SANS | Research Program

Survey

SANS 2024 SOC Survey: Facing Top Challenges in Security Operations

Written by **Christopher Crowley**

May 2024

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 SOCs. 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.

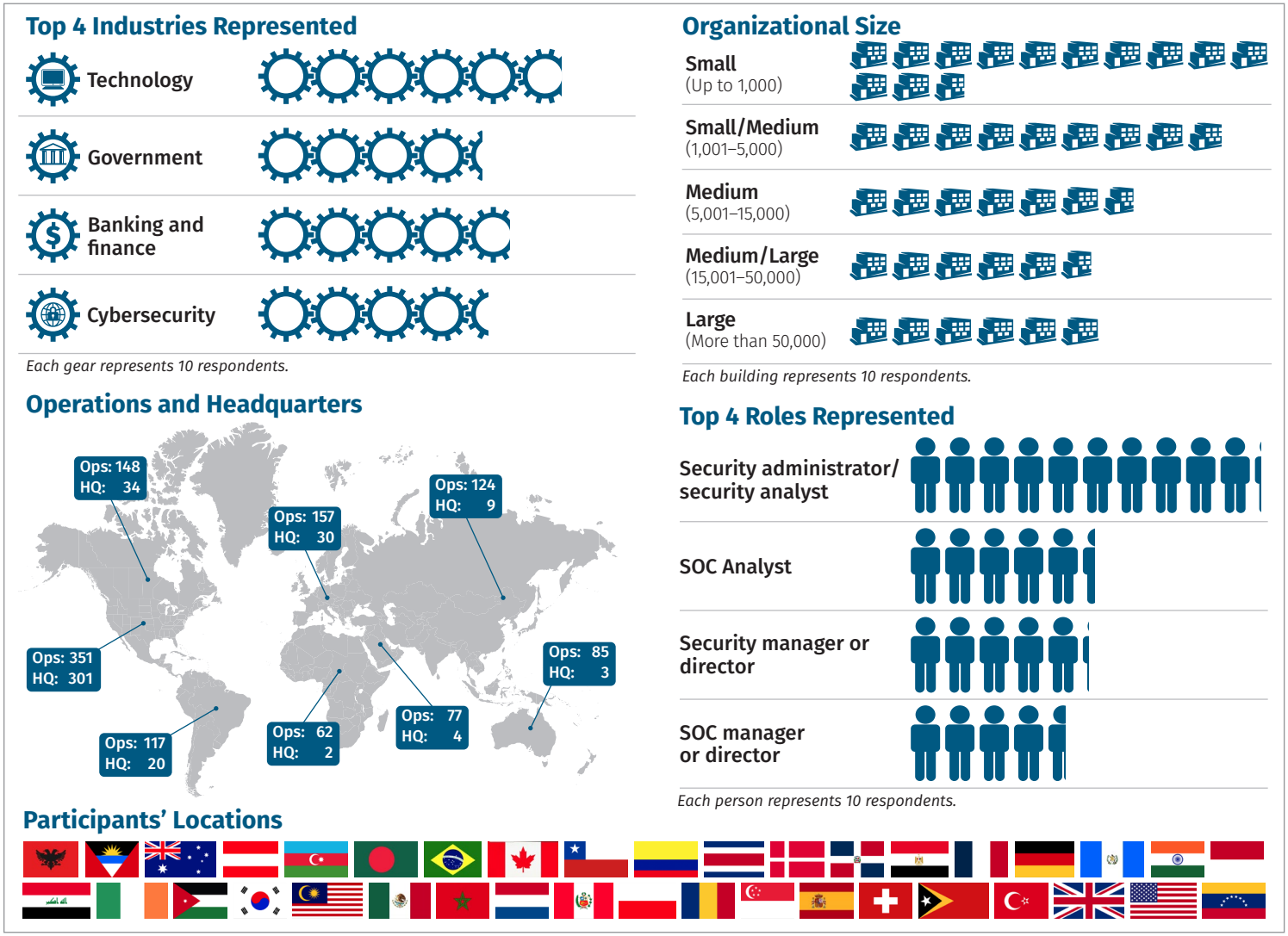


Figure 1. Survey Demographics

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.

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

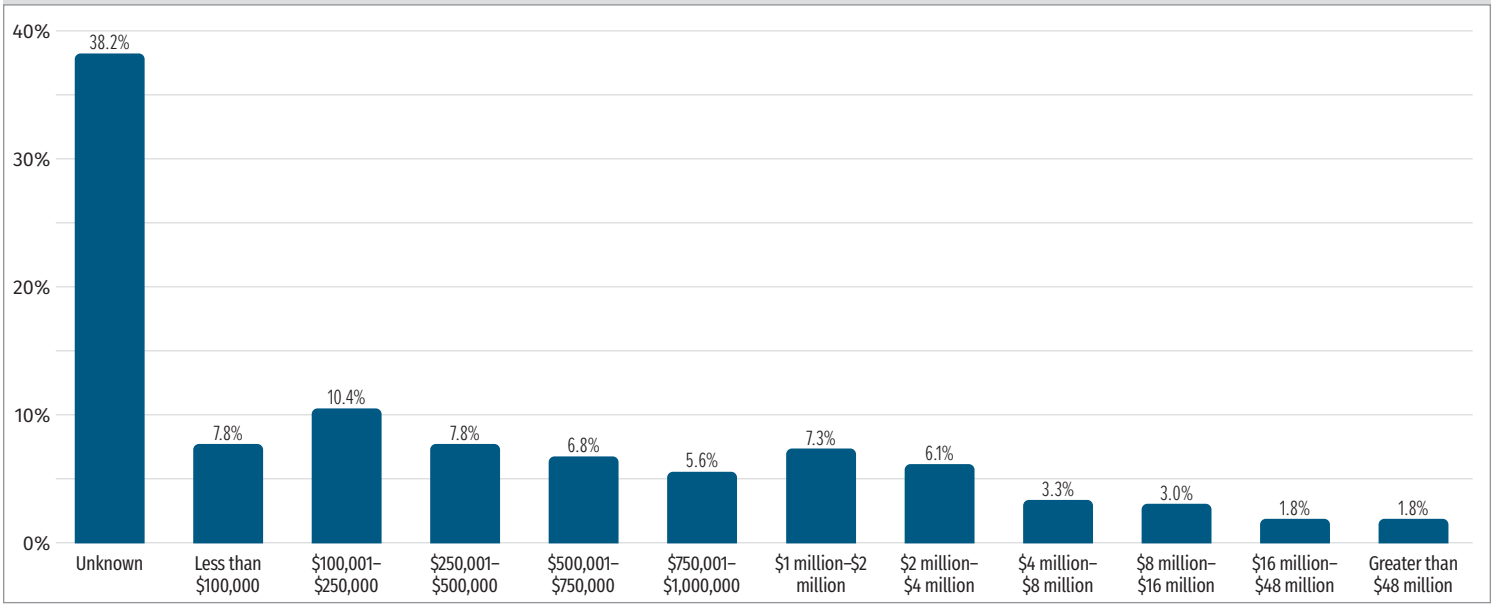


Figure 2. SOC Budget

You're reading this report to understand how it is going in other people's SOCs. 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.

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.***

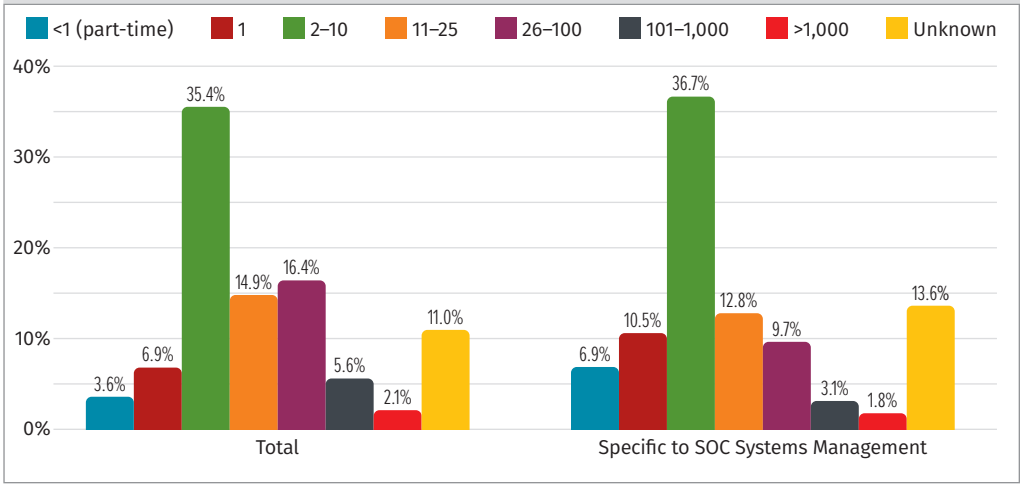


Figure 3. SOC Staffing

"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?"

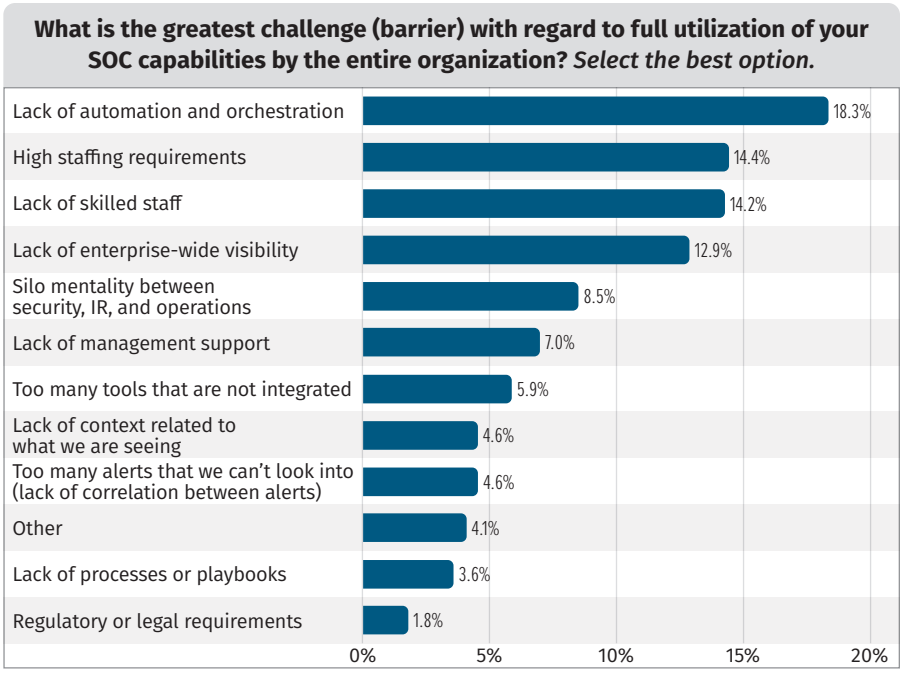


Figure 4. SOC Automation

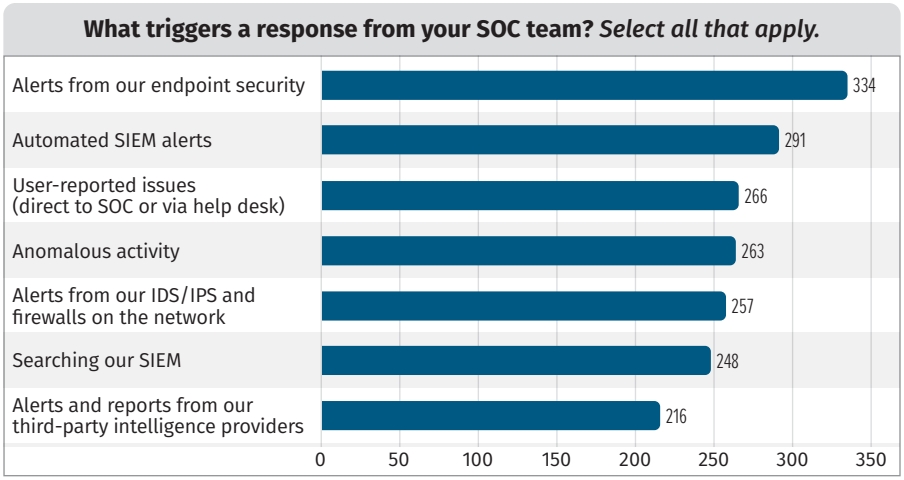


Figure 5. Response Triggers

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?"

