CYENTIA INSTITUTE

VOICE OF THE ANALYST STUDY

An Inside Perspective on Security Operations

Commissioned by respond

VOICE OF THE ANALYST STUDY

This research was commissioned by Respond Software. Respond participated in identifying research goals, but otherwise had no influence over findings shared in this report.

Respond Software redefines Security Operations with the first security expert system, the Respond Analyst. Driven by its patent-pending Probabilistic Graphics Optimization (PGO) technology, the Respond Analyst emulates the decision-making of an expert security analyst, effectively becoming a SOC team member that specializes in high-volume, low signal use cases while it applies, adapts and maintains an organization's tribal knowledge 7x24x365. Respond Software was founded by security operations veterans and world class product technologists to serve its customers across multiple industries.

Find out more: www.respond-software.com.

CYENTIA INSTITUTE

This research was independently conducted by the Cyentia Institute. Cyentia seeks to advance cybersecurity knowledge and practice through data-driven research. We curate knowledge for the community, partner with vendors to create analytical reports like this one, and help enterprises gain insight from their data.

Find out more: www.cyentia.com.

Executive Summary

The word "cybersecurity" often evokes images of hooded attackers lurking in shadows or racks of sleek-looking technologies that promise to defeat them. But it has been well-established over the years that breaches aren't simply a dice roll pitting attacker strength against technical defenses. Most security incidents, rather, stem from operational inefficiencies and failures that directly or indirectly lead to the organization being compromised. This makes security operations centers[1] (SOCs) and the analysts[2] who staff them the cornerstone upon which effective cybersecurity defenses are built.

Because of this critical role, SOCs are a common subject of security studies and whitepapers. But these efforts tend to focus on the entity itself (structure, performance, tooling, etc.) rather than the individuals who comprise it. This "Voice of the Analyst Study" is designed to do just that; we focus on the human side of the SOC to build understanding, share insights, and empower SOC teams to be the best they can be.

> "The SOC provides real-time protection for critical systems and assets, and is arguably one of the most important functions for a security organization. I'm glad to be participating in that mission."

In these pages, you'll see statistics and quotes (like the one above) from vetted analysts about what drew them to the SOC, whether those expectations have been met, and how satisfied they are in their current role. We also learn how they spend their time, and gather perspectives on common SOC activities like event monitoring, intrusion analysis, incident response and forensics, threat intelligence and hunting, and several other operational support tasks.

Using input from participants, we compare these activities along several dimensions to identify which ones are, for instance, challenging, enjoyable, and valuable vs. tedious, boring, and wasteful. We conclude the study by offering data-driven recommendations on which SOC activities offer the best "bang for the buck," which ones warrant additional investment, and which are most suitable for automated decisioning and workflow orchestration.

Thank you for your interest in this research, and our sincere thanks as well to all those who participated in it. We hope the insights you glean will be well worth the time you invested.

KEY FINDINGS

45% say reality in the SOC does not meet expectations

1 in 4 express dissatisfaction with their current job

Dissatisfaction is 25% higher among experienced analysts

30% do not feel respected by peers outside the SOC

1 in 3 are actively seeking other job opportunities

28% confess they've never stopped an intrusion or don't remember doing so

Analysts who spend the most time on event monitoring are least likely to catch intruders.

Generalists are twice as likely to claim recent detections

Hunting, forensics, intel and intrusion analysis rate favorably among analysts

Training, collaboration offer biggest bang for the buck

Event monitoring ranks high among activities that could benefit from automation

[1] We use "SOC" inclusive of traditional SOCs as well as Cyber Incident Response Teams (CIRTs) and entities of similar scope.

[2] We use "analyst" to refer to anyone working to monitor, detect, analyze, respond to, or otherwise handle security incidents.

The Respondents

Who participated in the study?

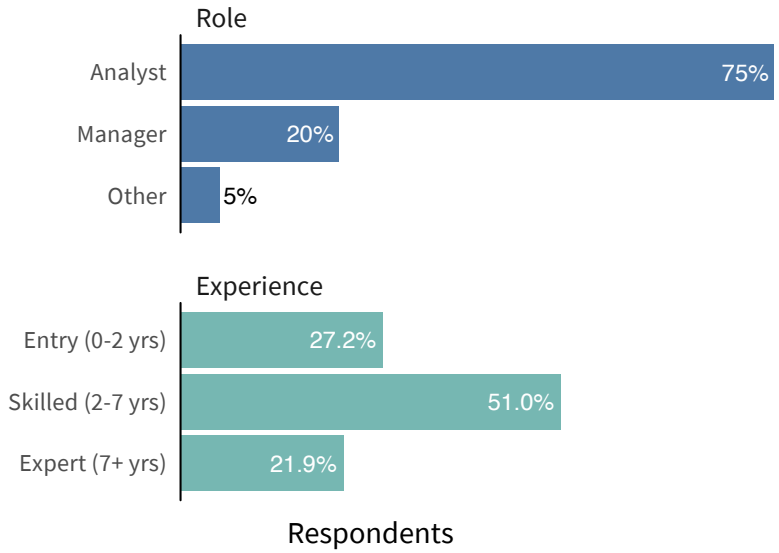
This is the "Voice of the Analyst" study, so it makes sense to begin by getting to know those who let their voice be heard. The sampling methodology used for this study is summarized below and a more detailed description can be found in Appendix A. Our goal in providing this information is not simply to describe the sample set, but to assist you in determining how well it may be representative of your organization and requirements.

Across the multiple samples comprising this study, we received 167 responses, but 7 were removed for quality reasons. Of the 160 remaining responses, 87 come from organizations that voluntarily participated as a SOC unit and 73 are qualified individuals who were invited directly. Most of these are analysts of various levels and specialties, but about 1 in 5 are SOC managers or directors. The smattering of "Other" roles includes mainly engineers and project managers working in the SOC.

Tenure looks to be an important factor in several areas of this study, and we'll call those out as we go along. For now, let's group respondents based on their amount of SOC experience. We'll label anyone with up to 2 years of experience as 'entry,' 2-7 years as 'skilled,' and those with 7 or more as 'expert.' In addition to being practically intuitive, these thresholds align perfectly with the 1st quartile (entry), 2nd and 3rd quartiles (skilled), and 4th quartile (expert) of the experience range in the dataset.

FIGURE 1

Respondent roles and experience (n=160 and n=151)



Source: Cyentia Institute

GENERAL PURPOSE

To examine the perceptions of SOC/CIRT analysts to understand their attitudes, experiences, activities, challenges, opinions, and ideas regarding their profession

TARGET POPULATION

All security operations analysts and managers currently working to monitor, detect, analyze, respond to, or otherwise handle security events and incidents.

SAMPLING METHOD

Surveys of vetted SOC staff and teams from multiple independent sources using a mix of convenience, expert, and snowball sampling techniques

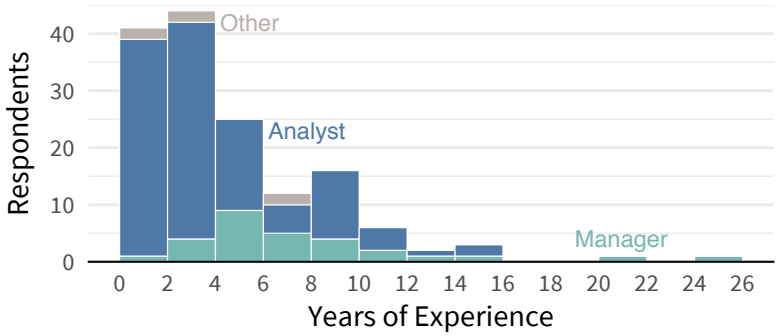
SAMPLE SIZE

160 qualified respondents of varying roles, tenures, and specialties from a wide range of internal SOCs and MSSPs

On average, respondents to this study have 5 years of experience in security operations, with the longest tenure being 25 years (median is 4). That experience, unsurprisingly, differs among analyst/responder (avg = 4.3) and manager/director (mean = 8.3) roles, as shown in Figure 2. The 'Other' category is sparse, but shows a wide range of experience as well.

