. The overall top three most important technologies for new hires to be familiar with are SIEM for analysis, host based EXDR, and Vulnerability remediation. See Table 1.

Analysis: SIEM (security information and event manager)	138
Host: Endpoint or extended detection and response	98
Host: Vulnerability remediation	73

Most SOCs are trying to figure out what the right workload is per analyst. So, we asked the hard question, “how you calculate per-analyst workload.” Figure 21 shows that most people use the ticket data for start and stop time on a ticket. While this can have some error if ticket opening and closure isn’t done consistently between analysts, it’s a good approximation of level of effort.

Presumably there’s some further calculations to gauge busy time, optimize for expensive work, and looks for per-analyst discrepancies to address skills, knowledge, and training deficiencies as well as varying performance levels. Or, probably not to all of that. “Other” answers aren’t worth a full word cloud. There are primarily “we don’t do this” type answers, “outsourced it’s the MSP’s problem” type answers, and a variety of SIEM and other variations or nuanced tuning on the offered answers.

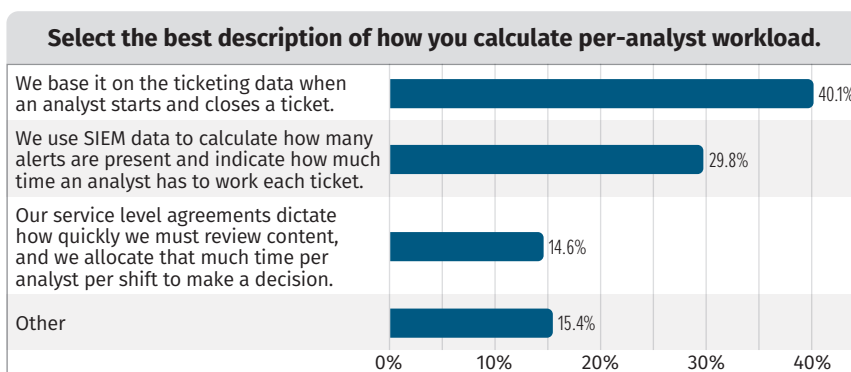


Figure 21. SOC Workload

# Threat Intelligence

**Section Summary:** Threat intel is used for incident response and hunting; typically done based on intuition.

Threat intelligence is supposed to be used to gain tactical and strategic advantage over the threats to our environment. In Q3.21 we asked a “check all that apply” type question on how threat intelligence is being used, and the top response with 194 affirmations was for “Incident Response” follow closely by “Threat Hunting” with 191 responses out of 276 respondents to this question.

We also wondered about the analysis work in threat intelligence, since there are no clear parameters of accuracy and the data pieces can fit together in multiple seemingly meaningful ways, like a mosaic. The top “used frequently” method for CTI analysis was “Intuitive or experienced-based judgement” with 152 responses out of 263 answers. Threat modeling was the top “Used Occasionally” method with 123 of 163 answers.

## Metrics

**Section Summary:** Metrics summary: For outsource functions, metrics are commonly used; the most common is “number of incidents handled.”

A SOC uses metrics to assess performance. As we saw there are several activities which are outsourced, so we asked about metrics for outsourcing in Q3.52. Time based metrics are great, when paired with quality metrics. We have the list ranked based on total in Figure 22.