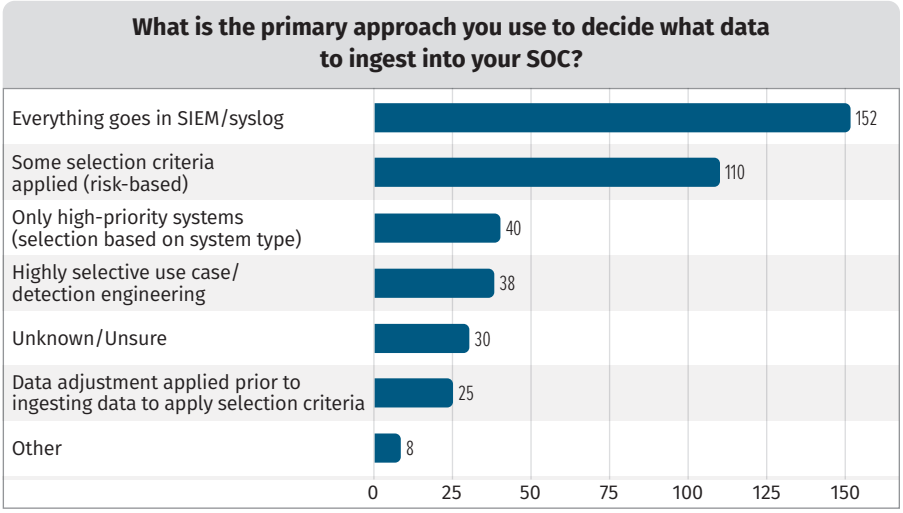


Figure 6. SOC SIEM

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.

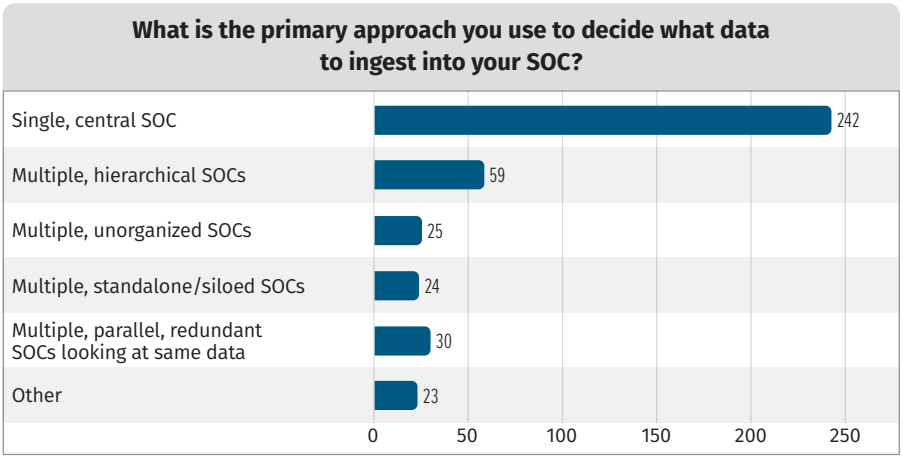


Figure 7. SOC Architecture

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 8.

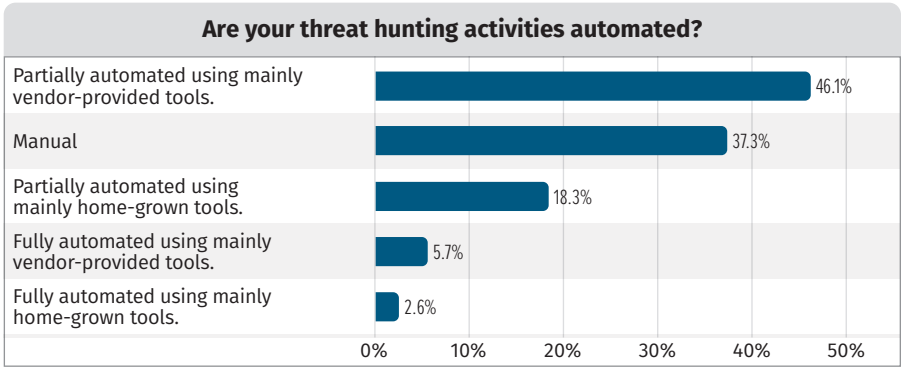


Figure 8. Hunting Automation

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.

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.

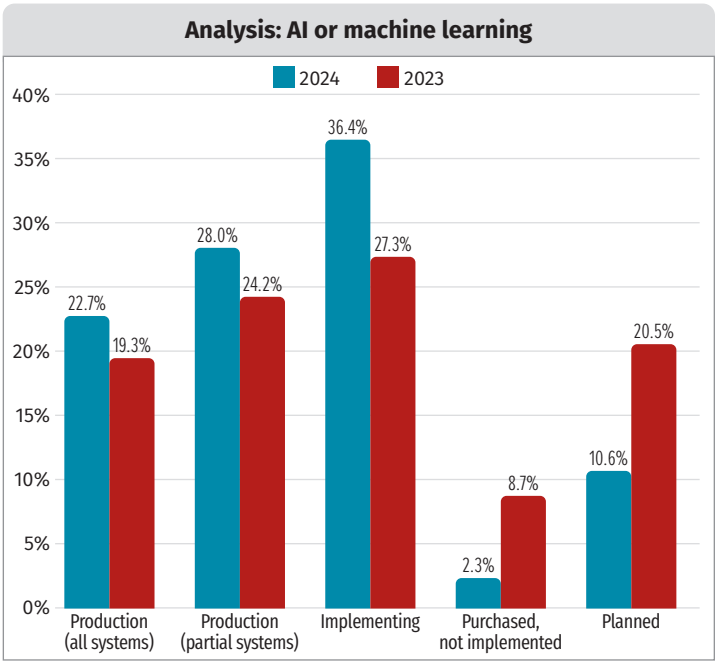


Figure 9. AI Implementation

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.

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.

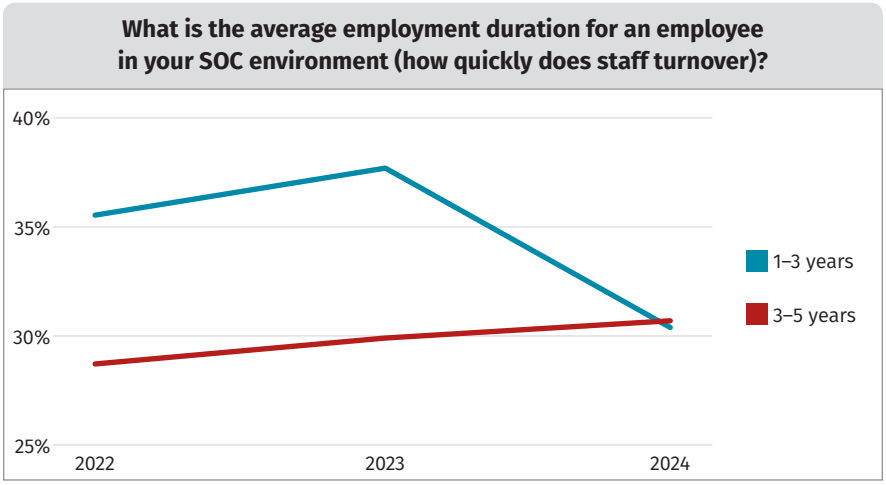


Figure 10. Employment Duration

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.

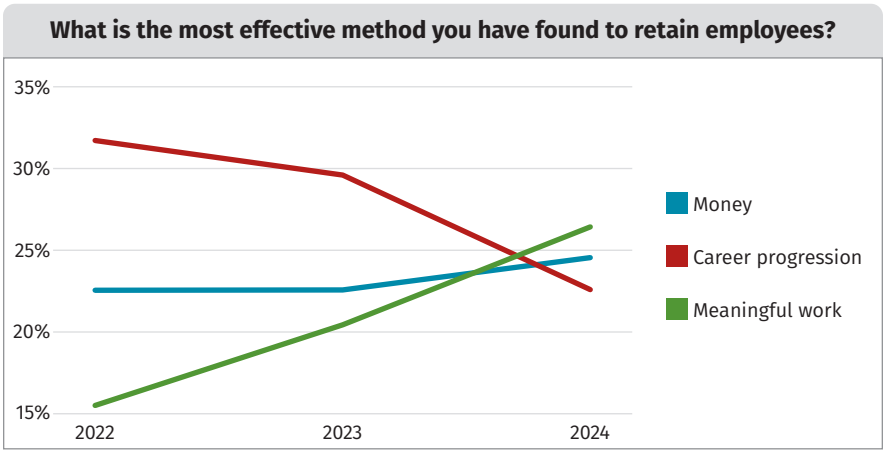


Figure 11. Retention

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.

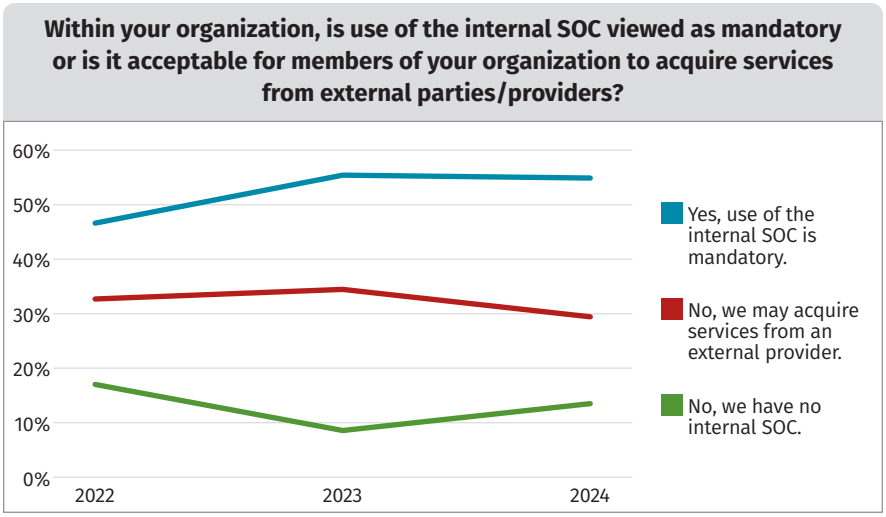


Figure 12. SOC Mandatory

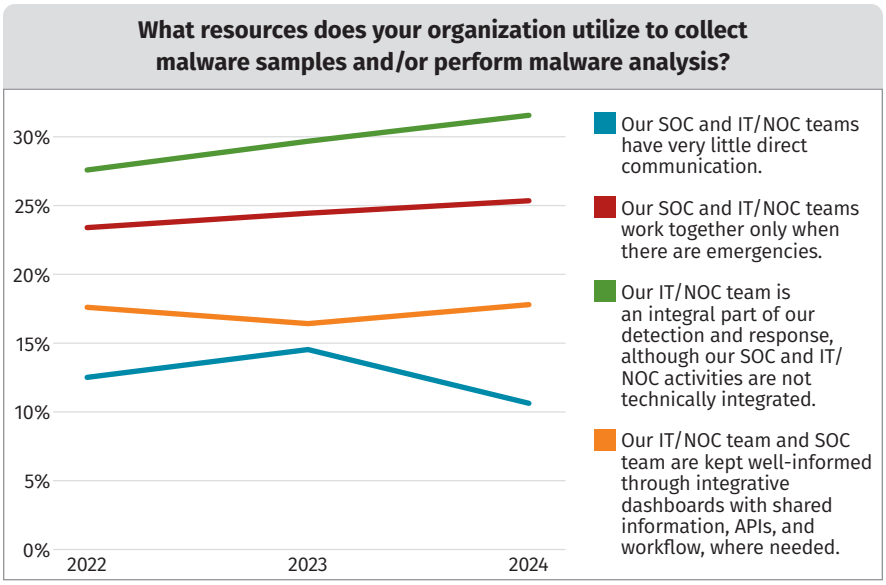


Figure 13. NOC/SOC Relation

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 14 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 15 on the next page 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.