FIGURE 2

Distribution of experience by respondent role (n=151)

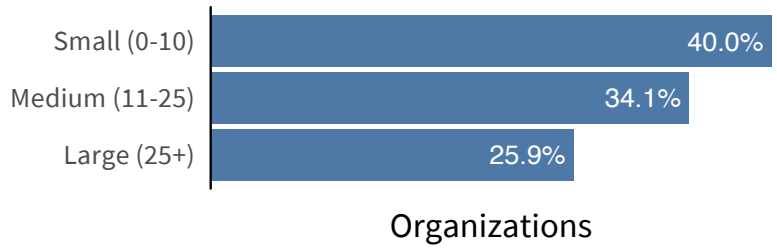


Source: Cyentia Institute

Statistics about the SOCs these respondents work in are a bit tricky, due to our sampling methods, which are explained in Appendix A. In short, we had several SOCs participate as a whole unit, meaning multiple respondents gave the same answer to questions about staffing levels, country, industry, etc. That amplifies stats for those SOCs relative to individual responses, but we adjust for that where necessary.

FIGURE 3

Size of SOC teams represented by respondents (n=85)



Source: Cyentia Institute

Respondents typically work in SOCs ranging from 10 to 20 members (median = 11), though about 10% of them report a staff of 50 or more. According to one participating SOC, the median staff of 11 may not be a coincidence because 10 plus a manager is about right for a 24x7 operation. Running 24x7 appears to be the norm among these teams (70%) according to these results. This is especially true of larger SOCs, which makes sense as more shifts require more staff.

A geographic breakdown of host countries is shown in Figure 4. About half of respondents work in a U.S. SOC, but the U.K., Netherlands, Australia, and India round out the top 5 with good representation as well. Those top countries also correspond to SOCs that participated as a unit, which boosts their share of voice.

VOICES FROM THE SOC

"SOC work is the quintessential entry-level infosec role. I took this job thinking I would learn a lot."

"I like challenges and making a difference. That can still happen in a SOC."

FIGURES 2 & 3

Respondents had a wide range of experience, with the average being 5 years. We assigned tenure labels (*entry*, *skilled*, *expert*) that you will see throughout this report .

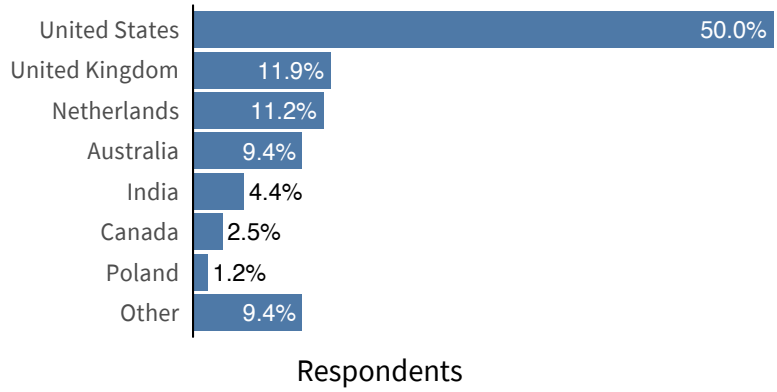
"My original motivation to work in a SOC was my desire to move from a helpdesk style role to something more challenging intellectually."

"Since school I've wanted to be in the cyber security industry. I was fascinated by attacks and how to detect them. Working in a SOC gives me this oportunity."

Moving on to the industries represented in the study, we need to first acknowledge the heavy influence of Managed Security Service Providers (MSSPs). Nearly half of all respondents work for an MSSP, which would be odd were it not for the scope of this study. In this case, it makes sense; MSSPs are major employers of SOC personnel.

FIGURE 4

Distribution of experience by respondent role (n=160)

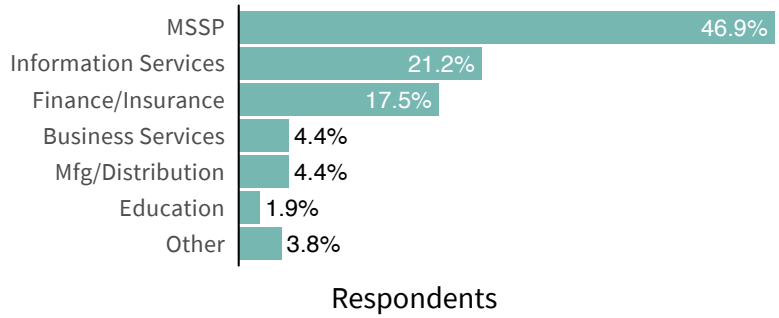


Source: Cyentia Institute

As for the other half+ of respondents, Financial Services and Telecoms are the big employers. This also seems reasonable, as organizations of these types have both deep pockets and large operations. The only other sector grabbing more than 10% share is Information Services, which includes hardware, software, and SaaS providers.

FIGURE 5

Industries represented by respondents (n=160)



Source: Cyentia Institute

"Knowing that you're relied upon by customers for the safekeeping of their network and business critical systems makes the job feel worth it."

"Information security is an exciting field with great career growth opportunities. A SOC analyst is a way to get started in this industry."

"I really enjoy how close I can be to technology while working in a SOC. I can make it my job to learn new things and try new technologies."

"I just kind of fell into it. Afterward, the analytical work became appealing."

FIGURE 5

Nearly half of respondents work in SOCs for MSSPs. Another large proportion work in Financial and Information Services firms.

"My secops career started as a consultant. Expectations were to catch bad guys, but over the years I realized that most incidents could have been avoided by following basic security principles."

"Find evil; stop badness."

Views from the SOC

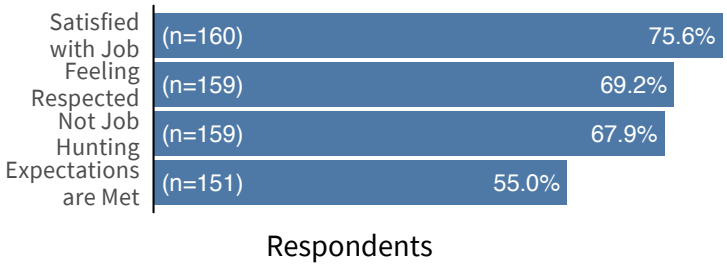
How do analysts view their work?

Beyond describing analysts and their organizations, we wanted to gauge attitudes and perspectives to get a feel for the climate in which they work. The first introspective question we asked respondents pertained to the motivations and expectations that lead them to a role in security operations. Roughly 3 out of 4 point to a desire for more intellectually challenging work, the chance to learn new skills, and/or a chance to defend and help the business. Job security, flexibility, and growth opportunities also drew many into the SOC.

When asked if the reality in the SOC met those expectations, roughly half responded in the affirmative. Another one-third are on the fence, while fewer than 10% express unmet expectations. Not surprisingly, reasons given among those with unmet expectations hark back to the same dreams and drivers mentioned in the preceding paragraph. In many cases, these dreams weren't violently dashed to pieces, as much as they were ground down over time by various elements and forces.

FIGURE 6

Respondent perspectives on job satisfaction, respect, retention, and expectations



Source: Cyentia Institute

The fact that SOC life mostly meets expectations does not necessarily equate to satisfaction among those living it, which is why we asked about that next. The answers we received show a 3-to-1 split between analysts on the "satisfied" and "unsatisfied" sides of the spectrum. Once again, many respondents pointed to the very same unrealized expectations cited above as the root of their dissatisfaction. "Better compensation," "clear career path," "more support/training," "bigger budgets/staff," "less tedium," and "greater freedom/range of duties" were all common suggestions for improving morale in the SOC.

"In my opinion, a lot of satisfaction and respect is about a feeling of 'am I making a difference?' and 'do those around me care about what we're doing?'"

"Most outside the SOC are unaware of what we do."

"I've found quality analysts are better recognized as cybersecurity gains priority - though this depends a lot on organizational culture."

"I was drawn to the SOC by misguided youthful ideals, which have been ground into a fine powder by years of poor management and lack of support from higher-ups."

"The SOC's achievements are highlighted by upper management, illustrating their value and impact on the organization."

So people working in an SOC do not appear to be an entirely unsatisfied lot, but do they feel respected by those outside the SOC? For the most part, our findings suggest they do—less than a third say they get little or no respect. We did notice, however, that respondents in the 'Other' job role (mostly engineers and project managers) may have a different take on that. Only one of them reports feeling respected by other staff. We're wary of making a big deal of such a small sample, but it does agree with experience. And even if we're wrong, it can't hurt to buy them a cup of coffee, hear their ideas, and make them feel part of the team, can it?

The picture painted by the results above is not one of SOC staff hating their jobs and aching to jump ship. So it may surprise you to know that almost 1 in 3 respondents say they are actively hunting for other jobs. Given that, we can't help but think that even more are open to interesting opportunities and/or better offers.

