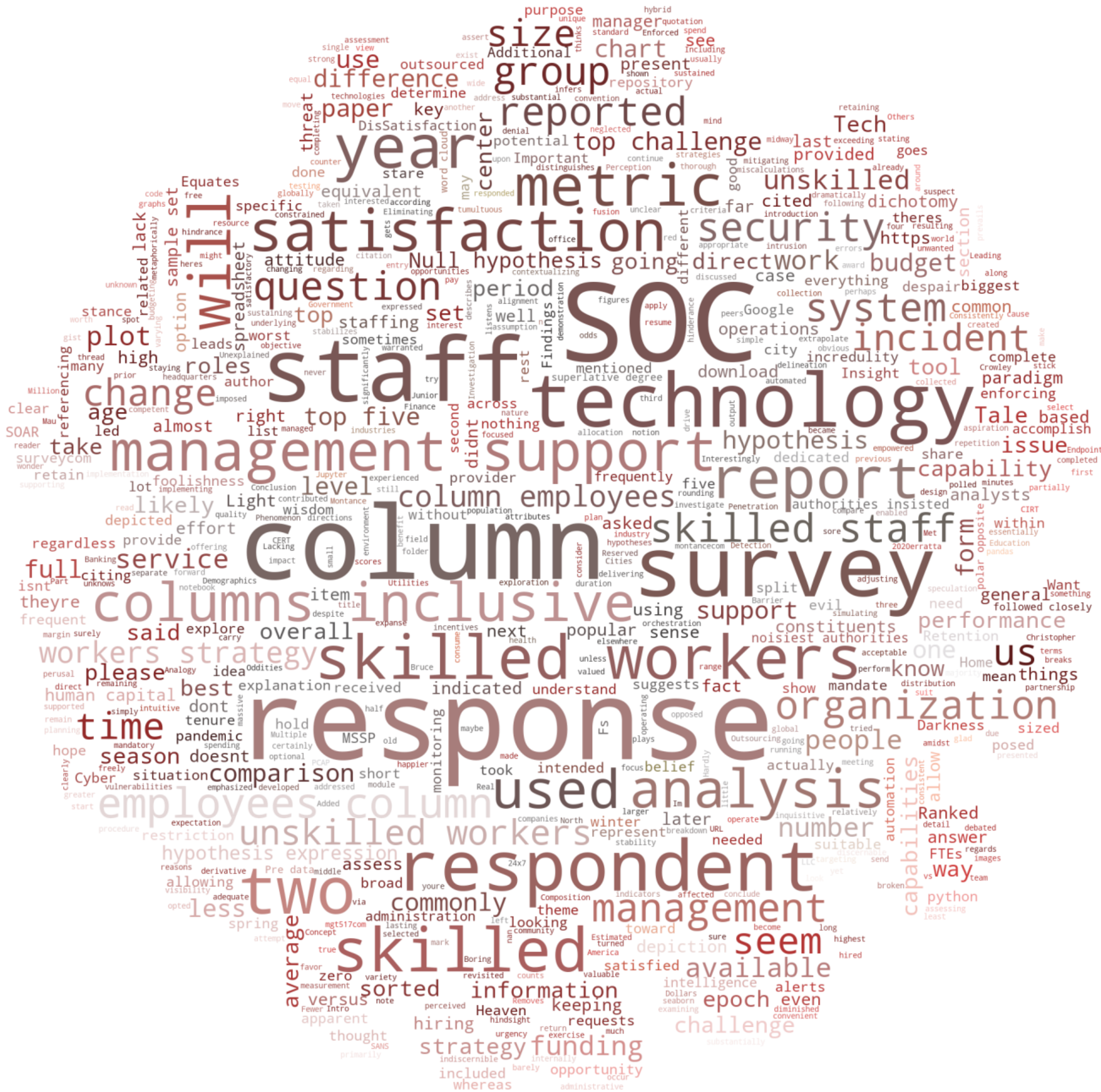

2020 SOC-Survey
A Tale of Two SOCs

Montance® LLC

Christopher Crowley

Intro

It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other way—in short, the period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or for evil, in the superlative degree of comparison only.[1]

In 2020, there wasn't adequate vendor interest for the SANS Institute SOC Survey; however, I felt that there was a need to provide year-to-year coverage and provide an additional avenue for community-driven questioning. Thus, the 2020 SOC-Survey was conducted. There were changes for the 2020 SOC-Survey from previous years. The sense of things changing dramatically yet staying the same is strong, yet this is not explored in this report because this report deals with 2020 SOC-Survey responses only. In 2021, there will be additional comparisons on trends over the past several years of surveys, possibly including past SOC Surveys and published peer reports.

All the survey responses were thorough, that is the respondents took the time to completely answer all the questions. The information the respondents provided will surely be valuable to you in your planning and response amidst apparent stability and tumultuous change.

Figure Intro-1 shows one distinction that is used throughout this report based on the 2020 responses. There are two groups, or cities that the respondents are separated into. Those SOCs where management supports the SOC knowledge workers as distinct and skillful: the "skilled" strategy. The other SOC city is the "unskilled" strategy. This split was observed after reviewing response data, and became the theme of inspection of the responses.

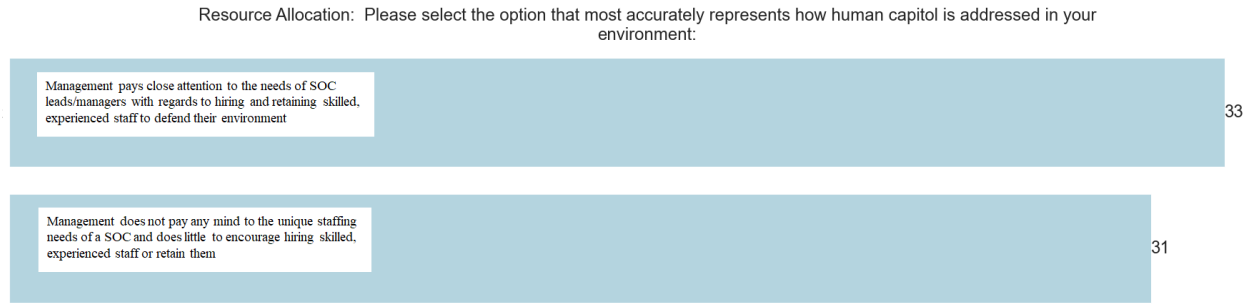

Figure Intro-1. n=94, Human Capital Attitude. Column=97

Data and Analysis Available for Review, Collection and Reporting Methods

There are many potential dichotomies and distinctions that could be identified. A spreadsheet is available for download and is freely available to use for derivative works with appropriate citation. https://mgt517.com/2020-survey-download is the repository with responses spreadsheet, and all analysis code used for this report. This link shorted URL (or https://soc-survey.com) is suitable for

[1] Charles Dickens, A Tale of Two Cities, Book the First, Chapter I. Also, https://archive.org/stream/adventuresofoliv00dickiala#page/n401/mode/2up

referencing this report, where it will remain available for download. The jupyter notebook used to create all plots is also available at the URL, for double checking all work if you choose to.