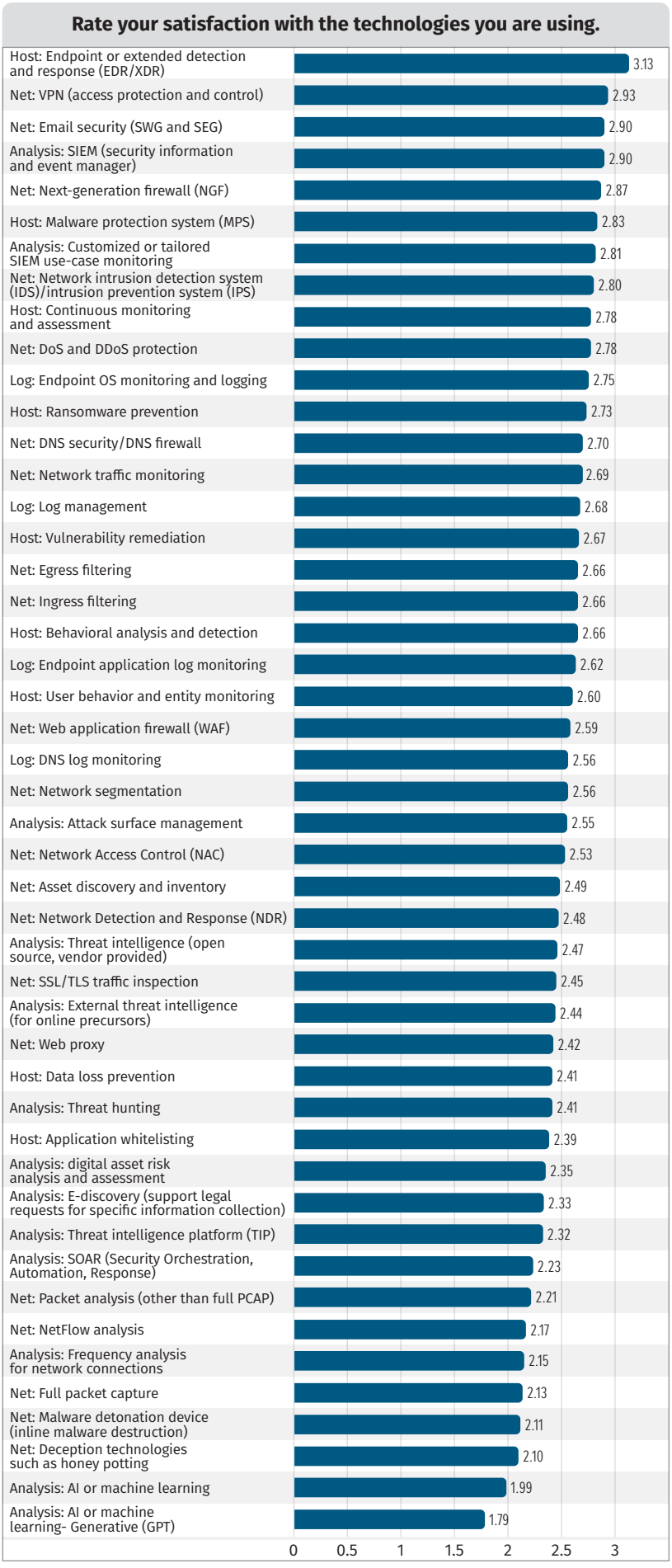


Figure 14. Grade Point Average

Rate your satisfaction with the technologies you are using.

	Production (all systems)	Production (partial systems)	Implementing	Purchased, not implemented	Planned	GPA
Net: Email security (SWG and SEG)	111	25	11	3	2	2.90
Host: Endpoint or extended detection and response (EDR/XDR)	103	39	10	3	2	3.13
Net: VPN (access protection and control)	102	39	9	1	1	2.93
Host: Malware protection system (MPS)	90	37	16	1	3	2.83
Net: Next-generation firewall (NGF)	89	39	12	2	3	2.87
Analysis: SIEM (security information and event manager)	88	43	10	3	5	2.90
Host: Vulnerability remediation	87	45	12	1	4	2.67
Net: Network intrusion detection system (IDS)/intrusion prevention system (IPS)	87	34	14	2	8	2.80
Net: DNS security/DNS firewall	87	29	20	3	1	2.70
Host: Ransomware prevention	86	45	11	4	5	2.73
Host: Behavioral analysis and detection	82	46	14	0	5	2.66
Net: Network segmentation	81	49	18	1	4	2.56
Log: Endpoint OS monitoring and logging	80	51	12	1	7	2.75
Net: Network traffic monitoring	80	50	11	3	4	2.69
Net: Ingress filtering	79	35	9	2	9	2.66
Log: Log management	78	56	13	3	3	2.68
Host: Continuous monitoring and assessment	77	46	13	3	6	2.78
Net: DoS and DDoS protection	77	46	16	4	2	2.78
Log: DNS log monitoring	77	45	20	3	6	2.56
Net: Asset discovery and inventory	75	49	17	2	5	2.49
Net: Web proxy	71	34	21	2	13	2.42
Log: Endpoint application log monitoring	69	50	17	5	7	2.62
Net: Web application firewall (WAF)	68	44	26	1	6	2.59
Net: Egress filtering	67	42	20	2	12	2.66
Host: User behavior and entity monitoring	64	48	25	3	7	2.60
Net: Network Access Control (NAC)	64	40	23	3	6	2.53
Analysis: Customized or tailored SIEM use-case monitoring	61	47	22	2	6	2.81
Analysis: Attack surface management	61	40	28	4	6	2.55
Net: Network Detection and Response (NDR)	61	36	26	2	9	2.48
Net: SSL/TLS traffic inspection	59	49	22	1	7	2.45
Analysis: Threat intelligence (open source, vendor provided)	54	54	25	2	9	2.47
Host: Data loss prevention	53	50	37	3	3	2.41
Host: Application whitelisting	53	47	32	2	10	2.39
Analysis: External threat intelligence (for online precursors)	50	53	27	3	7	2.44
Net: NetFlow analysis	50	45	26	3	14	2.17
Analysis: SOAR (Security Orchestration, Automation, Response)	50	38	33	6	11	2.23
Analysis: E-discovery (support legal requests for specific information collection)	48	48	27	3	8	2.33
Analysis: Threat intelligence platform (TIP)	45	41	35	6	9	2.32
Analysis: Threat hunting	43	61	33	1	8	2.41
Net: Malware detonation device (inline malware destruction)	42	43	28	3	16	2.11
Analysis: digital asset risk analysis and assessment	42	42	34	2	10	2.35
Net: Full packet capture	39	43	36	2	14	2.13
Net: Packet analysis (other than full PCAP)	38	54	29	3	16	2.21
Net: Deception technologies such as honey potting	38	29	43	2	20	2.10
Analysis: Frequency analysis for network connections	36	45	33	2	11	2.15
Analysis: AI or machine learning	30	37	48	3	14	1.99
Analysis: AI or machine learning- Generative (GPT)	26	33	51	2	17	1.79

Figure 15. Technology Satisfaction Report Card

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 16 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.

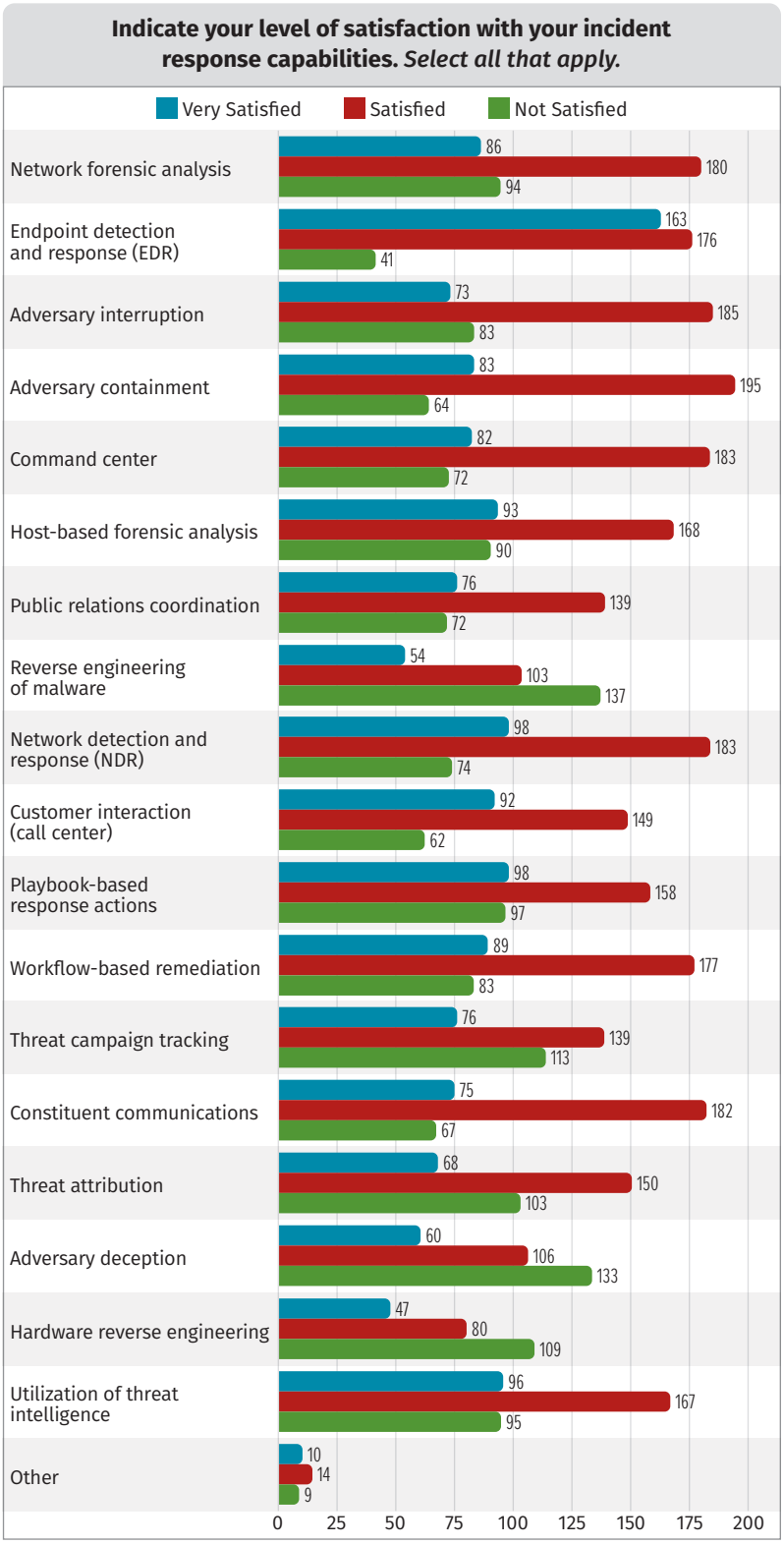


Figure 16. IR Satisfaction

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 17 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!

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.