This seems to suggest that negative factors are not the only reason analysts explore the job market. The same "positive" reasons that lead them to the SOC in the first place (e.g. new challenges, broadening/ sharpening skills, better compensation, a chance to make a difference) are the ones that will lead them to another role in another SOC. If you want to keep them around, offering those same positives in-house is just as important as eliminating the negatives that drive them out.

"Other teams act annoyed when the SOC needs help from them to investigate or resolve an incident."

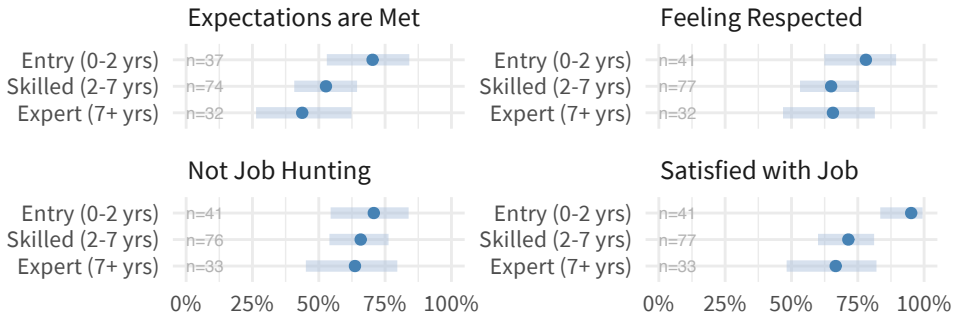
"I'd appreciate not being punished or laughed at for not knowing something."

The Lens of Experience

Do the attitudes discussed above change with experience? That's the question behind Figure 7, but unfortunately the answer isn't exactly clear. For instance, consider the chart in the upper left comparing the percentage of met expectations across the 3 experience levels. The views of entry-level analysts (70%) seem to differ substantially from those of experts (43%), but the overlapping confidence intervals caution against assuming that the difference is statistically significant[3]. The most we can say is that we have some evidence here suggesting the expectation vs reality gap *may* widen with experience.

FIGURE 7

Effect of experience on respondent perspectives



Source: Cyentia Institute

The effect of experience on perceptions of respect appears even less compelling than it does for expectations. And there's virtually no difference between tenure groups in terms of their interest in the job market. The chart on job satisfaction, however, points to entry-level staff being happier with their lot in life. Some may find that surprising, since level 1 SOC roles are often described as "grunt work." Respondent comments reveal that many entry-level analysts view their role as a) an improvement over what they were doing previously and b) a chance to get their feet wet in the field of cybersecurity. One 'skilled' analyst offers a clue to the eroding satisfaction seen in Figure 7 "*This is something I'm very interested in but the career and progression have not gone to plan.*" We suspect that sentiment is not restricted to participants of this study.

[3] *For more information on confidence intervals and why we show them, see this blog post (http://cyentia.com/2018/01/07/confidence-intervals/).*

Activities in the SOC

How do SOC analysts spend their time?

Now that we understand more about how analysts view their work, let's examine how they do their work. We talked to experts and reviewed literature to identify the 12 SOC activities listed in Table 1. This is not an exhaustive list, nor is it applicable in its entirety to all organizations, but we believe it provides a good representation of common SOC functions.

TABLE 1

Common SOC Activities Examined in This Study

Activity	Label	Description
Daily shift operations	**Shift ops**	Tracking shift logs, shift turnover, burnout recovery, problem and change control, etc.
Real-time monitoring and triage	**Monitoring**	Monitoring ticket and event queues, triaging and classifying events, closing out tickets, escalating potential incidents, etc.
Event and Intrusion analysis	**Intrusion**	In-depth analysis of potential intrusions, information and artifact fusion, recommendations for further action, etc.
Incident response and remediation	**Response**	Responding to a confirmed incident to determine extent, contain exposure, remediate effects, and facilitate full recovery.
Forensic and malware analysis	**Forensics**	Collecting/analyzing digital evidence, artifacts, implants, malware, etc.
Threat intelligence and research	**Intel**	Collecting and analyzing the motivations, intent, capabilities, TTPs, indicators, and activities of threat actors.
Advanced threat hunting	**Hunting**	Proactively searching across networks and systems to identify signs of advanced, subtle, and/or evasive threats.
Collaboration and coordination	**Collaboration**	Working with other internal and external teams in support of SOC activities (e.g. law enforcement, intel sharing groups, notifying stakeholders or affected parties, etc.).
Reporting and documentation	**Reporting**	Includes analyst comments, case building, incident reports, management presentations, SOC metrics, etc.
Tool and content management	**Tools**	Tuning sensors, signature creation, developing use cases, prepping IOCs, maintaining tools, etc.
Proactive security operations	**Proactive**	Network mapping, vulnerability scanning, penetration testing, security assessments, configuring controls, etc.
Awareness, training and mentoring	**Training**	Keeping up with security news, research blogs and reports, attending training sessions, mentoring junior analysts/responders, etc.

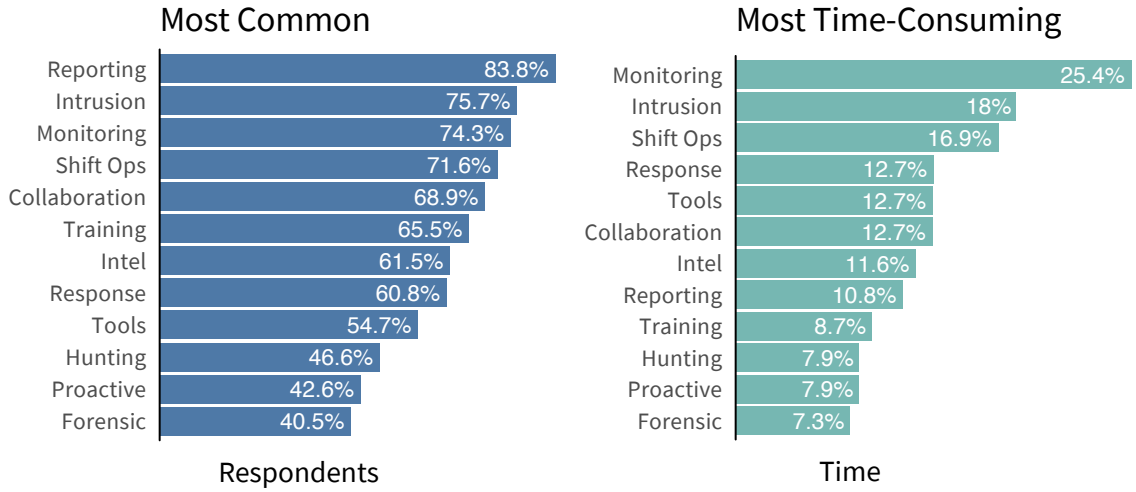
The question of how analysts spend their time across the activities in Table 1 can be studied in two dimensions. The first concerns which activities are the most common and the second which are most time-consuming. Figure 8 depicts both.

The "Most Common" side of the chart (left) shows the percentage of respondents who reported doing that activity (time = >0%). Of the top four, two can be looked at as core responsibilities of Tier 1 and Tier 2 analysts (Monitoring, Intrusion) and two can be looked at as "just part of the job" regardless of role (Reporting, Shift Ops). The more specialized SOC/CIRT functions appear at the bottom of the list, because they're often outsourced or done only by a subset of staff.

The “Most Time-Consuming” side of Figure 8 lists the average (mean) time spent on each activity among those who report doing it. The ordering isn’t hugely different from the left-hand chart, but it does offer a view that is perhaps more in line with how you’d expect SOCs to spend their time.

FIGURE 7

Effect of experience on respondent perspectives (n=160)



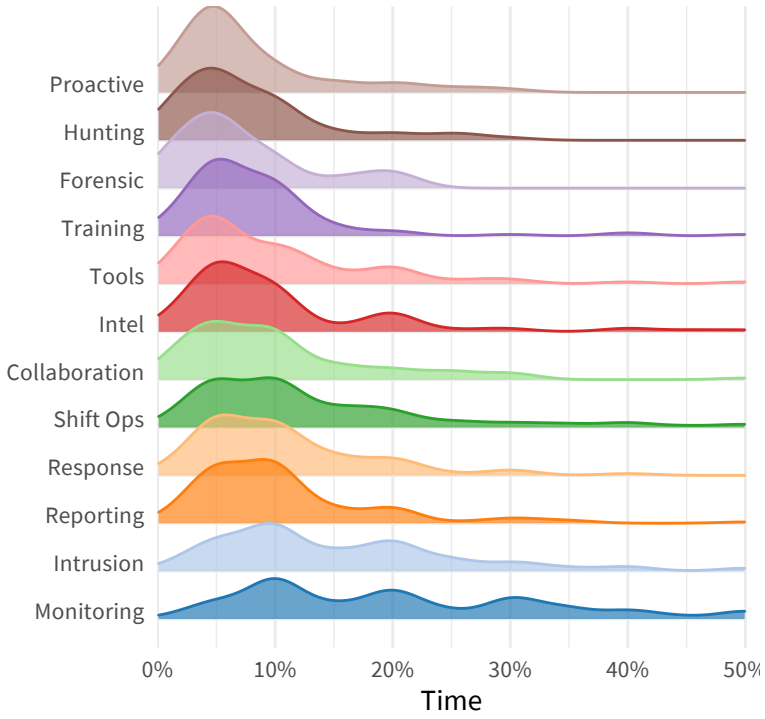
Source: Cyentia Institute

If the numbers on the right seem low, you’re not alone. We asked respondents to allocate a percentage of their time across the 12 activities based on a typical work week or month, and this may have caused an artificial balancing effect. Overall, we suspect what is shown reflects more accuracy in the ordering rather than precision in the stats.