Figure Intro-2. Jupyter notebook code for creation of charts.

The survey responses were collected via a Google Form, and the response collection was downloaded in the form of a spreadsheet. When referencing questions asked this report will use the convention of citing the column or columns the response(s) are in, based on the dataframe used in pandas. That dataframe starts numbering columns at 0. The jupyter notebook (above) has the gory details of the mapping.

There were four response options to the question of how human capital is addressed. Two are shown in Figure Intro-1 above. The two other response options were, "Management listens to the requests of SOC leads/managers with regards to hiring skilled, experienced staff, but does not understand the urgency to retain these skilled people" (count=25) and "Management thinks hiring many, less skilled employees to stare at alerts is an acceptable strategy for mitigating Cyber Security threats in their environment" (count=5).

Including the five "stare at alerts" responses with the "not pay any mind" group seems consistent, and doesn't change the allocation much (count=36 to 33 versus 31 to 33) so that group represents a more extreme stance of "not pay any mind."

The notion that effort is made to hired skilled people but not retain them seems at odds with itself, which is why it isn't depicted as a "third" city in this paradigm of explanation. If you allow the city as a metaphorical substitution for the strategy of managing a SOC, this third group represents the broad expanse between the two cities: scrub land of little recognizable or describable character.

Demographics

We'll resume our exploration and comparison between the two SOC paradigms (skilled vs. unskilled) after contextualizing the respondents.

Count

There were 107 respondents this year. This is down substantially from the (count=517) 2019 SANS SOC Survey[2]. The reduced response is likely due to diminished visibility and distribution of the requests to take the survey as well as incentives for completing the survey. Of the 107 respondents for this year's survey almost all (count=97/107) completed the last question, so the quality of responses is high. The survey likely took 30-45 minutes to complete. To those who spent that time, we appreciate your effort and community contribution.

[2] Crowley, Chris and John Pescatore. "Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey". *SANS Institute Reading Room.* URL: https://www.sans.org/reading-room/whitepapers/analyst/membership/39060?soc-class=true. Accessed 18 Dec 2020.

Respondents Information

Fifty-one (51) of the respondents cited North America as the headquarters for the organization discussed (column=187). Twenty-nine (29) cited the organization's size (column=182) as between 1,000 and 5,000 people (the most popular answer) with seventy-five (75) citing an organization size of less than 20,000 people.

The most commonly cited single industry supported (column=184) was Banking and Finance (count=12), with Education (count=9), Government (count=8), Technology (count=5), and Utilities (count=4) rounding out the top five. Multiple responses included two or more industries.

The SOCs discussed were imposed upon constituents (column=183) according to about half the responses (count=52) stating the internal SOC is a mandatory service. Others didn't know (count=7), or the internal SOC was an optional service (count=35) which could be opted out of in favor of some other offering. The question didn't address if "no security support" was an option.

Key Findings

Since all the responses and plots of the responses are available for perusal, this report will focus on a few key findings and items of specific interest along the dichotomy of paradigms mentioned in the introduction: "Skilled staff versus unskilled staff." No historical trending is presented in this report.

2020 – Work from Home?

Added to the 2020 SOC-Survey midway, the question most appropriate for the year 2020 was "Do you allow SOC analysts to work from home?" (column=191)? Yes, without restriction was the most common (count=14) response. Yes, with restrictions (count=7) was less common.

Some (count=8) said they are only allowing it because of the pandemic, but plan to return to the old way of analysts at the office once the global health situation stabilizes, and a few (count=4) said they're allowing it because of the pandemic but will allow this change to become standard operating procedure going forward. Hardly suitable numbers to extrapolate to the general population. The 2021 and later surveys will have the benefit of hindsight to see how this plays out.

Capabilities

What counts for being a Security Operations Center is sometimes debated. Is that a CERT or a CIRT? How about the fusion center? Do you need to operate 24x7 to count as a SOC?

The survey tried to answer this question in terms of capability. The question offered three options, to capture if this was done internally only, or if a service provider of some form was used. There were 16 different capabilities posed as 100% internal, 100% outsourced, or a hybrid. The top five Internal responses are listed in Figure KeyFindings-1.

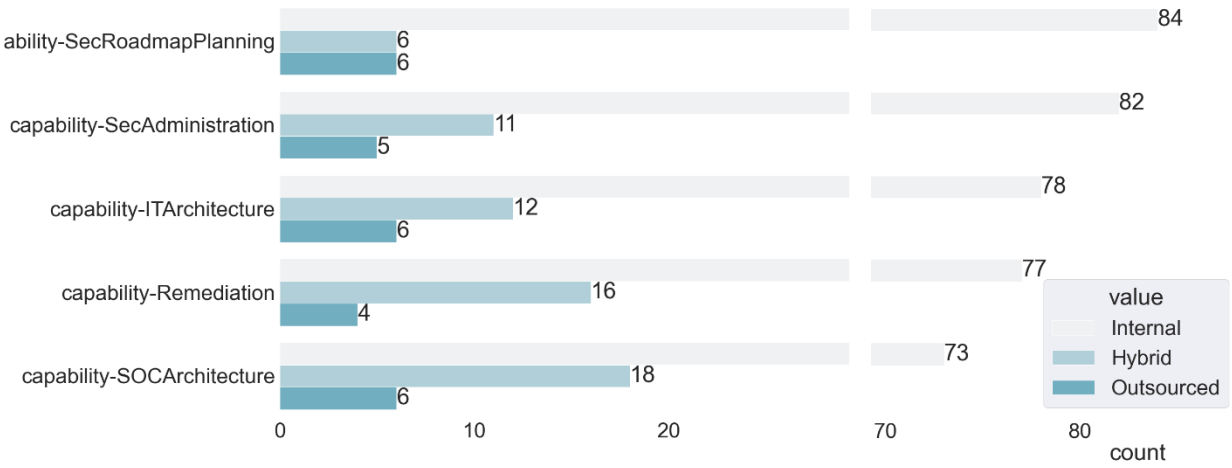

Figure KeyFindings-1. Top five capabilities sorted by Internal (Columns=3-19, inclusive)

Outsourcing

The capability might be available but not internal, and the survey aimed to determine which capabilities were necessary but outsourced. Some organizations choose to use both internal staff and third parties, citing a hybrid model.