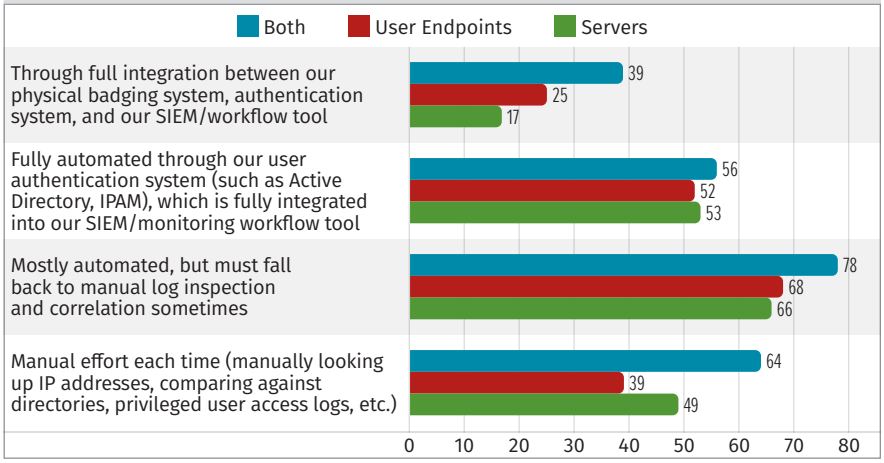


Figure 17. Correlation

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 18.

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?

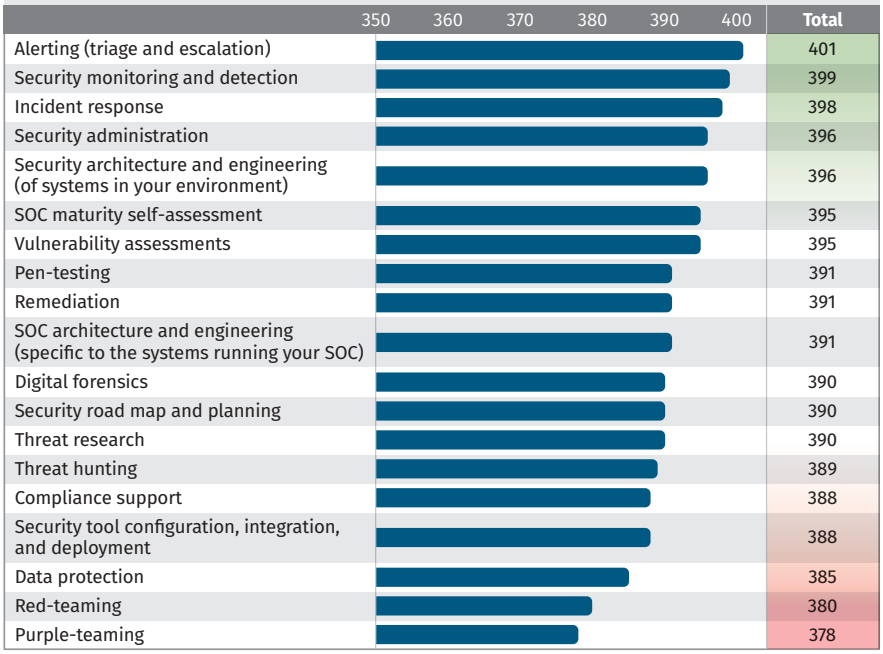


Figure 18. SOC Capabilities

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 20 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 21 shows that NIST-CSF and MITRE ATT&CK are about equal in the capabilities assessment.

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?

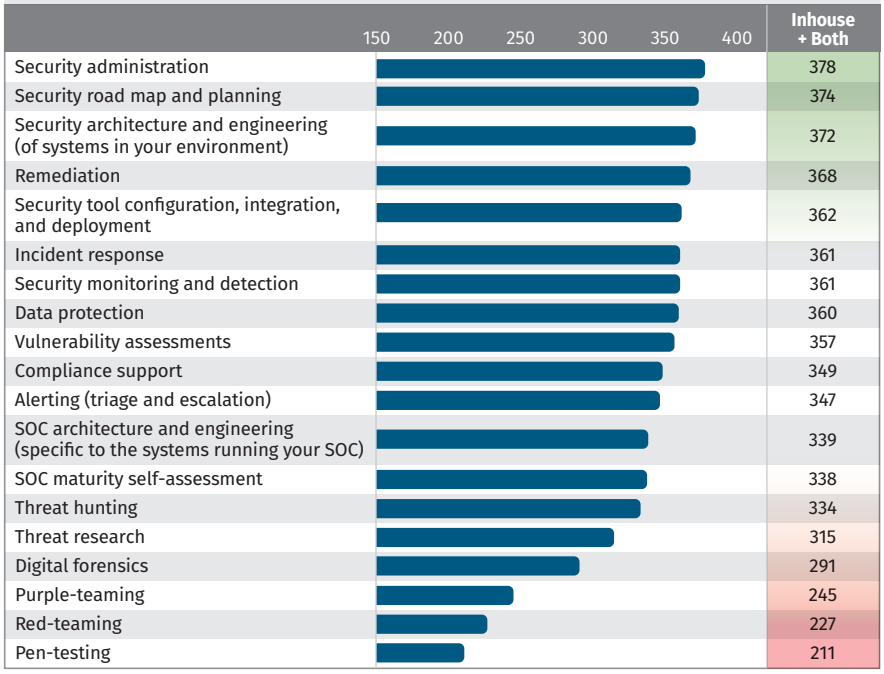


Figure 19. SOC Internal and Internal/Outsourced

What model(s) are you using to determine what capabilities your SOC needs?
Select all that apply.

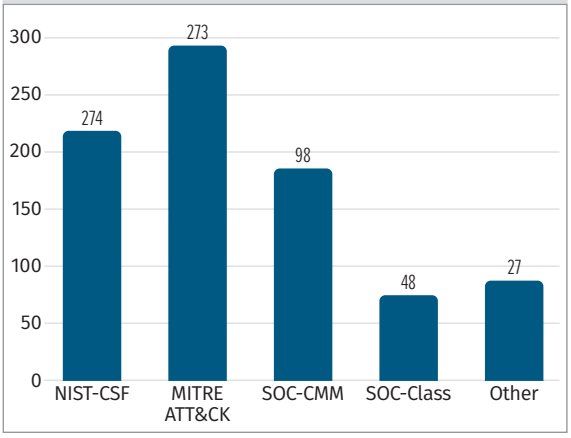


Figure 21. Capability Basis

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?

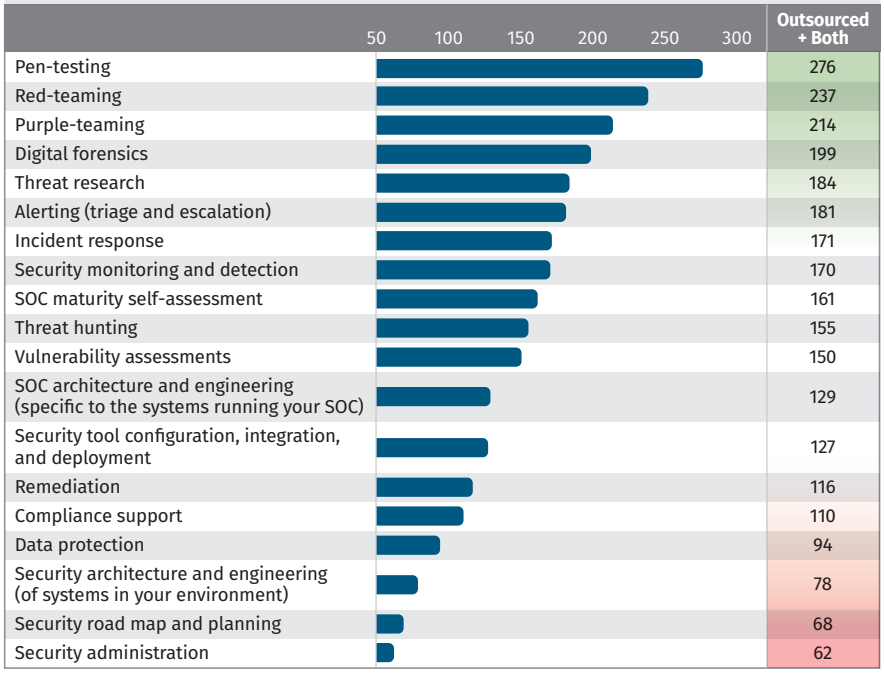


Figure 20. Outsourced + Both

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.

Table 1. Top SOC Skills

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 22 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.

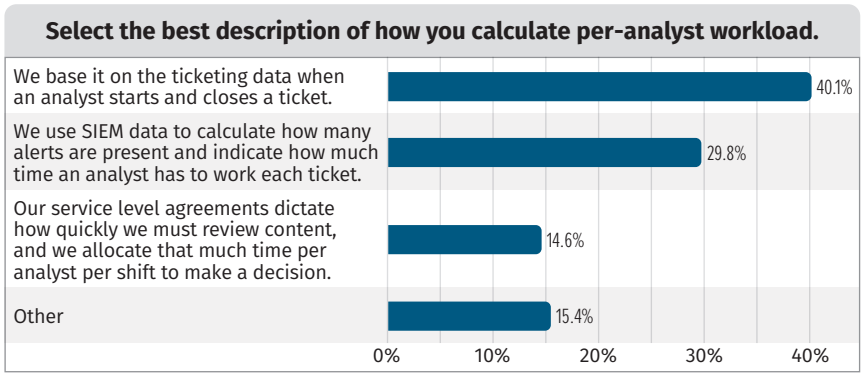


Figure 22. SOC Workload

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.

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 23.

For outsourced functions (or capabilities), what key performance indicators and/or metrics do you request or receive from your MSSP for tracking performance?
Select all that apply.

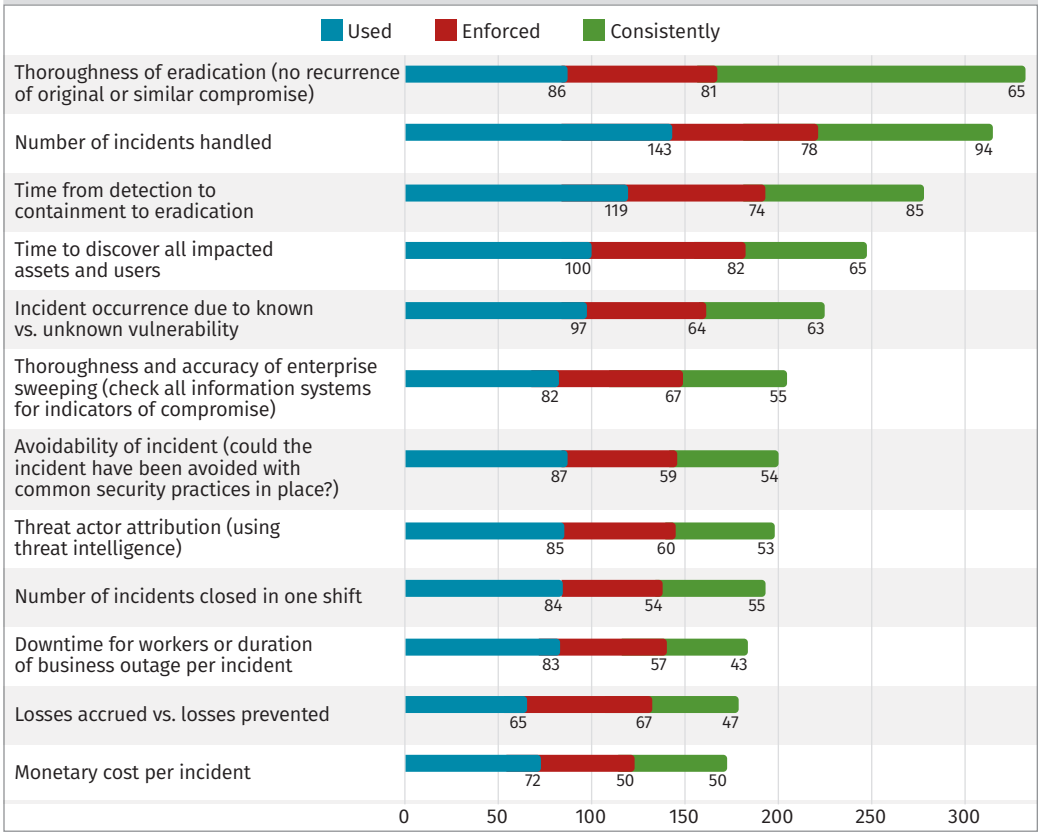


Figure 23. KPIs Used, Enforced, and Consistently Met

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 24 are depicted sorted by the total of used, enforced, consistently met, and all three.