Even assuming a precise measurement, not everyone spends exactly 25.4% of their time on real-time monitoring and triage; that’s just an average. Figure 9 illustrates the distribution of time spent on activities and, especially for monitoring, the variation around the mean is quite high.

FIGURE 8

Distribution of respondent time spent on SOC activities (n=148)



Source: Cyentia Institute

“No one is an expert in this field. Just learn and do new things everyday.”

“I’d like to be able to spend less time reviewing the ‘same old’ events. We’re moving in that direction, and have already improved alot.”

“Neural implants would be nice. There are not enough hours in the day to do all the research on all the things.”

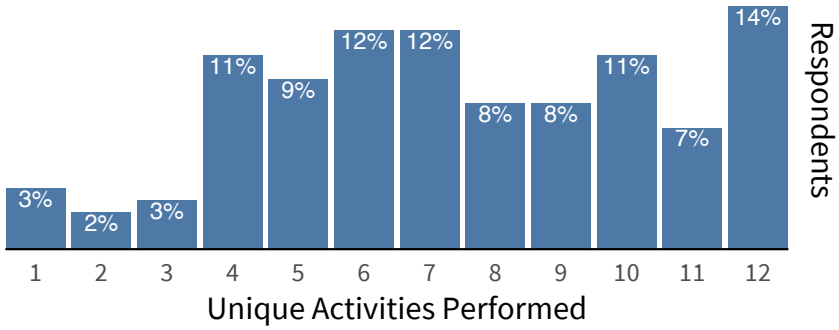
Generalists vs Specialists

Knowing which SOC activities are most common and time-consuming is certainly interesting, but it doesn't really show us what a typical analyst's day looks like. How many hats do they wear? Do they wear them equally? These kinds of questions lead naturally to the notion of generalists vs specialists.

Let's start that discussion by examining the number of activities juggled by SOC personnel. Figure 10 reveals that most have more than three balls in the air, and just shy of one-third handle at least 10. If that sounds like a lot—it is! Welcome to secops, where dropping balls because "that one's not mine" isn't an option. Also keep in mind that several of these activities deal with standard tasks like documentation and shift operations that pretty much everyone does to some extent.

FIGURE 10

Number of unique activities performed by respondents (n=148)

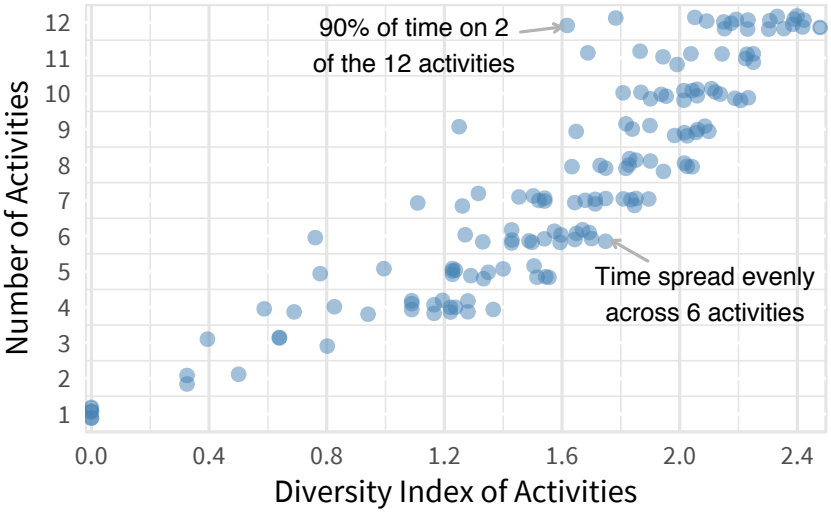


Source: Cyentia Institute

If we define generalists as those whose time is spread across many different activities listed in Table 1, Shannon's Diversity Index is an appropriate measure for this. A higher index value means more activities, with time spread more equally across those activities. Figure 11 plots all respondents according to their activity diversity index (x) and number of activities performed (y).

FIGURE 11

Measure of activity diversity scores among respondents (n=148)



Source: Cyentia Institute

"We need to do more host investigations, malware reverse engineering, and cyber hunting."

"I try to never have the same day twice. I enjoy the challenge of always learning new things and expanding my professional skills."

"Expectation: It would be challenging and a chance to do the 'fun' work without having to 'fix' the problems. Reality: It's all that but also a lot of the 'same-thing-over-again' activity."

"We need less load and more time to analyze incidents and work on processes."

FIGURE 11

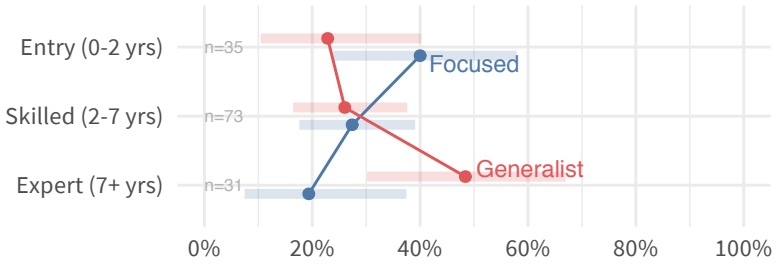
With a measure of activity diversity for each analyst, we can distinguish between generalists (do many activities) and those with more narrowly focused responsibilities.

For example, the analyst represented by the point in the upper right (12 activities, 2.47 task diversity) reports spending 12% of their time on intrusion analysis and 8% on each of the 11 other activities. We've annotated a few more examples in Figure 11 to give a sense of what we're doing here.

With a measure of activity diversity for each respondent, we can begin to distinguish between those who are generalists (do many activities) and specialists (focus on fewer activities). We're going to apply the 'generalist' label to the upper third of activity diversity scores and use 'focused' (rather than 'specialist'[4]) to refer to the lower third. Now we're able to compare generalist and focused SOC staff based on their experience, in Figure 12.

FIGURE 12

Effect of experience on activity diversity in the SOC



Source: Cyentia Institute

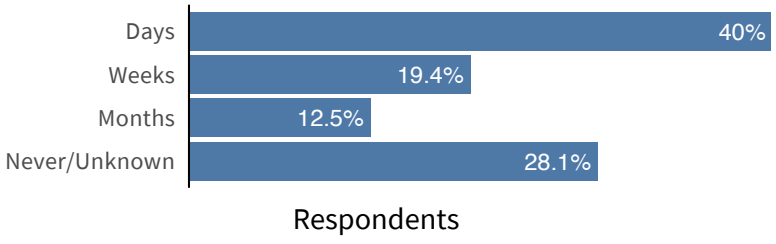
The chart provides some evidence that experts are more likely to generalize across many activities, while entry-level team members focus on a few. That's not always the case, of course (and note the overlapping confidence intervals), but the chart suggests the typical career path in the SOC is wearing more hats over time (or juggling more balls, if you prefer). The entry-level analyst who spends most of their time on real-time monitoring, then begins racking up skills, experience, and insight, and eventually becomes the got-to person for everything is the prototypical example of what we see in Figure 12.

Catching Intruders

In addition to asking analysts about how they spend their time in the SOC, we posed a simple question to learn about the fruit of those labors. We asked, "*When was the last time your efforts tangibly led to catching/stopping an intruder?*[5]", and tallied responses in Figure 13.

FIGURE 13

Amount of time since respondents last caught an intruder (n=156)



Source: Cyentia Institute

"The majority of events require very little security knowledge. Some require a decent amount, and the odd one requires quite a bit."