Penetration testing (the assessment and demonstration of impact of vulnerabilities) and closely related red team capability (sustained operations simulating an actual intrusion group) are the most popular purely outsourced capabilities (both, count=36) as shown in Figure KeyFindings-2.

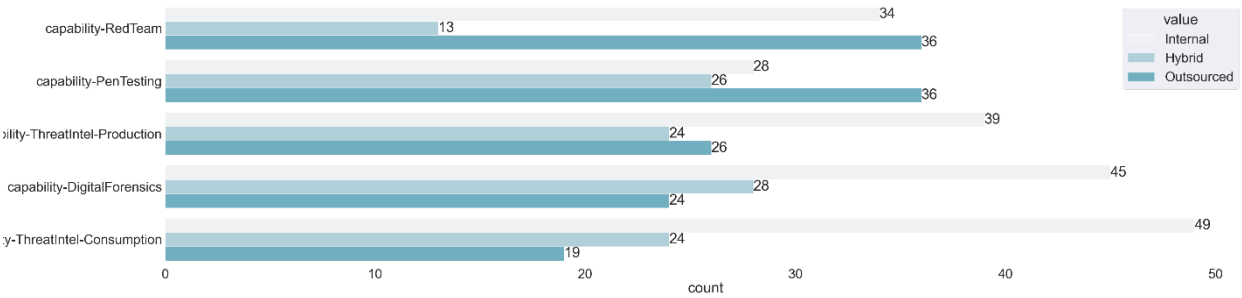

Figure KeyFindings-2. Top five capabilities sorted by Outsourced (Columns=3-19, inclusive)

Funding

SOC budgeting was reported, and significantly, most of the responses (count=34) indicated the budget was unknown (column=95) depicted in Figure KeyFindings-3.

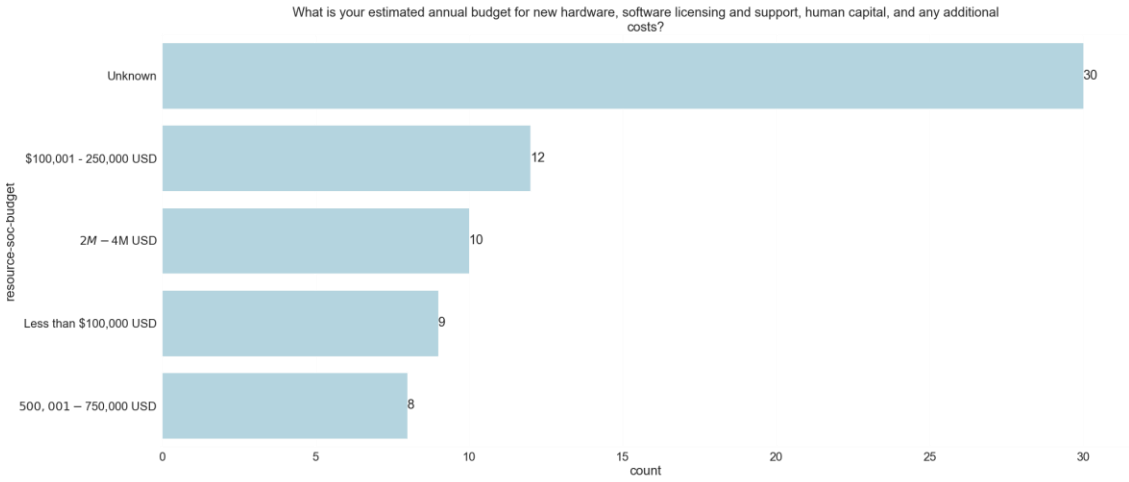

Figure KeyFindings-3. Estimated budget (column=95)

From this, the author of this paper infers that the respondents work within the SOC, and are primarily not the overall managers of the SOC. This is based on the assumption that the manager of the SOC would know the budget. Eliminating the unknowns (count=30), the theme of dichotomy prevails in the remaining answers which are all expressed in US Dollars. $100,001-250,000 is the next most popular answer (count=12) followed closely by $2-4 Million (count=10) above, in Figure KeyFindings-3. Which is followed closely by less than $100,000 (count=9) and $500,001-750,000. In a later section, the "tale of two SOCs" comparison will be revisited to compare the budget of the staffing "empowered" versus the staffing "neglected."

Metrics

Metrics provide a depiction of performance to the organization, twenty-four (24) of the respondents indicated they do not provide metrics (column=26) to management in Figure KeyFindings-4.

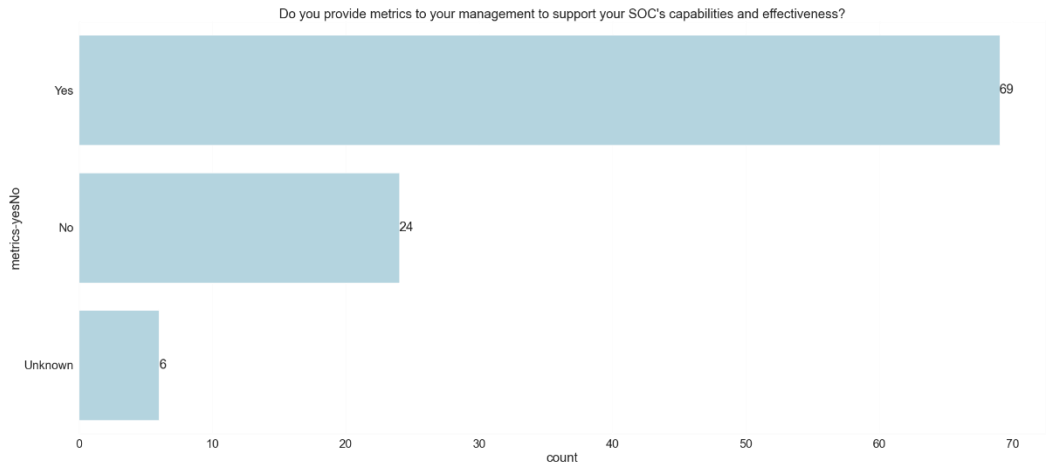

Figure KeyFindings-4. Metrics provided (column=26)