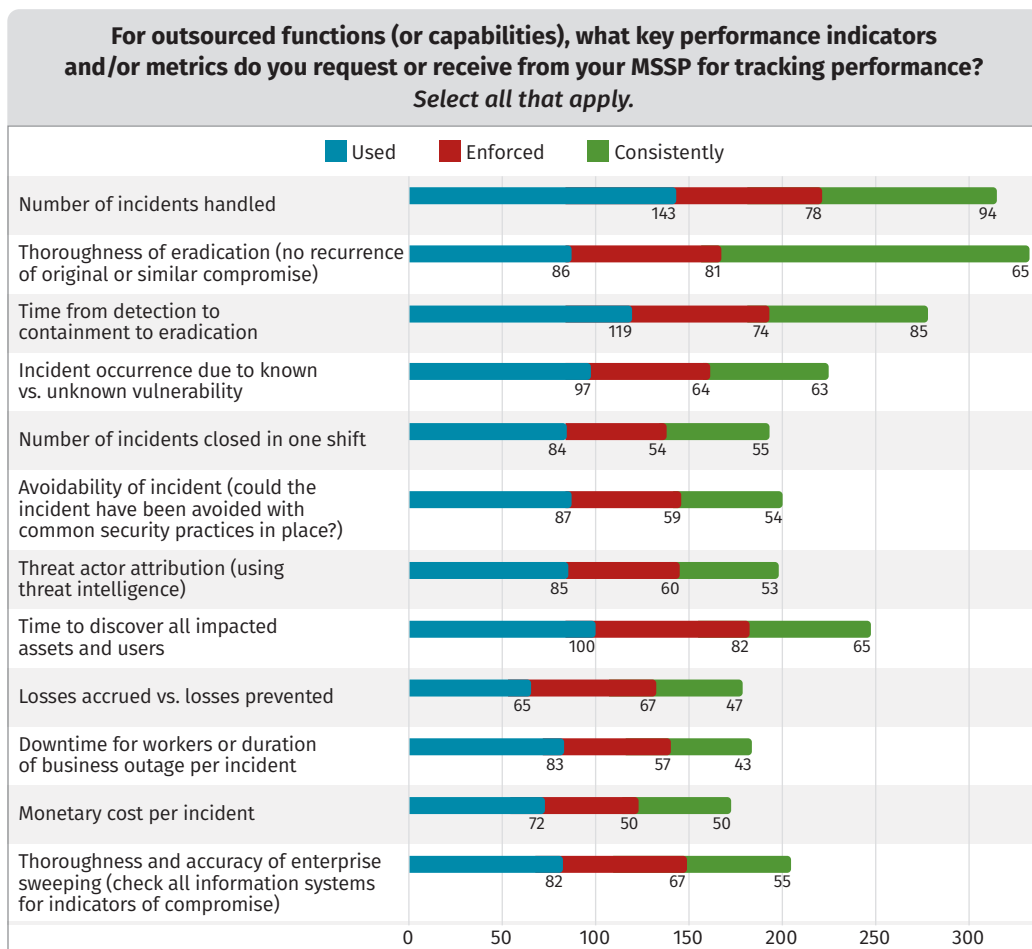


Figure 22. KPIs Used, Enforced, and Consistently Met

Instead of judging the external service provider, SOCs also assess themselves and their performance for their constituents. It has been mentioned in the past that the “number of incidents” seems a reasonable enough metric, but establishing a service level agreement and meeting it on the number of incidents seems improbable. The items in Figure 23 are depicted sorted by the total of used, enforced, consistently met, and all three.

## Conclusion

Cloud-based is new top structure. Everything goes in SIEM is more common than it has been in the past.

Changes from past years: a single, central SOC is more common; vendor-tool based threat hunting is more common; fewer SOCs report planning to deploy AI/ML; people express lower grade for AI/ML than last year; TLS inspection is decreasing; employee duration of employment is increasing; and career progression is more important for retention.

Similar to past years, the internal SOC is mandatory to use and the NOC/SOC are not integrated but coordinate.

Budget of SOC isn’t known to most respondents to the survey. Metrics are provided by 67% of respondents, and the most common metric is number of incidents handled.

Capabilities of the SOC are very consistent across almost all respondents. Frequently outsourced items are pen-testing, forensics, threat-intel, and alert triage.