If you provide metrics to your constituents (customers, internal resources protected by SOC), indicate whether these metrics are used to enforce SLAs and whether your SOC consistently meets the service level represented by that metric.

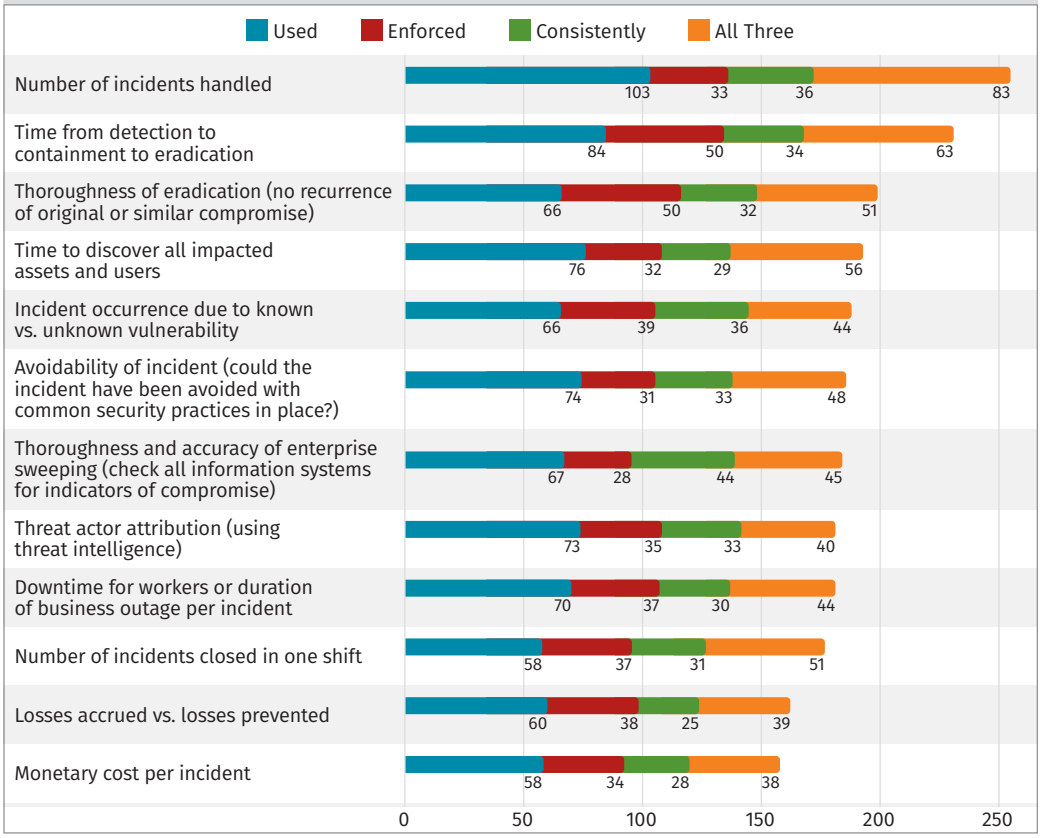


Figure 24. Metrics to Constituents

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.

Sponsors

SANS would like to thank this survey's sponsors:

SANS | Research Program

Product Briefings for SOC

The 2024 SOC Survey represents the latest edition of SANS Institute's poll of security professionals. The sponsors of this year's survey all offer advanced capabilities that we believe will be of interest to SANS' clients, and, for this reason, we're presenting the following product briefings on some of their relevant offerings.

Abnormal

SANS | Research Program

Product Briefing

SOC with Abnormal:

Insights from the 2024 SANS Institute SOC Survey

July 2024

The job of the SOC gets bigger every day. The budget often does not. Attracting and retaining experienced staff is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

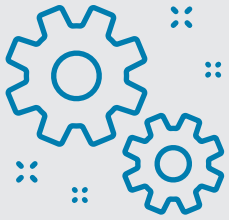
Abnormal Security

Lots of companies are offering AI these days, but Abnormal Security's platform is AI-native, designed from the beginning to understand normal human behavior and use that known baseline of behavior to stop attacks like business email compromise, credential phishing, malware, vendor fraud, and more.

Humans, as you know, are the biggest vulnerability in most systems, and email is still the easiest way to access them. SANS' Incident Response report from 2023 found 95% of breaches were the result of spear phishing. Despite years of training and awareness programs, many people, even those in responsible roles, are still far too trusting, and therefore far too likely to click a bad link or be fooled by a fake message from the CEO.

The advent of cloud email systems brings new attack vectors, including some that don't touch the user at all. While some organizations have seen attackers pivot from the email servers to other parts of the organization's cloud environment, others have seen sophisticated attacks across applications like Slack that are hyper-targeted, able to personalize to a staggering degree and thus fool a user into thinking the sender is a trusted colleague or trusted organization.

Key Findings



Lack of automation and orchestration is a significant problem reported by respondents to the SANS SOC Survey.

Staffing issues – high staffing requirements and lack of skilled staff – are the top barrier SOC teams face.

Increasingly, SOC teams are automating threat hunting activities.

Abnormal Security provides comprehensive protection against these attacks and more, including account takeovers, internal-to-internal phishing, and even chat messages. It can also protect against attacks that are invisible both to users and to most commonly used security solutions by detecting suspicious behavioral deviations—rather than solely relying on known threat intelligence or policies. By understanding known behavior, the platform recognizes permission changes, anomalous sign-ins, and many other indicators of compromise (IOCs), bringing an industry-leading amount of detection firepower to your environment. Where conventional email security architecture staggers, Abnormal steps up and provides reliable protection. See Figure 1.

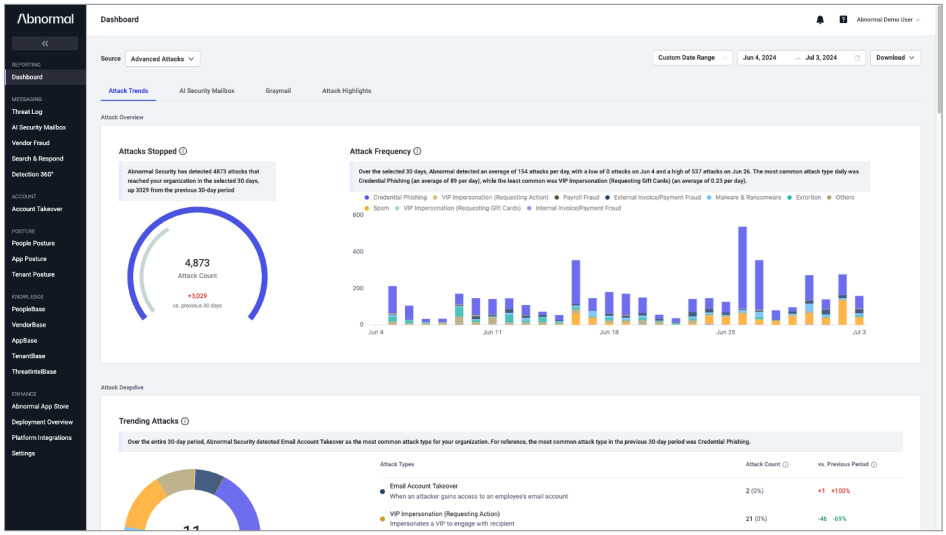


Figure 1. Abnormal Dashboard

While much of the world's AI is still in a shakeout phase, Abnormal's systems are trained on human behaviors in real business situations using real systems. That means the SANS SOC Survey users who say they need automation and orchestration can turn to Abnormal Security as an AI solution they can trust to do its job – stopping more attacks with fewer false positives. Because Abnormal is AI-native, the people building the software are deeply versed in data science and security. And because Abnormal serves thousands of customers of all sizes, it can correlate anonymized data from the expanding customer base and determine when coordinated attacks are happening.

In addition, Abnormal integrates with your employee-reported phishing workflow through a phishing mailbox, mailing list, or phishing button. Its autonomous AI then automatically triages, judges, and remediates reported messages across all inboxes. The solution also delivers an AI cybersecurity assistant that users can ask questions related to reported messages or other cybersecurity topics, receiving accurate answers from the AI, educating them on their submissions, and enhancing the organization's overall security awareness program.

It's clear from the SANS SOC Survey results that many security operations team members are feeling pressured to do more with the same or fewer staffers. Abnormal eases the load on analysts without adding overhead – it deploys in 60 seconds and uses easy-to-manage APIs to connect to your existing systems (see Figure 2).

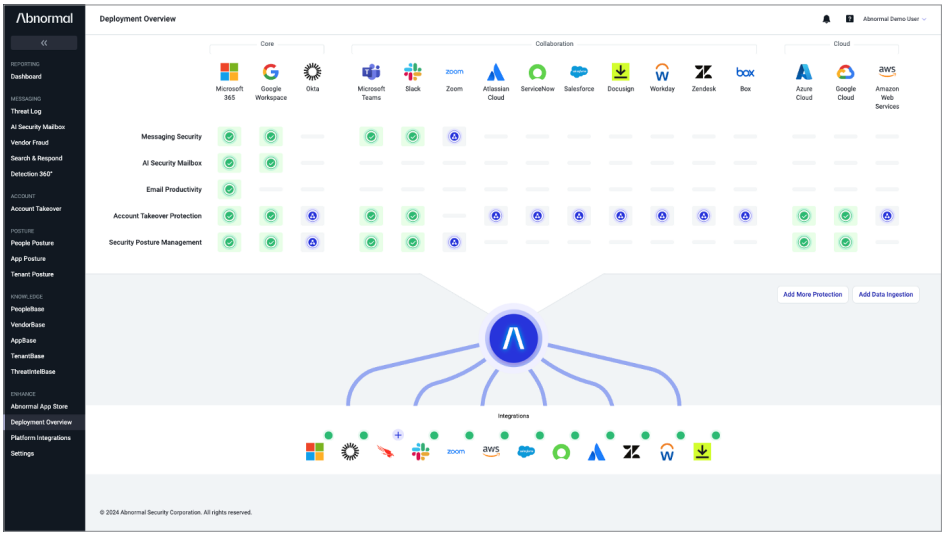


Figure 2. Deployment Overview

Abnormal is so powerful and effective that 70 percent of customers have used it to replace their Secure Email Gateways (SEGs). Its behavioral AI detection allows Abnormal to stop attacks that have never been seen before, while maintaining continuous monitoring of the organization's cloud risk.

If email is crucial to your organization and you want to stop attackers from reaching it, visit **https://abnormalsecurity.com**

ANOMALI

SANS | Research Program

Product Briefing

SOC with Anomali:

Insights from the 2024 SANS Institute SOC Survey

July 2024

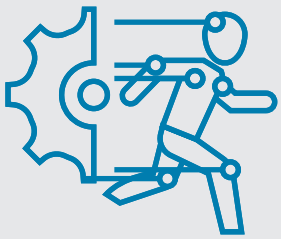
The job of the SOC gets bigger every day. The budget often does not. Attracting and retaining experienced staff is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

Anomali

Anomali's Security Operations Platform combines security information and event management (SIEM), security orchestration, automation, and response (SOAR), user and entity behavior analytics (UEBA), and threat intelligence platform (TIP) into one fully integrated solution. It delivers real-time security insights—along with historical context—and correlates them with up-to-the-minute threat intelligence so SOC teams can take immediate action before an attack gains traction. SANS SOC survey respondents understand that this type of context is hard to come by since most products provide only limited analysis of historical data.