There were a broad variety of metrics presented (columns=40-52) to determine if each was used, but also if that measurement became a service level objective in some form. The “Consistently Met” and “Enforced” indicators were intended to assess if the respondent had an expectation of performance criteria by the organization, or by the SOC itself, as shown in Figure KeyFindings-5.

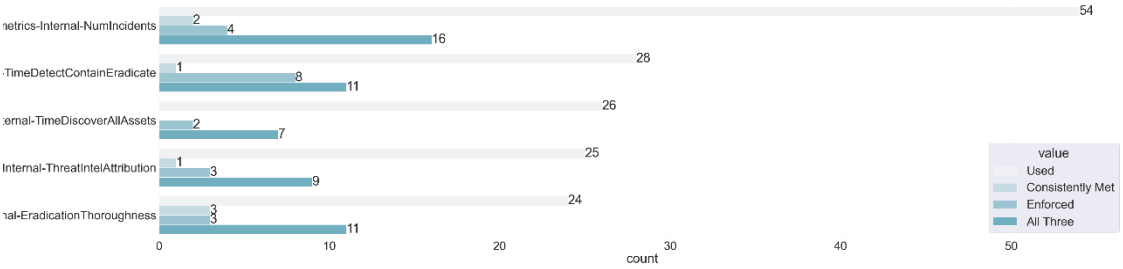

Figure KeyFindings-5. Internal metrics sorted by Used (Columns=40-52, inclusive)

Related is the idea of what managed security service providers are delivering as metrics to assess the services provided by that MSSP (columns=27-39). See Figure KeyFindings-6.

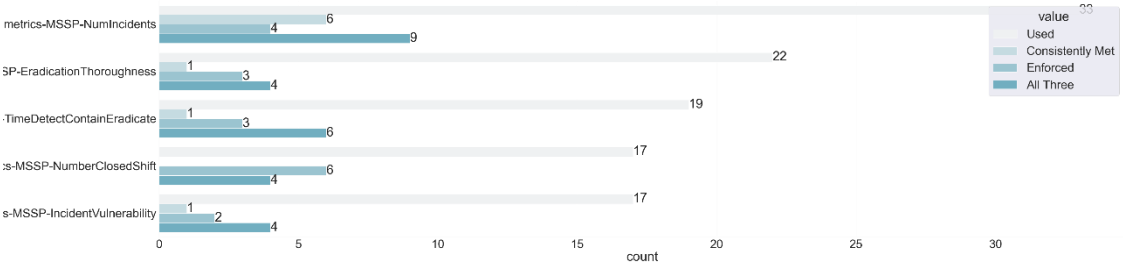

Figure KeyFindings-6. MSSP metrics sorted by Used (Columns=27-39, inclusive)

In both cases, a simple count of incidents is the most common metric used by a wide margin. The idea of “meeting” or “enforcing” a number of incidents is counter-intuitive to the author of this paper. It is unclear what enforcing the number of incidents would mean, unless that means there is a mandate for zero incidents. This seems to be denial of the fact that cyber security incidents occur, perhaps a “not in my city,” mandate from the constituents of the SOC.

According to the responses, metrics are most commonly only partially automated (count=49) to report (column=53). Maybe the manual effort involved is why some responded that they don’t provide metrics (column=26) at all?

Staff

The most popular SOC Staff size (count=54) in the response set was between 2-10 people (column=85) depicted in Figure KeyFindings-7, more than double the next most popular answer of 11-25 full-time employees (FTE). The full chart set breaks down the varying staff roles (columns 87-94) of SOCs, and distinguishes the support and system administrative roles from analysts.

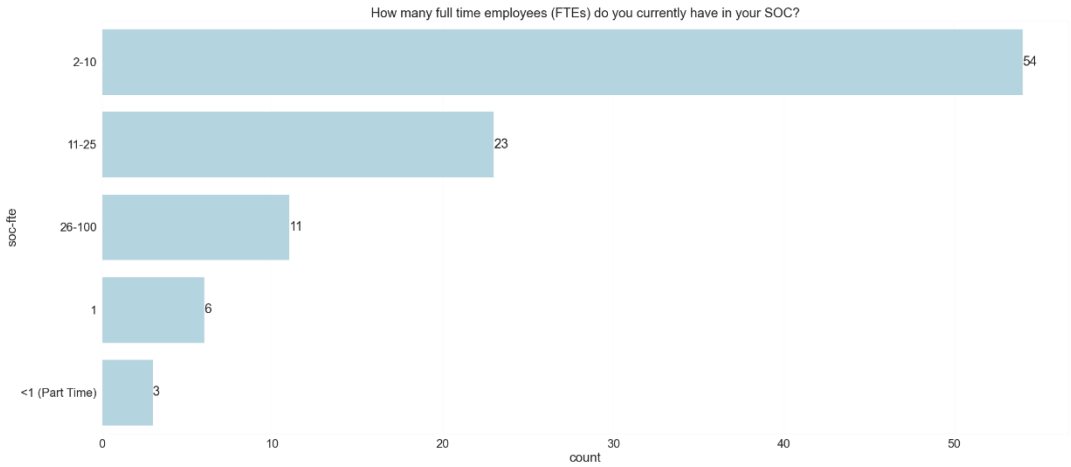

Figure KeyFindings-7. Full Time Equivalent Staff Roles. (column=85)

In Figure KeyFindings-8, it seems these staff don't stick around for long (column=86), however. The most commonly reported average tenure is 1-3 years (count=39) and the next most frequent response duration (count=34) is 3-5 years. An average lasting more than 5 years (count=13) was reported by only a few respondents. Shown in the same figure, almost as many (count=9) reported an average tenure of 1 year or less as reported an average of 5-10 years (count=11).