FIGURE 12

The chart provides some evidence that experts are more likely to generalize across many activities, while entry-level team members focus on a few.

"I don't think management and operations really understand the job or the mission, and it's too interrupt-driven. There is a reactive feel instead of a proactive strategy."

"It's hard to say when I last caught an intrusion. I don't have visibility into customer network configuration. I can only provide them analysis and recommendations."

[4] Though technically accurate, we find the term "specialist" a misleading here, and we have chosen to label those who spend most of their time on relatively few activities as "focused."

[5] We would have loved to ask about probabilities, annualized frequencies, etc., but people generally struggle with such estimates, especially without calibration. This keeps it simple.

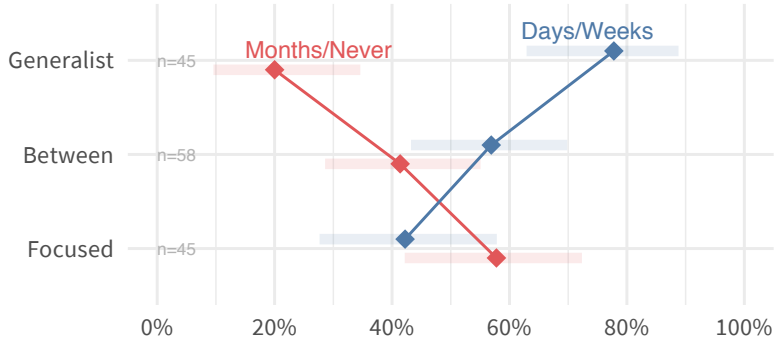
Readers used to the lengthy time-to-detction stats from Verizon's Data Breach Investigations Report may find Figure 13 a welcome sight. But keep in mind that report focuses on confirmed data breaches rather than attacks successfully thwarted by defenders. We'd expect SOC teams to be squashing baddies on a regular basis. Figure 13 suggests that may be a daily event for just shy of 40% of respondents. Another 20% of respondents say it's been weeks since they stopped an intrusion and around 13% fall in that infamous DBIR-esque "months" zone.

But the real story here lies with the 28% who say their efforts have never led to stopping an intruder or don't remember the last time that happened. It's tempting to chalk this up to a lack of experience, but the differences between entry-level analysts (54%) and experts (69%) who report recent stoppages fall within the margin of error.

What about the generalist vs. focused distinction—could that shed some light on what's happening in the Never/Don't remember area of Figure 13? According to Figure 14, that notion may have some legs. The percentage of generalists who say it's been a long time since they last stopped an intruder is ⅓ that of staff with more focused responsibilities. Generalists are also twice as likely to claim recent detections.

FIGURE 14

Effect of activity diversity on intruder detection timeframes.



Source: Cyentia Institute

So an analyst's range of activities or responsibilities seems to be a more important factor in recently catching bad guys than pure experience[6]. Ok; where does that leave us? This finding may be related related to the traditional structure of the SOC, where lower-level, triage-focused analysts escalate potential issues to more broadly-skilled peers. A recent DarkReading article[7] titled "*Death of the Tier 1 SOC Analyst*" agrees with this explanation.

The article essentially argues that the combined pressures of emerging technologies, alert overload, and talent shortages are squeezing out entry-level SOC positions that are traditionally saddled with the inefficient and error-prone task of triaging the overwhelming flood of inbound threats. That's not to say entry-level positions in the SOC are going away—they're simply evolving into a different form that will be less shackled to narrowly-scoped, tedious responsibilities. In other words, they're becoming more generalist in nature, and Figure 14 suggests that could be a very positive trend for all involved.

"We just ticket potentially unwanted programs/apps and haven't properly tuned signatures, so we are ticket monkeys instead of hunting."

"Sometimes we lose vision of incidents we have reported to our CERT. We could be stronger by informing each other of successes achieved."

FIGURE 14

Generalists are twice as likely to claim recent detections compared to staff with more narrow responsibilities.

"Every day I am able to pull metrics that show the controls I implemented are effectively stopping active attacks. Without figuring out how to quantify these aspects of my role, I would have no way of knowing if what I was doing mattered."

[6] *We're speaking generally; although there's certainly some intercorrelation here. As we showed earlier, generalists are typically more experienced as well.*

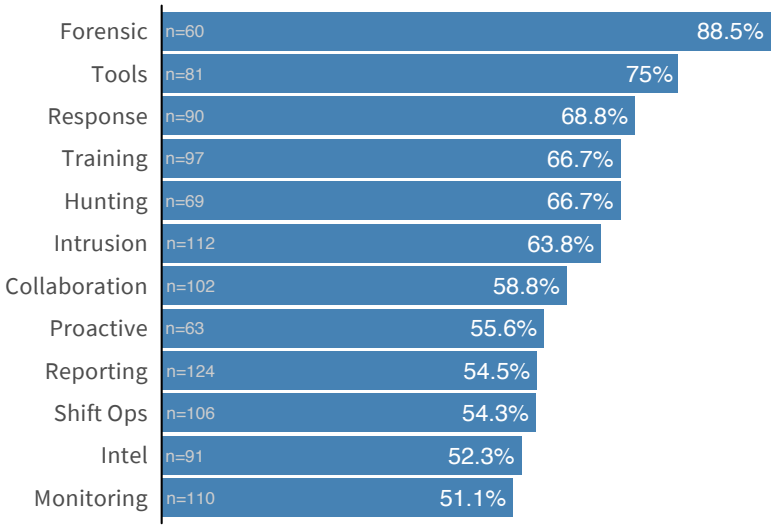
[7] *https://www.darkreading.com/analytics/death-of-the-tier-1-soc-analyst/d/d-id/1330446*

That would normally be a good note to end on, but it begs one final question. If indeed activity diversity trumps experience in terms of thwarting intruders, which activities are most/least associated with more recent stoppages? Figure 15 has the answer.

It's a little difficult to say which activities are more correlated with catching maliciousness, since many analysts do many activities. But if we look at the percentage of analysts spending an above-average amount of time on a task and then what percent of them caught an intruder within weeks or less, we get Figure 15. Of the 12 activities included in this study, forensics is the one most strongly correlated with more recent detections—though that's not really a fair comparison, because forensic analysis usually follows some hint of existing trouble.

FIGURE 15

SOC activities associated with recent intrusion detections



Source: Cyentia Institute

On the bottom side of Figure 15, monitoring is the least associated with catching intruders. If you remember that it tops the chart of most time-consuming activities shared earlier, the argument for freeing analysts of that burden really begins to gather strength.

The moral of this story seems to be that all these capabilities are necessary for a successful SOC. Ramping them up is a process that takes time and money, which makes it important to understand their relative pros and cons. We'll explore that very thing in the next section.

> **"The work we do is effective...when we aren't busy doing nonsense administrative work or so stressed out by a lack of staff that we need to go on 20 coffee/smoke breaks a night."**

"Continuous monitoring of endpoint telemetry (rather than traditional event logs or AV) and active threat hunting helps "move the needle" to stop attacks more quickly and effectively."

FIGURE 15

Among SOC activities, forensics shows the strongest correlation with recent intruder detections. Event monitoring and triage is the least correlated.

"Our tooling catches a lot of misuse but we haven't detected an active intrusion since I started here."

"I expected it would be a nonstop adrenaline rush. The reality is hours upon hours of log crawling and frustration at things that cannot be correlated."

"It is a very rewarding feeling to stop an attack."

Evaluating SOC Activities

What do analysts think about SOC functions?

Up to this point, we've explored common perspectives and activities in the SOC, as well as the effect of roles, responsibilities, and experience. But we haven't yet examined analyst attitudes toward those activities. For instance, what activities do they most/least enjoy? Which are considered most/least dynamic? What about most/least valuable? To measure these sentiments, we asked respondents to rate their activities along five dimensions using a Semantic Differential scale. The six dimensions and their contrasting 'attitudinal scale' can be seen in Table 2.