You may be familiar with Anomali's threat intelligence product, ThreatStream, which aggregates threat intelligence data from a wide range of sources, including open-source feeds, commercial feeds, dark web monitoring, and proprietary research. It also includes detailed and correlated threat actor profiles. ThreatStream has long been recognized for its depth, reliability, and reach. It facilitates collaboration and information sharing among its users to continually augment its knowledge base. This enables them to share data, research findings, and best practices with each other, creating an exceptional source of collective intelligence leveraged by many leading cybersecurity companies—including Splunk, Elastic, and SumoLogic.

Key Findings



Lack of automation and orchestration is a significant problem reported by respondents to the SANS SOC Survey.

Staffing issues – high staffing requirements and lack of skilled staff – are the top challenges SOC teams face.

AI and machine learning are not widely trusted yet.

SOC professionals are characteristically wary about over-reliance on AI, fearing that an automated system will react inappropriately in the face of threats or that it will be vulnerable to AI attacks. We saw that in the SANS SOC Survey, where AI ranked low on analysts' list of most valued tools. However, Anomali's AI is different. It's trained on vast amounts of security data that operates in a closed loop. It brings serious processing power to petabytes of log information, running even deep and complex queries in less than a minute. As mentioned earlier, Anomali can review years of historical data to pinpoint the source of a piece of sleeper code or a zero-day attack—critical in today's threat environment.

Anomali's generative AI Copilot lets analysts use natural language to request complex and detailed threat reports without learning specialized query languages. Copilot also helps summarize reports that SOC teams can share with leadership teams.

Anomali doesn't just spot threats—it actively prevents them. For example, Anomali Integrator reports problem behaviors directly to the firewall to stop specific attacks from ever penetrating the environment. The best-in-class speed of response prevents attackers from moving laterally to parts of the organization where they can do more harm. Anomali can also be configured to report threats to related organizations (or to ISACs), helping them stay protected while expanding the knowledge base of collective intelligence. In addition, Anomali's technologies are all cloud-native and easy to deploy and scale.

Figure 1. Anomali UI

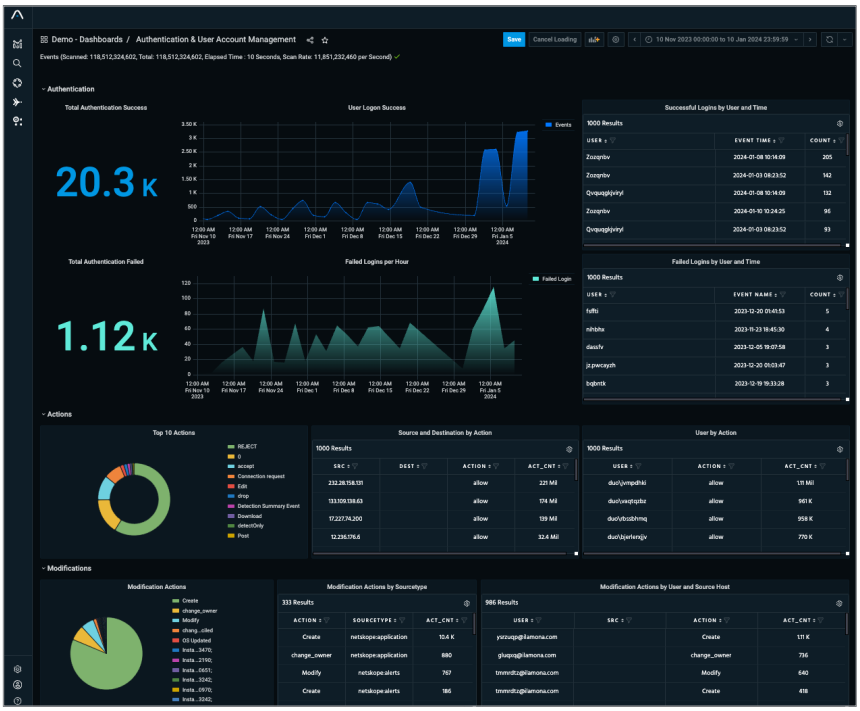


Figure 2. Anomali Dashboard

If you're ready to inject enterprise-grade speed and efficiency into your SOC, visit **www.anomali.com**

corelight

SANS | Research Program

Product Briefing

Security Operations with Corelight:

Insights from the 2024 SANS Institute SOC Survey

July 2024

The job of the SOC gets bigger every day. The budget often does not. Staffing is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

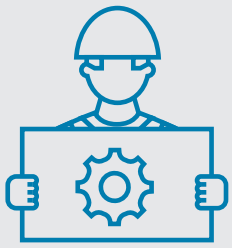
Corelight

Corelight sees and understands the struggle to keep a SOC staffed and hitting its metrics without burning out the humans who work there. As the SANS 2024 SOC Survey indicates, many security operations managers find themselves making do without enough experienced analysts. Even large and complex organizations often have just two to 10 people tasked with protecting the environment from attacks.

Developed from the open source ecosystem, Corelight's key technologies have been refined through years of real-world use. Corelight functions as a Tier 1 analyst, performing automated network detection and response (NDR) and surfacing only high-quality evidence and alerts to the human team.

Corelight uses AI to detect a wide range of sophisticated attacks, to enrich security data with contextual insight, and to provide SOC analysts with new capabilities for understanding and reacting to security alerts. Beyond AI, Corelight uses machine learning and behavioral and signal-based analysis to deliver results. Because Corelight draws on the vast amount of information developed in the open source community, the AI is already trained on relevant and reliable data, clearly labeled as AI-generated. None of your data is ever sent back to large language models, because we're all in the security business.

Key Findings



SOC staff report lack of automation and orchestration are frequent barriers.

Staffing—which includes both high staffing requirements and lack of experienced staff—is perhaps the most widely reported barrier.

SOC teams are more likely to feed all their logging data into a SIEM or other system, leading to a large volume of data to triage and a time-consuming number of false positives.

The human analyst reviewing an alert gets immediate links to the evidence used to create that alert and the endpoints affected. That lets the analyst check for accuracy, but also helps junior analysts build their skills by showing them the formulas that trigger alerts and the common signals of known attacks.

A big headache for SOC analysts is the volume of duplicates and false positives that many network detection systems generate. Corelight assesses alerts for validity and aggregates duplicates, so an event that generates 100 or more alerts reaches the human analyst as a single incident. Robust open source threat hunting communities help your SOC analysts keep up with new detections and emerging threats.

SOC managers can save even more time by automating common response and mitigation steps in Corelight. An analyst doesn't even have to leave Corelight to isolate a detected entity and begin an investigation. Corelight customers report faster MTTR (mean time to remediation), reduction in number of unsolved cases, higher case closure rates, and validated containment of threats. An analyst who wants to track evidence of a given event can get it in seconds.

SANS SOC Survey respondents reported issues with automation and orchestration—not just automating tasks, but creating automations that help different pieces of software work together to make an analyst's day easier. Corelight integrates easily with popular systems and platforms such as CrowdStrike and Splunk. It natively integrates with SIEMs, XDRs, and data lakes, plus network, host and cloud data across complex global environments. Corelight then delievers network telemetry for organizations that use these tools for their threat detection and triage while reducing the volume of alerts that need to be ingested in these tools. In most cases, there's no need for someone on the SOC team to spend time writing integrations—it just works (see Figure 1). Vendor lock-in isn't a problem, because Corelight is built on open source technologies Zeek and Suricata, allowing organizations to be sure they can keep their SOC operating even if they change providers.

SOC analysts need visibility into their environments, and the SANS SOC Survey shows many security operations professionals find their systems aren't delivering on this need. Corelight allows analysts to spot IoCs and emerging threats across multicloud environments and more than 50 protocols, including DNS. When detailed logs are needed, they're there—and when they're not, they're out of sight so analysts can focus on triage and mitigation.

Most cloud-native security tools rely on VPC flow logs for threat detections that can only detect a limited number of threats. Corelight's full packet analysis improves visibility and detects command-and-control threats with essentially any protocol tunnel or with unknown servers.

Multicloud environments mean inconsistent telemetry. Corelight's Open NDR delivers consistent telemetry from on-prem to cloud, which minimizes the need for SOC team retraining and addresses skilled staffing shortage. In addition, most cloud DevOps workloads are deployed without a security agent. Only Corelight can detect threats that evade the endpoint agents.

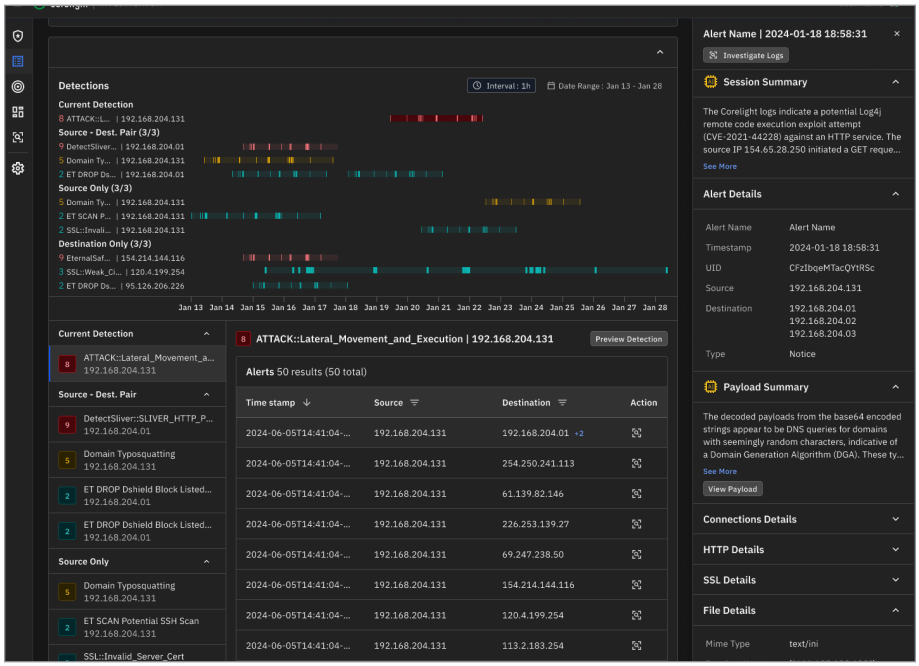


Figure 1. Open NDR Triage

If you're looking for a robust defense that will reduce, not expand, your SOC analysts' workload, visit **https://corelight.com**

Dropzone AI

SANS | Research Program

Product Briefing

SOC with Dropzone AI:

Insights from the 2024 SANS Institute SOC Survey

July 2024

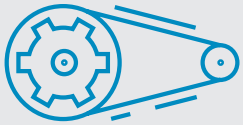
The job of the SOC gets bigger every day. The budget often does not. Attracting and retaining experienced staff is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

Dropzone AI

What if you could trust AI? That's the concept behind Dropzone AI, a SOC tool that emulates the work of a Tier 1 analyst, performing preliminary investigations autonomously. Created by founding engineers from top tech companies, Dropzone AI helps under-resourced security operations teams reduce their mean time to disposition (MTTD) and generate prioritized reports for human analysts.

The technology gives SOCs a tool to automate and orchestrate incident triage and reporting—just the sort of thing respondents to the SANS SOC Survey say is one of their biggest challenges. Dropzone AI delivers findings and recommends mitigation steps, but doesn't take action on its own, because human review still matters. SOC Survey respondents said they are struggling with inadequate staffing, and Dropzone AI eases the load on analysts with dependable, pretrained AI, using a patented large language model. Dropzone AI's systems is pretrained on security, with guardrails to prevent alerts based on false information. It knows what steps a human analyst would take, and consolidates inputs from various information sources in various formats to create actionable reporting.