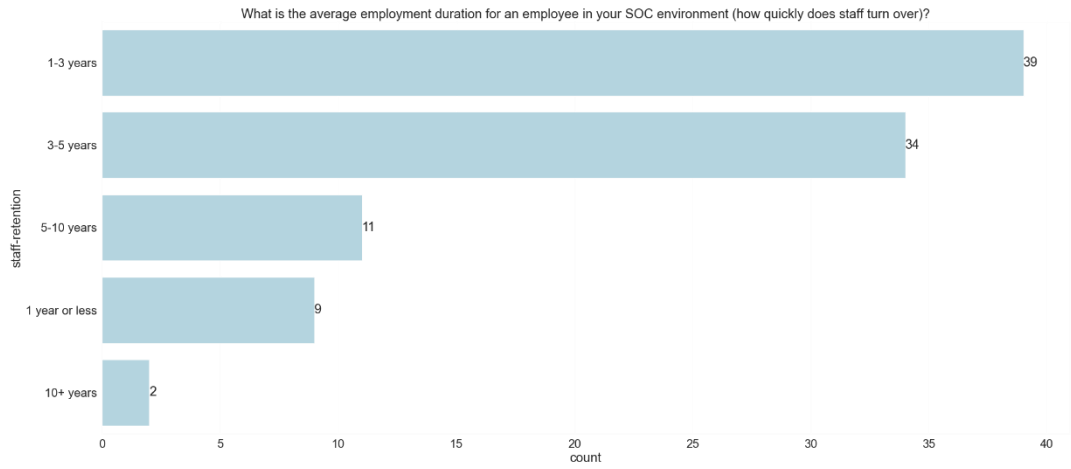

Figure KeyFindings-8. Staff Retention. (column=86)

There was a free entry field for the what works in retaining staff question. Using the word cloud module within python to create Figure KeyFindings-9, we see a visualization of size ranked words in the responses (column=87) based on frequency of repetition. Training, pay, and career development seem to be the most commonly expressed items.

Figure KeyFindings-9. Staff retention word cloud. (column=87)

Challenges?

The survey asked what the single biggest challenge is (column=79) and the result is shown in Figure KeyFindings-10. “Please select one of the following challenges that best describes the biggest hinderance to your SOC:”

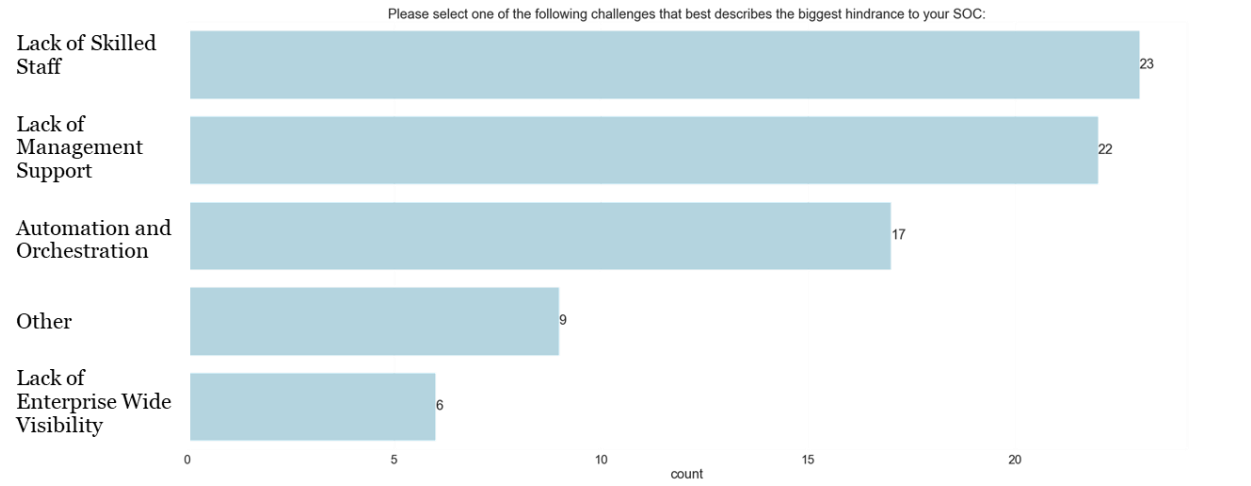

Figure KeyFindings-10. Biggest hindrance to the SOC (column=79)

This skilled staff response was the start of the inquiry which led to this year’s title: A Tale of Two SOCs. Lacking skilled staff (count=23) is the most commonly mentioned issue, and management not supporting the security efforts (count=22) is close behind, as seen in Figure KeyFindings-10. With a perceived lack of talent or competent people, it is no wonder that respondents have turned to automation and orchestration tools (count=17) to try to get things done.

Tale of Two Cities Analogy

Insight Leading to Concept of "Two SOC Dichotomy"

The almost even split between the polar opposite stances regarding attitude toward staff was an obvious one when looking at the column 97 plot. It led to the inquisitive thought, "how different are the SOCs in perceived performance by the respondents to this survey?"

This section presents two hypothesis which were developed prior to actually assessing the responses. Then, two more which were developed during assessment of the responses using this "dichotomy" as the basis for separating the responses for comparison.

The first "speculated hypothesis" is that management support for hiring unique staff leads to more funding. The second is that the satisfaction with the technology is high in the skilled staff set.

Hypothesis 1: Management Support Equates to More Funding

Pre-data analysis hypothesis: the "skilled staff" group will represent more funding (even adjusting for size of the organization).

Null hypothesis expression of this hypothesis is, "There is no difference between the funding levels of SOCs in equivalent sized companies if the management supports a "skilled workers" or "unskilled workers" strategy."

From the plots Figures TwoCities-1 through TwoCities-9 there is no clear delineation of the skilled workers having more budget at any organization size. So, the null hypothesis holds, as there is no discernable difference between the funding levels of equivalent sized organizations regardless of the "skilled workers" or "unskilled workers" strategy. Important to note, this is what *this* sample set of responses suggests. Investigation in a larger, representative sample set is warranted.

See the figures (columns=95,97,182) below.