The most commonly reported SOC size is 2–10 people. The highest cited barrier is lack of automation. EDR/XDR is the most common initial indication of a problem. Most SOCs are 24x7, about half are follow-the-sun and most allow work-from-home. 68% have some OT component to monitor, with about equal portions monitoring IT/OT separately as converged. Threat intel is used for incident response and hunting which is commonly based on intuition.

47 listed technologies were graded and EXDR is top GPA technology still, and AI/ML is lowest. Most satisfied with endpoint-based incident response capability but visibility and asset correlation continue to be a challenge.

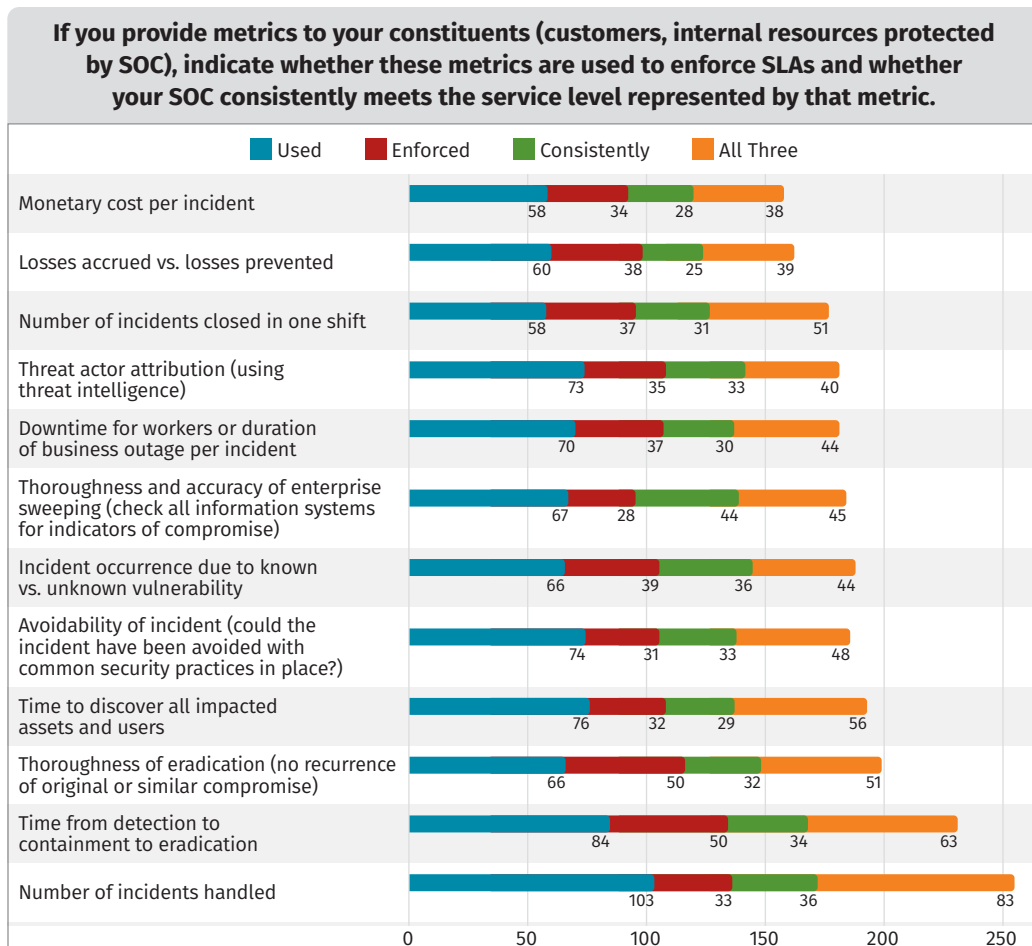


Figure 23. Metrics to Constituents

## Sponsors

SANS would like to thank this survey's sponsors:

Abnormal

ANOMALI



CARDINALOPS



The bridge to possible

corelight

Dropzone AI

Google Cloud

infoblox®

paloalto®  
NETWORKS

RadiantSecurity

SWIMLANE

torq=