Key Findings



The survey highlighted that the lack of automation and orchestration is the biggest barrier in SOCs, with 71 responses out of 388 noting this issue. Dropzone AI's autonomous SOC analyst directly addresses this challenge by automating repetitive and time-consuming SOC tasks. This not only reduces the need for high staffing levels but also helps bridge the gap caused by a lack of skilled staff. By handling routine tasks, Dropzone AI allows your team to focus on more complex and strategic issues, enhancing overall SOC efficiency.

AI/ML technologies received lower satisfaction scores, with "Analysis: AI or machine learning" GPA dropping from 2.17 to 1.99 from 2023 to 2024. While there is general dissatisfaction with AI/ML technologies because they simply don't work, Dropzone AI disrupts current technologies. This is because our approach focuses on practical, real-world applications that directly improve SOC operations. Dropzone AI's autonomous SOC analyst is designed to deliver tangible improvements in efficiency and effectiveness, addressing the pain points highlighted by the survey.

High staffing requirements and a lack of skilled staff are significant barriers, with combined responses indicating this as the top issue. By automating routine SOC tasks, Dropzone AI helps reduce the manual workload, easing staffing pressures. This allows your team to focus on higher-value tasks, which can lead to increased job satisfaction and better retention rates. The job of the SOC gets bigger every day. The budget often does not. Attracting and retaining experienced staff is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

Dropzone AI is easy to integrate, and takes less than an hour to adapt itself to your Environment—SIEM, EDR, firewalls, and so forth, as well as other security products that may be deployed. No need to write custom code, generate configurations, or create playbooks. It tests connections so it knows where to get data, then begins programmatically investigating everything it finds in the environment. The system also eliminates false positives by detecting whether a given piece of evidence actually poses a threat to the environment. For example, if nothing in your environment uses the log4j logging library, then the log4j vulnerability doesn't need to take up your analysts' time. See Figure1.

Investigation reports from Dropzone AI are easy to scan and understand, prioritized by severity, with an executive summary and recommended mitigation steps. Because many organizations are making do with less experienced analysts, and because everyone benefits when analysts learn, Dropzone AI also has a natural language chatbot. See Figure 2.

Analysts can ask questions in ordinary language and receive reliable answers, with links to further resources to create deeper understanding. Dropzone AI learns as well, from the feedback and context it gains as it spends time monitoring your environment. The longer you use it, the more time it saves your SOC.

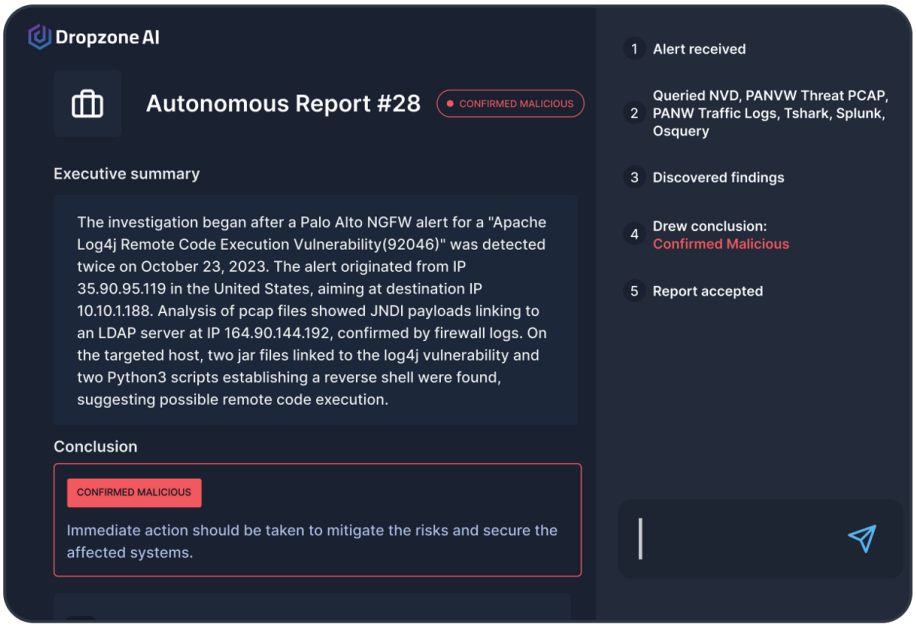


Figure 1. Example of Investigation Report Summary

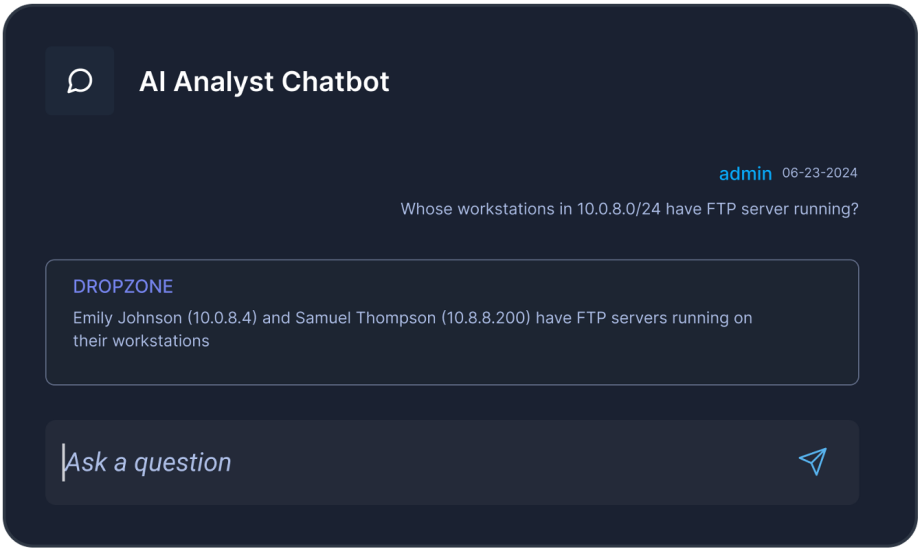


Figure 2. Dropzone's Natural Language Chatbot

If you're looking for a system to help you manage staffing challenges in the SOC, visit **https://www.dropzone.ai**

infoblox

SANS | Research Program

Product Briefing

SOC with Infoblox:

Insights from the 2024 SANS Institute SOC Survey

July 2024

The job of the SOC gets bigger every day. The budget often does not. Attracting and retaining experienced staff is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

Infoblox

Over the years, the annual SANS SOC Survey has shown steady growth in the use of DNS for passive monitoring as well as a more proactive defense through DNS firewalls and DNS security solutions. With so many tools focused on scanning traffic for malware, leveraging DNS allows organizations to monitor this foundational protocol to identify known threats and behavioral indicators of threat activity that go unseen by other defenses. This is where the Infoblox security offering sits, giving the SOC truly layered defenses instead of just deploying another malware scanner at another point in the attack chain.

The effectiveness of using DNS for more proactive security was noted by the NSA, which reported that 92% of malware and botnet activity could be blocked at the DNS layer. And, in a world where more than just laptops and servers connect to our networks, this becomes even more important as every endpoint, every robotic arm, every conference-room TV, every security camera, and every IoT device needs DNS. As a result, Infoblox can see and block threat activity that EDR, gateways, and other security tools miss. This is the enterprise-wide visibility survey respondents said they were looking for. Taking control of DNS can even provide greater visibility and control across multicloud environments.

Key Findings

When asked, "What is the greatest challenge (barrier) with regard to full utilization of your SOC capabilities?" the SANS 2024 SOC Survey identified the top three areas as:

Lack of automation and orchestration

Staffing: "High staffing requirements" and a "Lack of skilled staff"

Lack of enterprise-wide visibility

Even at the most basic level, the Infoblox BloxOne® Threat Defense solution immediately helps address some of these SOC efficiency challenges by reducing alerts and easing the burden on SOC staff. When analysts must wade through so many alerts, they face fatigue and burnout, which can prevent them from spotting the ones that spell real trouble. It's one reason many of the SANS SOC Survey respondents called out their need for better automation and orchestration, and why SOC staffing—especially retention of experienced analysts—is a perennial problem. By detecting threats at the DNS layer and blocking threat activity before it reaches other tools, the total number of alerts can drop dramatically, reducing staff stress and burnout.

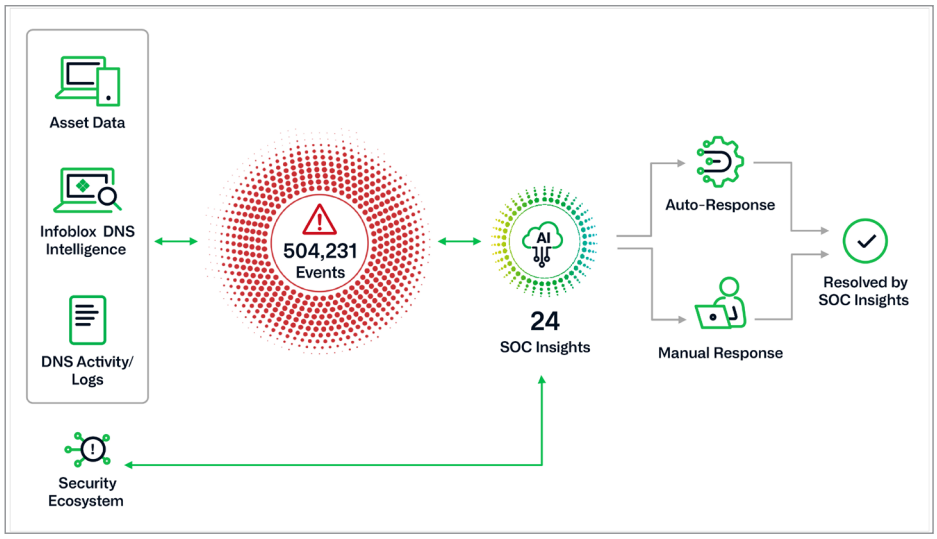


Figure 1. Events Distilled into Actionable Insights via SOC Insights

SOC Insights, an AI-driven analytic feature of BloxOne Threat Defense, mines mountains of network, event, and DNS threat intelligence to reduce hundreds of thousands of alerts into a handful of "insights" helping analysts to quickly focus on what matters most. This broader analysis of enterprise-wide data also allows Infoblox to identify threats when the individual components of the attack appear innocent and benign until their behavior is assessed as a whole.

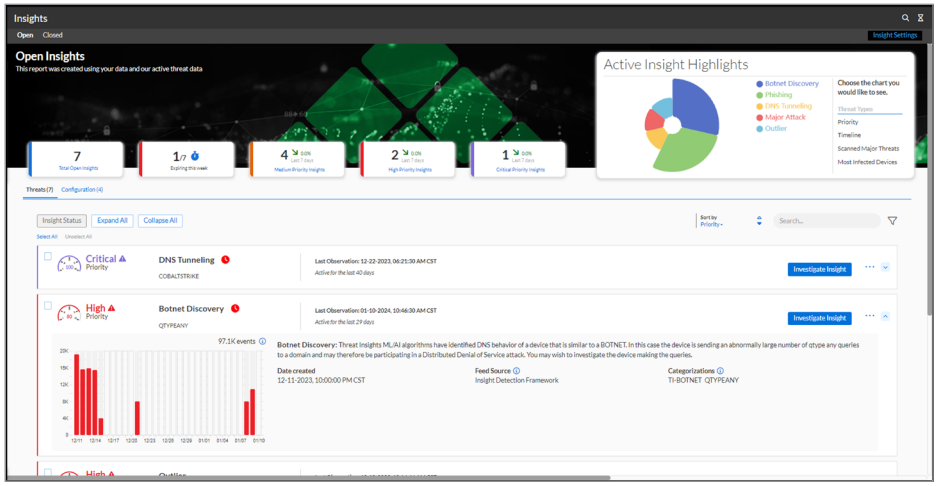


Figure 2. SOC Insights Summary Page

Infoblox BloxOne Threat Defense offers the SOC an integrated set of features ranging from threat research portals that reduce investigation times by two-thrids to unique lookalike domain detection and management capabilities they lack today. Many SOC analysts using this unique offering find it reduces stress and helps them feel more confident that they're making good decisions and not missing important threats. SOC leadership finds that this, in turn, helps with employee satisfaction and retention.