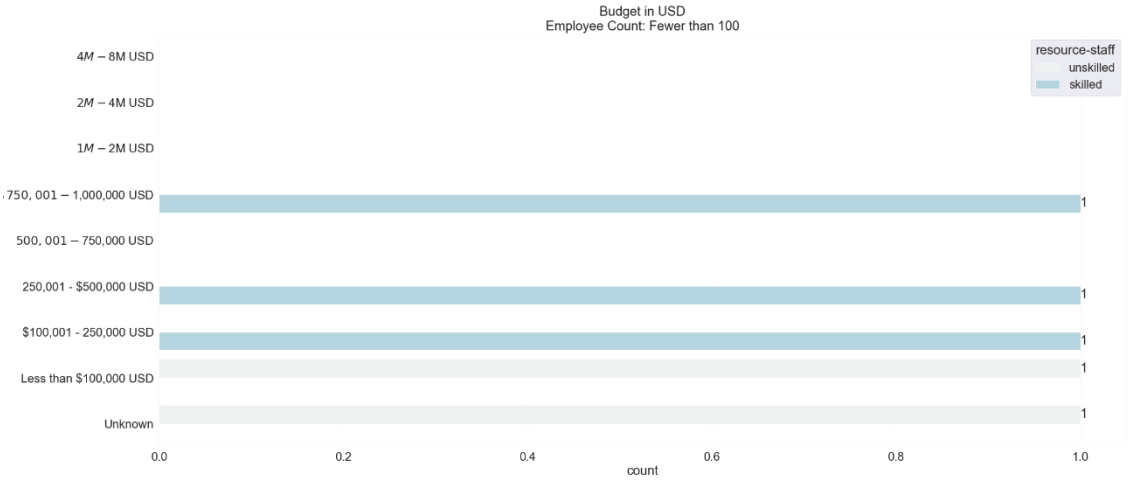

Figure TwoCities-1. Fewer than 100 employees. (column=95)

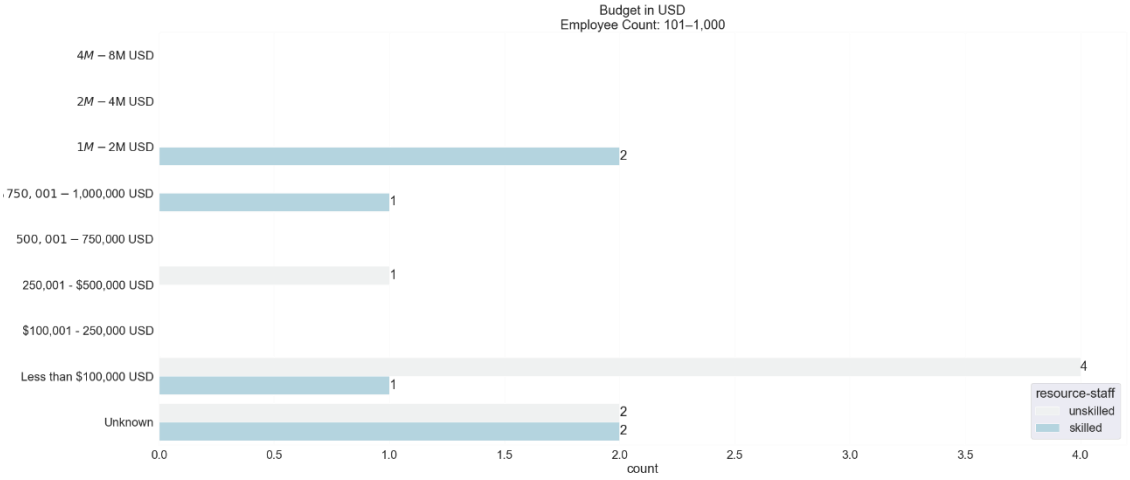

Figure TwoCities-2. 101 – 1,000 employees. (column=95)

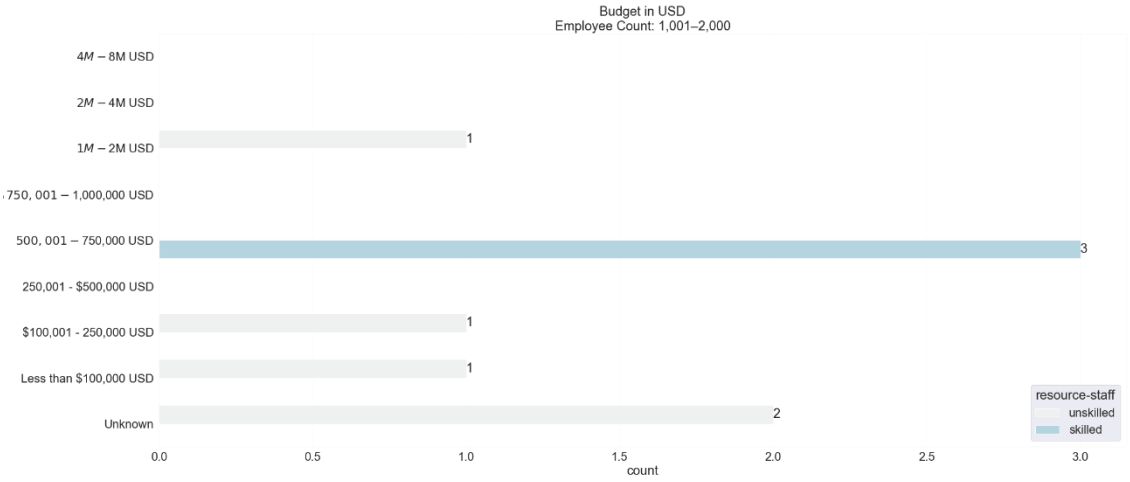

Figure TwoCities-3. 1,001 – 2,000 employees. (column=95)