TABLE 2

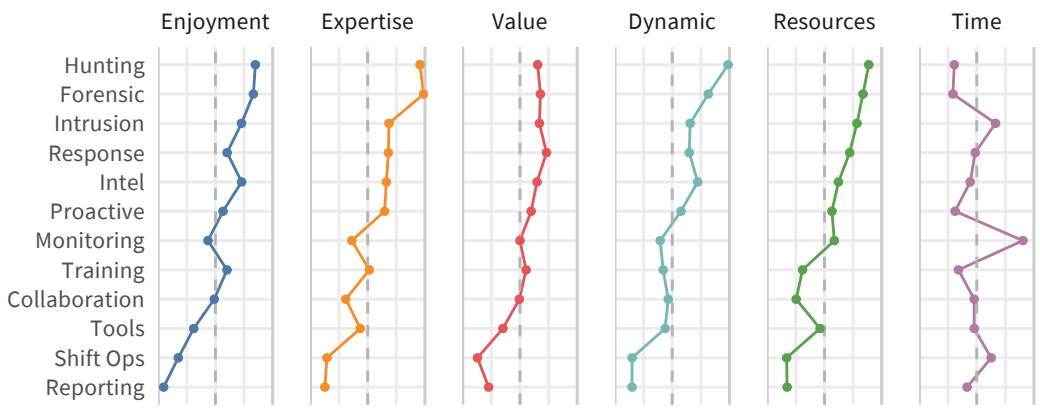
Activity Dimensions Measured in This Study

Dimension	Rating Scale	Question
Enjoyment	Hate....Love	How much do you personally ENJOY performing this activity?
Expertise	None....Extreme	What level of EXPERTISE or judgement is required to perform this activity well?
Dynamic	Never changes .... Always changes	How DYNAMIC or varied is the activity as you perform it over time?
Resources	None....Vast	What level of RESOURCES (info, tools, etc.) are required to perform this activity well?
Value	None....Huge	How much VALUE or impact does this activity have in terms of defending the organization/customers?
Time	Percent of time spent	Measured as a percent of time as seen in previous sections, but normalized to compare with other dimensions.

The outcome of this analysis can be found in Figures 16 and 17, which offer different views on the same general concept. Figure 16 is a bit more dimension-centric, making it easy to discern where activities stand relative to the mean value (dotted grey line) for each dimension. Overall, analysts view those at the top of the list more favorably across the dimensions than those at the bottom. The chart also makes it easy to spot standouts like the spike in time for monitoring relative to the other activities that meander closer to the mean.

FIGURE 16

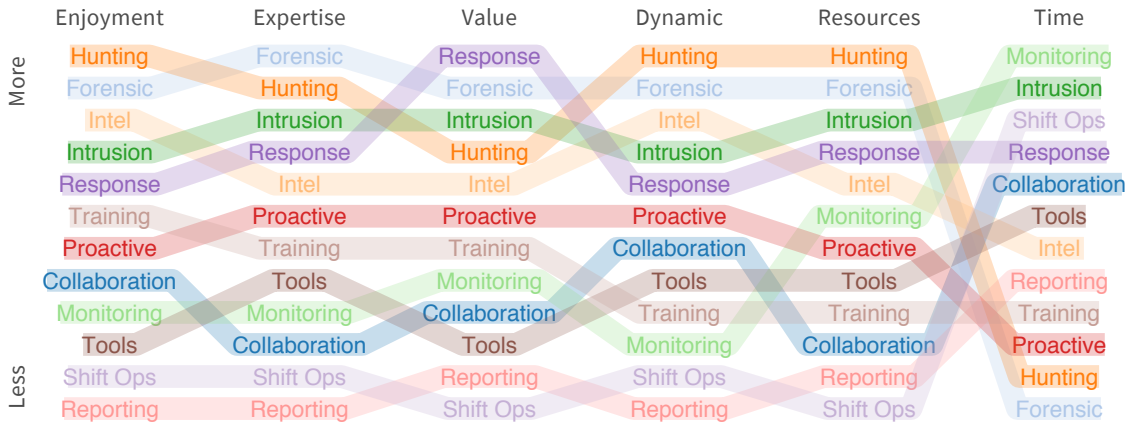
Respondent ratings of SOC activities on six dimensions



Source: Cyentia Institute

The worm chart in Figure 17 provides a complementary activity-centric view. Each column ranks the 12 activities in descending order, according to the six dimensions. The colored bands worming their way across the Figure help keep the activity perspective intact. For instance, monitoring slithers around at the bottom of the list, but climbs upward through the resources and time dimensions. This indicates respondents' view of that activity as fairly resource intensive and very time-consuming. Shocking, isn't it? On the other hand, response and forensics seem to provide excellent value compared to the resources and time invested.

FIGURE 17
Activity rankings across six perceptual dimensions



Source: Cyentia Institute

Beyond showing analyst perceptions and preferences for different activities, Figures 16 and 17 seem to suggest there may be a "pioneer, settler, planner" model within the SOC. Some people enjoy tasks that others view as boring, and those same people probably don't like the more dynamic activities. Some want to work their shift, then go home and forget about it. Others spend their evenings fiddling with their home network configuration and experimenting with various techniques. As we learned with activities, a successful SOC will incorporate all types of people and mentalities.

Activity-Dimension Associations

Following on from the last point about incident response being a good investment-to-value activity, taking a closer look at the associations among activities and dimensions may yield useful insights. We created Figure 18 to help with that. The six dimensions appear in a diagonal line connecting the upper-left and lower-right corners. On the right side of the intersection between any two dimensions, you'll find a grid that plots the 12 activities according to those dimensions. The correlation coefficient is given on the left side of those dimensional intersections, indicating the strength of relationship between them.

We admit the plots are tiny and dense, but the zoom function is your friend. Plus, there's a scalable full-size version[8] available for download if you find that easier. We'll also be showing some of the more interesting pairs in charts of their own, momentarily. For now, let's highlight a few of the stronger correlations.

Among the dimensions, the Dynamic-Expertise bond is the strongest. This means activities requiring high levels of expertise also tend to be very dynamic, which makes perfect sense. Where activities fall along that spectrum is where we're headed, but for now let's stick with the dimensional correlations. Enjoyment-Expertise and Expertise-Resources also exhibit a relatively strong correlation. Again, these are intuitive, but still a good reminder for SOC managers. Analysts enjoy tasks that challenge them and challenging tasks often require an array of human, technical, and informational resources to do effectively.

Beyond that, our advice is to treat Figure 18 like one of those old Choose Your Own Adventure books. Explore, go where you like. Find dimensional associations that interest you and then see which activities lie in the upper-right, lower-left, etc. You'll see some that are obvious and others that are less so. Note the former, ponder over the latter, and when you're ready, head to the Concluding Recommendations section, where more analysis related to Figure 18 awaits.

[8] *https://cyentia.com/wp-content/uploads/fig-18-activity-pairs.pdf*

FIGURE 18

Correlations among activity dimensions

Download [full-size version](#)[9]

The six dimensions appear in a diagonal line connecting the upper-left and lower-right corners of Figure 18. On the right side of the intersection between any two dimensions, you'll find a grid that plots the 12 activities according to those dimensions. The correlation coefficient is given on the left side of those dimensional intersections, indicating the strength of relationship between them.

We admit the plots are tiny and dense, but the zoom function is your friend. There's a scalable full-size version available for download if you find that easier. We'll also be showing some of the more interesting pairs in charts of their own, momentarily.

Source: Cyentia Institute

[9] *https://cyentia.com/wp-content/uploads/fig-18-activity-pairs.pdf*

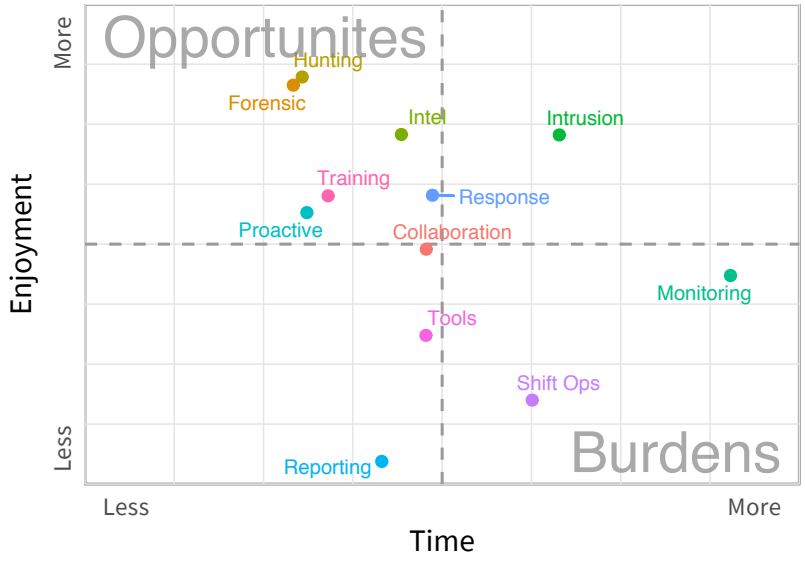
Concluding Recommendations

Most reports use the concluding section to tie a bow around the packaged document, offer a few recommendations based on key findings, and shut it down. And that's normally the tact we'd take as well. But we'd like to do things a little differently with this report because the concluding recommendations we'd like to make require yet more analysis. We've organized these under several headings, starting with activities that may help improve morale in the SOC.