If you're looking for added confidence, time-saving automation, and greater overall efficiency for your SOC, visit **www.infoblox.com**

RadiantSecurity

SANS | Research Program

Product Briefing

SOC with Radiant Security:

Insights from the 2024 SANS Institute SOC Survey

July 2024

The job of the SOC gets bigger every day. The budget often does not. Attracting and retaining experienced staff is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

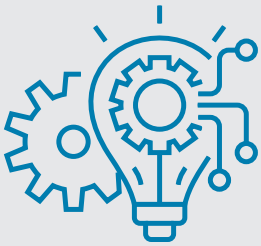
Radiant Security

Radiant supplements your staff with AI SOC analysts, trained on the choices and thought processes of experienced humans. They do 80 to 90 percent of the work of a Tier 1 human analyst – threat detection, triage, investigation, and even response.

It's a big step forward from standard solutions, because Radiant AI is trained to ask questions and make decisions the way a human analyst does. It picks up a lot of the load of triage and investigation – work that many SOCs do in a time-consuming, manual way.

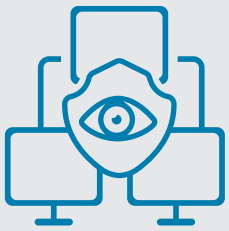
While some organizations use SOAR for response, the SANS SOC Survey shows that most analysts who have SOAR don't find it that valuable. Part of that is because it's hard to speed up resolutions using SOAR when the middle part of the process – triage and investigation – is still being done slowly. Radiant can do a lot of response actions, but it also does a lot of the thinking that the analyst might normally expend on a given event. That saves time through the entire incident flow. See Figure 1, on the next page.

Key Findings



Lack of automation and orchestration is a significant problem reported by respondents to the SANS SOC Survey.

Staffing issues – high staffing requirements and lack of skilled staff – are the top barrier SOC teams face.



Increasingly, SOC teams are automating threat hunting activities.

If you investigated every alert, you'd need a huge and expensive team, and you'd wind up finding a lot of false positives. SOC specialists know that, and they know how to spot the events that are really worth investigating. Radiant's AI knows that, too, and surfaces only the meaningful alerts to the humans on the SOC team. The Radiant dashboard shows alerts in a decision-ready form, with response plans already mapped out. It saves time and preserves your SOC analysts' energy for the really gnarly problems.

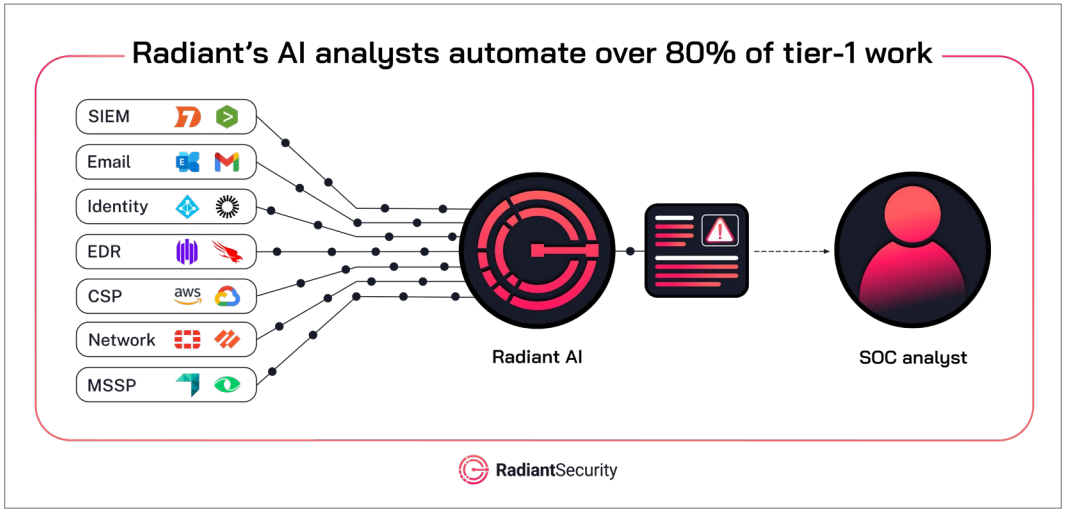


Figure 1. Security Alert Flow Using an AI Analyst for Investigation

Of course, the question on everyone's mind when it comes to AI is "How do you know it's accurate?" Radiant employs state-of-the-art machine learning and data science techniques to protect against hallucinations. The system validates both inputs and outputs.Radiant takes a "human in the loop" approach where a security team regularly reviews the system output and tuning the AI models to ensure accurate, repeatable results.

The training of an AI SOC analyst includes everything you wish all human analysts knew. It starts with security tools and telemetry, then moves on to learning what normal behavior is in an organization, plus investigation tools and techniques. It also incorporates security industry knowledge bases and stays up to date with the latest threats. All that happens before you deploy Radiant.

Respondents to the SANS SOC Survey were clear that they needed their software to provide more automation and orchestration. One reason SOAR is not widely loved is that it causes a lot of overhead for the SOC team in the form of long implementation times and engineering overhead. Another time-saver for your hard-working SOC team: Radiant is quick to deploy and easy to integrate with your existing systems. Unlike other systems that require time-consuming playbooks and hand-coded integrations, Radiant just works.

Radiant detects signs of trouble across your existing systems, bringing together disparate sources of information, and delivers decision-ready results within three minutes – a report with an investigation summary (and links to evidence), a root cause analysis, and an incident-specific response plan. You choose whether it provides instructions for the response, a one-click (semi-automated) response plan, or fully automated response.

If you're ready to take your SOC to the next level, visit
https://radiantsecurity.ai

SWIMLANE

SANS | Research Program

Product Briefing

Security Operations with Swimlane:

Insights from the 2024 SANS Institute SOC Survey

July 2024

The job of the SOC gets bigger every day. The budget often does not. Staffing is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

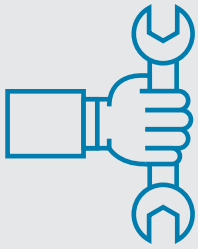
Swimlane

Swimlane's guiding principle is to empower SOC teams through AI-enhanced automation that serves as the system of record for any environment, use case, or stakeholder. They believe that if you invest in quality security automation, you'll improve the barriers to successful security operations that protect the organization without burning out its people.

Its security automation platform goes beyond the SOC to help all parts of the security operation accomplish more with less. By bringing information into a central repository, Swimlane helps tear down silos between the SOC and operations teams.

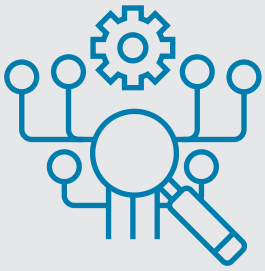
Swimlane provides a cloud-native and low-code solution to manage incidents and cases collaboratively with inputs from all sources, not just the standard stack of cybersecurity tools. This level of orchestration enables infinite integrations that facilitate the monitoring of identities, access, permissions, and data, all at the same time. From a single pane in Swimlane Turbine, an analyst can run queries, automate remediation steps, and conduct investigations – even collaborate with others in Teams and Slack conversations.

Key Findings



Lack of automation and orchestration is the single most reported problem by respondents to the SANS SOC Survey.

Staffing issues – high staffing requirements and lack of skilled staff combined – are the top barrier SOC teams face.



Another barrier is lack of enterprise-wide visibility into the SOC operation.

SANS SOC Survey respondents were clear: SOC teams need more automation and orchestration capabilities and better-trained staff to accomplish their goals. Yet many times, budgets won't stretch and the right candidates aren't available. With Swimlane Turbine, an organization can train a new SOC analyst in a couple of weeks, instead of spending months on the underlying tools.

Turbine saves time in the onboarding phase, so the new person becomes an asset more quickly. With the time saved, that person can now train to become a subject-matter expert wherever the team needs one. And that's before you add in the time saved and expertise gained from using Turbine's, robust case management application, which streamlines and standardizes incident response processes based on lessons learned and best practices.

Turbine goes well beyond the capabilities of traditional SOAR applications with its cloud-native architecture, low-code approach, robust case management, and AI-enhanced features. The priority when building Swimlane Turbine has been flexibility, scalability, and simplicity, because not only are organizations different from one another, but they're all different from what they were six months ago. Depending on your organization's needs, it can deploy in the cloud, on-premises, or in an air-gapped environment. See Figure 1.

Thanks to Canvas, Turbine's low-code playbook building studio, most of the work to deploy and build automation can be done in a no-code fashion. The beauty of low-code is that Turbine also offers SOC teams the ability to write a little quick Python code to make something work exactly how they want it to. AI-enhanced features simplify the Python scripting experience so that teams can build in Turbine without requiring master coders at every stage of the game.

Infinite integrations are available for Swimlane Turbine. This capability is the secret behind Swimlane's ability to take automation beyond the standard use cases – customers use it to automate threat hunting, vulnerability management, identity provisioning, patch management, auditing, and even compliance. If an integration is needed but not yet available, Swimlane will build it on-demand at no cost.

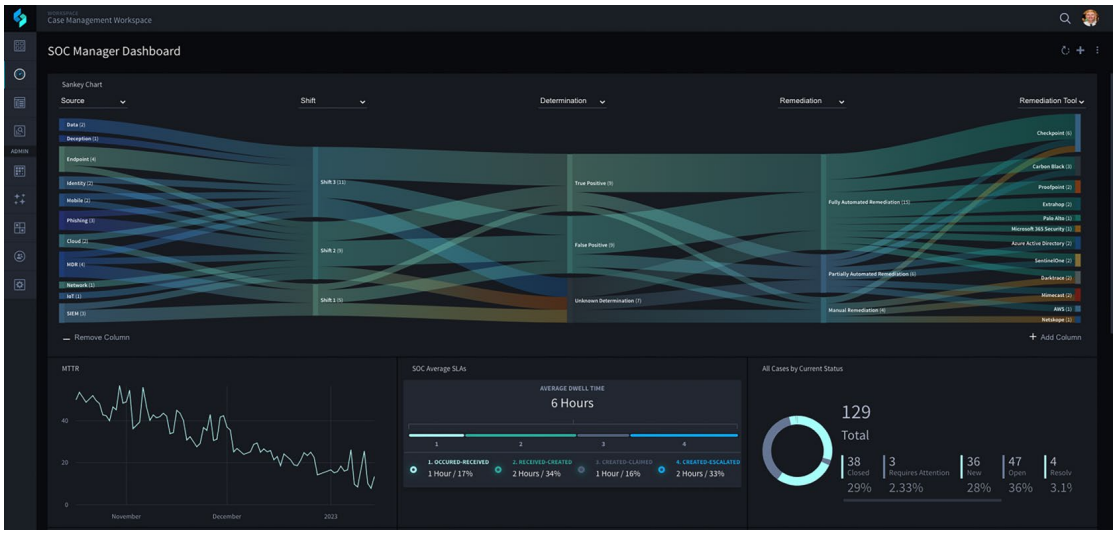


Figure 1. Swimlane Turbine SOC Manager Dashboard

Swimlane Hero AI is a collection of AI-enhanced innovations built on Swimlane's own secure large language model, available in Turbine. Features like case summarization, recommended actions, secure crafted prompts, text-to-code scripting assistants all work to make SOC teams more efficient without losing granular control by humans.

Many SANS SOC Survey respondents also noted issues with visibility into their organization's activities. Turbine provides SOC teams with seamless enterprise-wide visibility by aggregating and prioritizing all SecOps activities through robust case management, highly composable dashboards, and reporting. These visual applications help managers make good decisions and analysts work more effectively.

If you're ready to bring the power of AI-enhanced security automation to the job of making your SOC – and your whole security organization – more effective, visit **https://swimlane.com**