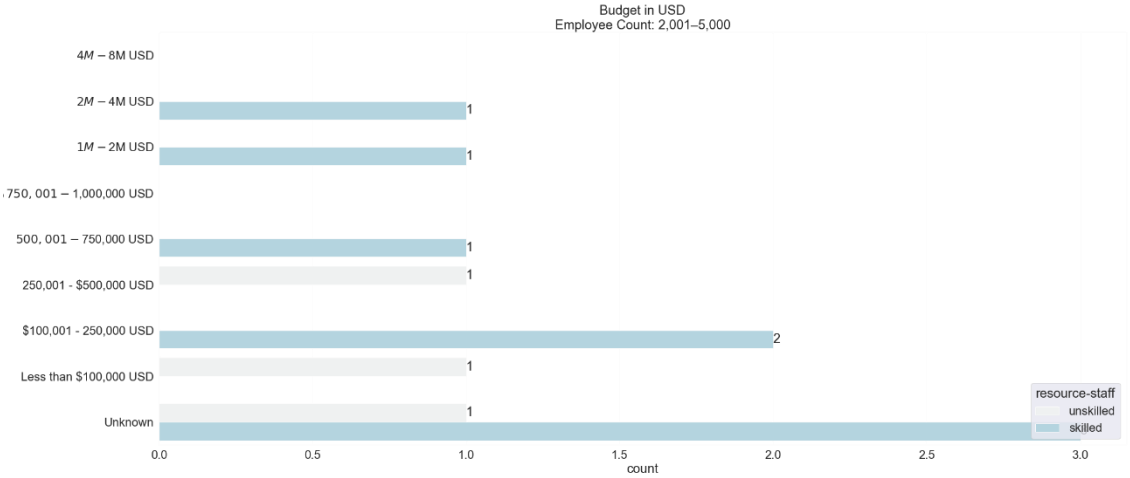

Figure TwoCities-4. 2,001 – 5,000 employees. (column=95)

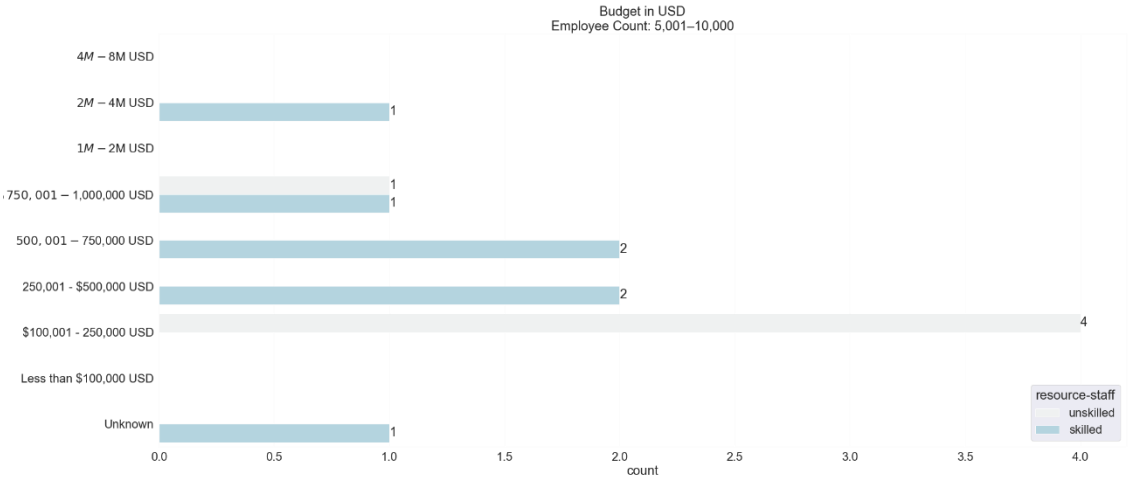

Figure TwoCities-5. 5,001 – 10,000 employees. (column=95)

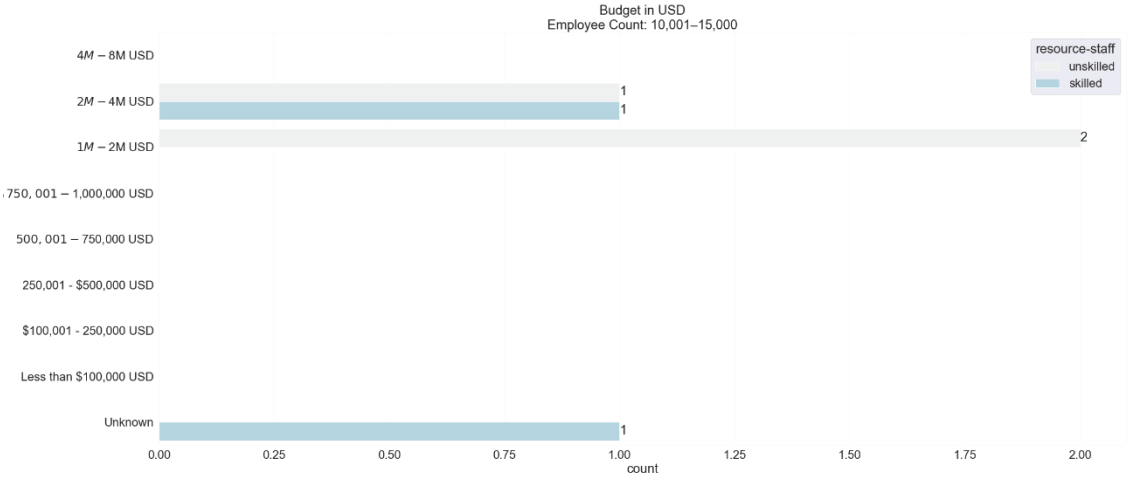

Figure TwoCities-6. 10,001 – 15,000 employees. (column=95)

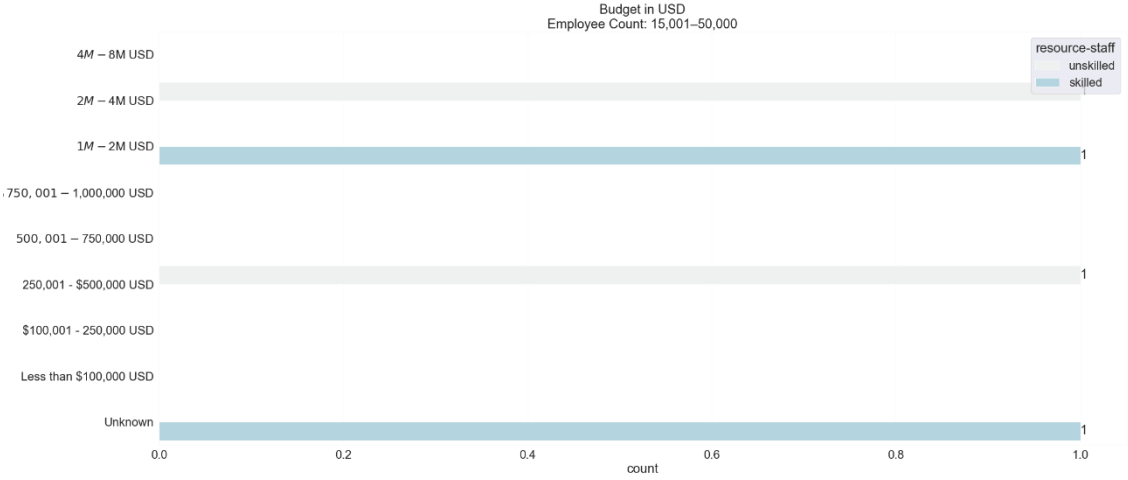

Figure TwoCities-7. 15,001 – 50,000 employees. (column=95)