Improve Satisfaction & Retention

News Flash: People like doing things they enjoy and don't like their time to be wasted. It shouldn't be a surprise that people in the SOC are no different. Figure 19 isolates the Time-Enjoyment grid from Figure 18 to help identify burdensome activities that may contribute to lower satisfaction and retention levels among analysts.

FIGURE 19
Activity alignment along the Time-Enjoyment dimensions



Source: Cyentia Institute

In the lower-right quadrant labeled "Burdens," we see that event monitoring and shift operations don't sit well with respondents. Tool and content management is pretty close, too. Of course, monitoring is a must-do function for any SOC. Daily shift operations offer a chance to retain tribal knowledge and enable smooth operational transitions.

"The concept of 'leverage' is a great way to think about impact for a given activity. To increase leverage (ROI), you can 1) reduce time invested in an activity, 2) increase impact produced from it, or 3) replace it altogether with one that's higher leverage than either prior option."

RELEVANT RESOURCE:
Presentation from Edmund Lau, "Leverage: The Key to Creating a Disproportionate Impact" View on YouTube

I'd like more advanced work to do, mentors that i could learn from...and better salary."

"I was hoping for a low stress environment with satisfaction after a day's shift. Instead, it is repeating grinding for the same false positive alerts with little opportunity for growth."

Maintaining tools is critical for well-tuned sensors and streamlined processes. All these things must be done, regardless of whether analysts enjoy them or not. But finding ways to reallocate time from these activities to those in the upper two quadrants—without sacrificing effectiveness—could be a major morale booster.

"Finding ways" is admittedly vague for a recommendation, but strategies for facilitating this 'Burdens>Opportunies' shift will be different for each SOC. Better processes and tools might help. Training may aid the transition (see the next section). Perhaps security automation and orchestration could alleviate burdens for analysts. Outsourcing lower-level, repetitive tasks so internal staff can focus more on 'opportunities' is another option.

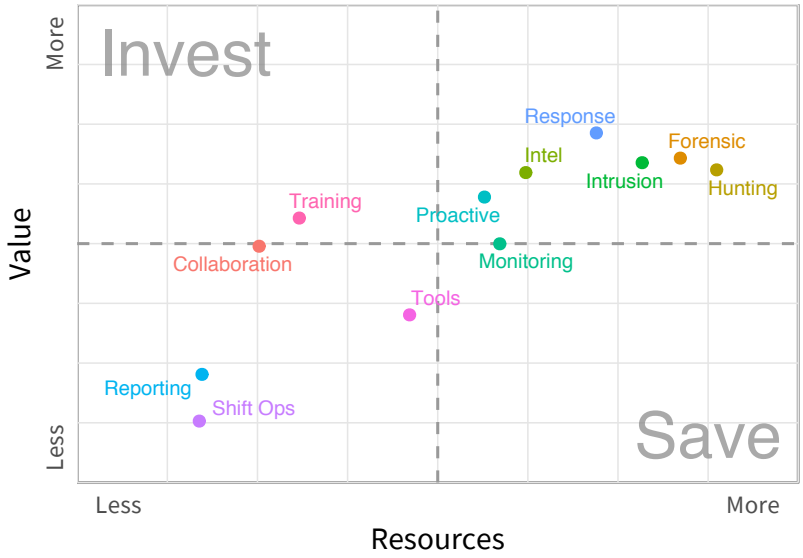
Recommendation: Free your analysts from burdensome tasks (like monitoring, shift ops, and reporting) so they can spend more time on those that drive greater enjoyment and productivity (like hunting and forensics).

Invest in People for High ROI

The next chart we'd like to pull out is the Value-Resources comparison. In theory, activities in the upper-left of Figure 20 would offer good value at comparatively low cost. The two fitting that bill are training and collaboration. If you were hoping to see some of the detection-oriented tasks to in that zone, we're sorry to disappoint. It appears those don't run cheap. But keep in mind that training your people and enabling them to collaborate are relatively low-cost ways to recoup more value from the investments you're making in those activities. It's also a great way to facilitate the 'Burdens>Opportunities' shift we discussed in the last section. Furthermore, a well-run training program is generally less expensive than relying on hiring outside experts to fill the skills gap.

FIGURE 20

Activity alignment along the Resources-Value dimensions



Source: Cyentia Institute

"Orgs that focus too much on technology and neglect their people and process are only fooling themselves. Blinky boxes will not save you, but this is a lesson that every org needs learn on their own."

RELEVANT RESOURCE:
Forbes article, "Looking To Sign A Security Rock Star? Money Isn't Everything"
View article

"The thing I want more than anything is a training budget. Technology moves fast, and security moves faster. I cannot continue to stay current and relevant without constantly learning more."

"The increased training we are receiving lately is great, but not when it comes at the expense of the number of people left in the SOC to actually keep doing the work we have to do. We either need more staff or to organize training better so less people are out of the SOC at the same time."

We see no activities in the lower-right 'No Man's Zone' of Figure 20, but monitoring strays dangerously close to that line. We've already seen that real-time monitoring and triage soak up a lot of time in the SOC, and this chart makes it clear the ROI on that time isn't great. Thus, finding ways to reduce the resource drain of monitoring while retaining or even improving its value seems like a sound bet. More on that below.

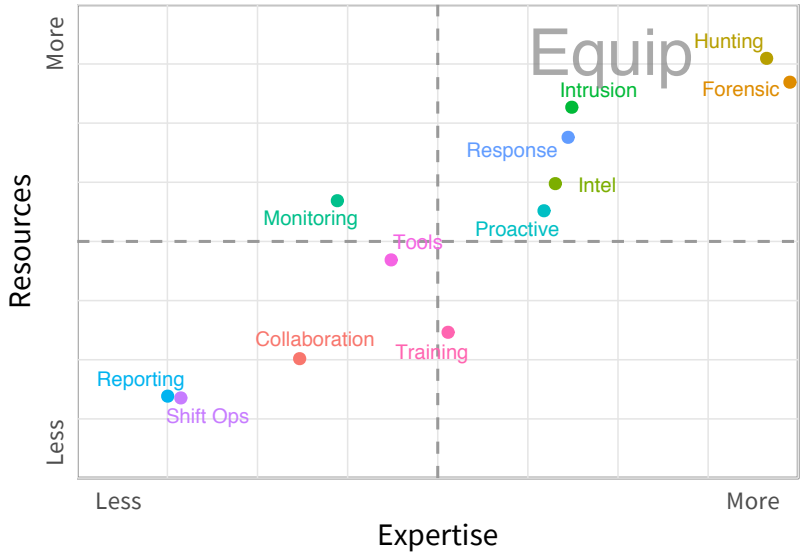
Recommendation: Invest in your people (especially in training and collaboration). Help them be the best they can be individually and collectively.

Equip Analysts for Complex Tasks

The previous two charts highlight the opportunity to shift analysts to more enjoyable and valuable activities, but how do we make that transition happen? The next two charts offer some solid options to consider, starting with Figure 21 showing how activities align along the Expertise-Resources dimensions.

FIGURE 21

Activity alignment along the Expertise-Resources dimensions



Source: Cyentia Institute

We already know from Figures 16 and 17 that the activities listed in the upper-right quadrant are also considered enjoyable, valuable, dynamic. If those sentiments are true, these are the things we want and need our SOC staff spending more of their time on. Because they require a lot of expertise and resources, however, a directive to "do more of that" won't work. We mentioned previously that training is one way to make these activities more accessible, but even expert analysts need adequate resources to perform them effectively. It's no accident the correlation between expertise and resources is among the strongest from Figure 18.

Resources in this context mainly refers to people, tools, and information. Beyond hiring more people, the best way to empower your analysts to do activities like those in the upper right of Figure 21 is to provide them the information and tools they need to succeed.

"I'd like more advanced work to do and mentors who I could learn from."

"Reduce the scope creep of tasks on my plate. Improve data feeds to SIEM. Purchase appropriate data hunting technologies and threat intel services. Get leadership that has a clue about the difficulties faced by the SOC."

RELEVANT RESOURCE:
Huntpedia, a collection wisdom from some the industry's most seasoned threat hunters Get it here.

"Better funding for equipment and tools. I don't expect the 'one of everything' approach, but a lot of basic infrastructure needs a refresh, and it demotivates the team."

"How about tools that work?! We spend too much time fixing tool issues instead of tracking down badness."

Start by asking them how many tools and info/intel sources they use to perform common tasks. How much time is wasted working around and compensating for resources they don't have on hand but need? How do they obtain additional context or intelligence on active threats and vulnerabilities? How difficult is it to stitch all the info scraps together in order to act appropriately? Could time be saved with better access, consolidation, and/or analytics? You may not like the answers you get to these questions, but they're worth asking nevertheless.

"Equip" is the operative word for this recommendation, but we should add that giving analysts the flexibility and autonomy to equip themselves is important as well. Allowing them to build a solution will improve their acumen for complex tasks and may create something that helps level up other analysts as well.

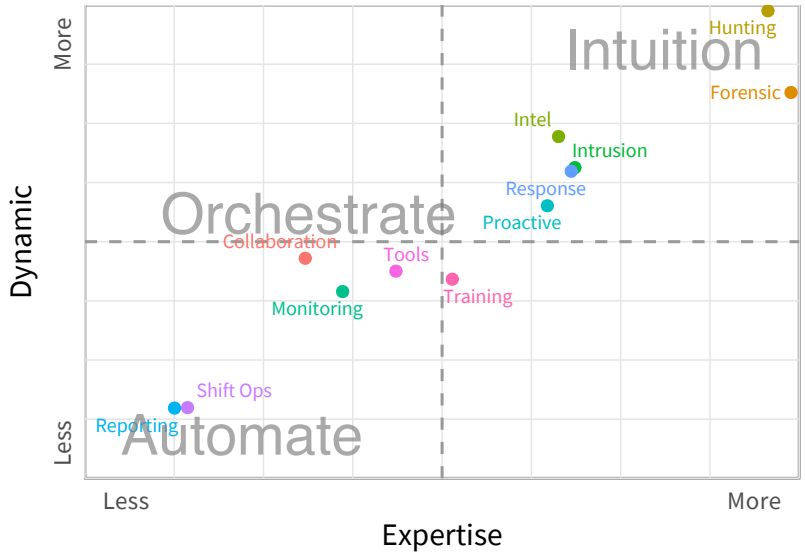
Recommendation: Equip analysts with the information and tools they need to perform complex tasks (like hunting, intrusion detection and forensics) better, smarter, and faster.

Use the Powers of Man & Machine

In terms of the positioning of activities on the grid, Figure 22 looks fairly similar to Figure 21 above. But the comparison of the Expertise and Dynamic dimensions shown here has a different purpose. We essentially want to distinguish between higher-order activities that require humans in the mix and the lower-level ones that can be adequately handled by machines.

FIGURE 22

Activity alignment along the Expertise-Dynamic dimensions



Source: Cyentia Institute

There's a lot of buzz in the cybersecurity industry of late around artificial intelligence (AI), automation, and orchestration. Some view them as the Next Great Hope, while others would replace that last word with "Hype." We're not entering that fray, but we would like to share some data-driven observations for both sides to consider.

"Analysts won't be successful studying events in isolation from other non-technical staff. A successful SOC brings together all stakeholders towards a common purpose."

"More automation and less drive from management to do more work (tickets) for metrics improvement."

"The meaningless shift reports and documenting of events needs to be automated ASAP."

"I expected it would be a nonstop adrenaline rush. The reality is hours upon hours of manual log crawling and frustration at things that cannot be correlated."

"We need better/easier automation between tools. Writing APIs for all these systems and maintenance of them take lot of time, but would greatly help with auto remediation and intel sharing across platforms."

Despite what you might hear from some optimistic vendors, AI and automation can't solve all your cybersecurity challenges. For example, highly dynamic activities that require a great deal of expertise are not the most suitable candidates for automated decisioning. Human intuition is essential to things like hunting and forensics (at least for now). But automation can work wonders for simpler, repetitive, time-guzzling tasks that require human fingers more than human brains. Activities found in the lower-left fit this bill, and among those, the one that stands out is monitoring.

If you've followed this report, analysts have a rather unfavorable view of real-time event monitoring and triage. It takes a lot of time. It's tedious and repetitive. It is not very effective. The list goes on. Thus, monitoring ranks highest on the list of detection-oriented tasks that could benefit from automation to free up analyst intuition for higher-leverage activities toward the upper-right of Figure 22.

So we've discussed activities on either end of the Man-Machine continuum, but what about those in the middle of Figure 22? There's no universally-accepted definition for the difference between automation and orchestration, but one common view is that you automate within a task, process, or workflow and orchestrate across them. The purpose of orchestration isn't to fully accomplish an activity, but rather guide or handle certain aspects of it to make the analyst more efficient. For instance, responding to a exploit, gathering related intel, scanning for vulnerable systems/indicators, and then mitigating them is a classic security orchestration combo blending algorithm and analyst. Based on these resutls, orchestration could help streamline these middle-ground processes so they become more approachable by more analysts.

Recommendation: Leverage the automation and orchestration boom to your advantage, but don't view algorithms as a replacement for intuition. There's a lot of snake oil going around, but solid solutions exist that can help your SOC run like a well-oiled machine (made of humans).

We don't have time (and don't see it as our place) to discuss specific products or services related to the recommendations above, but we hope this research helps you plan and pack for the trip. On that note, we're sure our sponsor, Respond Software, would appreciate you including them in that evaluation.

Thank you for taking the time to read this report; we hope it helps your SOC be the best it can be for the analysts that comprise it and the organizations that depend upon it. And thanks once again to all those who participated in the study; we hope you feel your time was well spent and well reflected in this final product. If you have questions or comments about this report or would like to join our contact list for future research projects, contact us via Twitter (@cyentiainst), email (research@cyentia.com), or visit www.cyentia.com.

"A lot of cycles are wasted on mundane tasks. Freeing analysts from their rigid day-to-day duties and leveraging them for threat hunting has produced more high profile incidents than monitoring in my personal experience."

RELEVANT RESOURCE:
36th IEEE Symposium on Security and Privacy keynote from Dan Geer, "Dark Matter: Driven By Data"
View on YouTube

"Before you even think about going down the automation path, you need a really good feel for what you are doing. Review processes and find out what analysts are doing vs the documented process."

"Thank you for doing work on what the SOC actually needs from the business, not just what the business needs from the SOC."

Appendix A

Sampling Methodology for This Study

Our purpose in conducting this study was to examine the perceptions of SOC analysts to understand their attitudes, experiences, activities, challenges, opinions, and ideas regarding their profession. As such, the target population of "SOC analysts" includes all those whose current role involves monitoring, detecting, analyzing, responding to, or otherwise handling security events and incidents (or managing others who do those things). In that sense, we're blending traditional SOCs and CIRTs (Cyber/Computer Incident Response Team) under the same heading.

After considering that target population, we determined obtaining a probabilistic sample was unrealistic. Not only is the target population a subset of an already fairly specific domain (cybersecurity), but SOCs are particularly sensitive work environments. Several we invited expressed interest in the study, but said organizational policy restricted them from participating.

Rather than defaulting to the "blast out invites until enough people respond" method of convenience sampling so typical in cybersecurity research, we endeavored to construct a reasonable supersample comprised of multiple independent samples. Our largest pool of respondents came via LinkedIn, where we randomly selected and directly invite people matching search criteria for relevant job roles. We also invited members of peer groups such as the SANS Digital Forensics and Incident Response (DFIR) mailing list and alumni of the SANS MGT 517 (Managing Security Operations: Detection, Response, and Intelligence) course, but participation was low compared to direct invitations via LinkedIn.

We also invited several individual enterprise SOCs and Managed Security Service Providers (MSSPs) to take part in the study as a unit. For this, a separate instance of our survey was created for each organization and the SOC Director/Manager distributed the invitations to their respective teams. This not only resulted in highly-vetted responses, but gave us multiple viewpoints from analysts within the same SOC. Over half of the responses for this study were collected in this manner, and those were split fairly evenly between enterprise SOCs and MSSPs. As a thank you for their time, participating organizations received a custom report containing additional details and comparisons not published in this report.

The resulting dataset is still a nonprobability sample, but we hope our approach helps to minimize bias and maximize its representativeness. The sample statistics provided in this report should assist you in determining how well your organization and requirements may be represented.

> **Interested readers like you are the key to our ability to conduct and share research like this. If you're open to participating in future Cyentia Institute studies, drop us a line at research@cyentia.com.**

VOICE OF THE ANALYST

CYENTIA INSTITUTE

> "I would love to see this survey taken and findings shared so we can talk more about the difficulties of the day to day SOC"