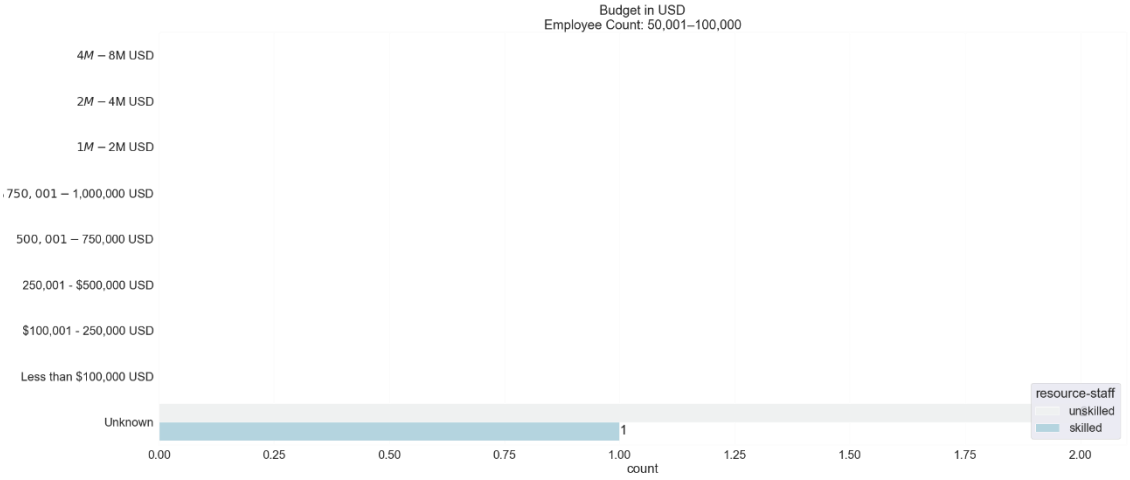

Figure TwoCities-8. 50,001 – 100,000 employees. (column=95)

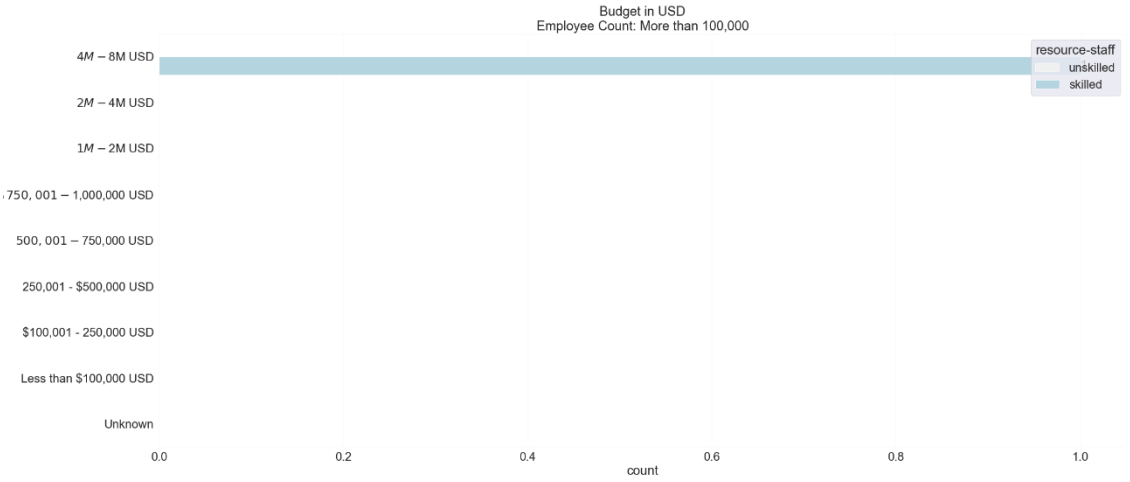

Figure TwoCities-9. More than 100,000 employees. (column=95)

Figures TwoCities 1 through 9 depict no obvious distinction in the funding levels of SOCs of equivalent size organizations between the “unskilled” and “skilled” management stance on employees in the SOC. Taken in the positive light, the inference is that the management with the “skilled” worker stance insist on maximizing value of expenditure.

Hypothesis 2: Management Support Equates to High Technology Satisfaction

Pre-data analysis hypothesis: the “skilled staff” group will be happier with the technology used. The speculation is based on the fact that “skilled staff” understand how to use the tools, how to apply the right tool to the right situation, and will have a valued partnership with SOC management (and constituents as needed) to change technology to suit the SOC’s needs, resulting in greater satisfaction.

Null hypothesis expression is, “There is no difference between the indicated levels of satisfaction with technology in SOCs if the management supports a “skilled workers” or “unskilled workers” strategy.”

Interestingly in these plots, there is a clear depiction that there is in fact a difference between levels of technology satisfaction between the skilled and unskilled strategies. Figure TwoCities-10 shows the top-5 overall satisfactory technologies, based on highest number of “A” scores for that tech across all responses, from the respondents in the “skilled” group. Figure TwoCities-11 shows the top-5 overall satisfactory technologies, based on highest number of “A” scores for that tech across all responses, from the respondents in the “unskilled” group.

There are about equal numbers of skilled strategy (count=33) and unskilled strategy (count=31) respondents. Looking at these “best” technologies, the skilled strategy respondents clearly reported more satisfaction in the technology in use. The technology satisfaction charts for all respondents are shown later in the “Boring Lists” section of the report.

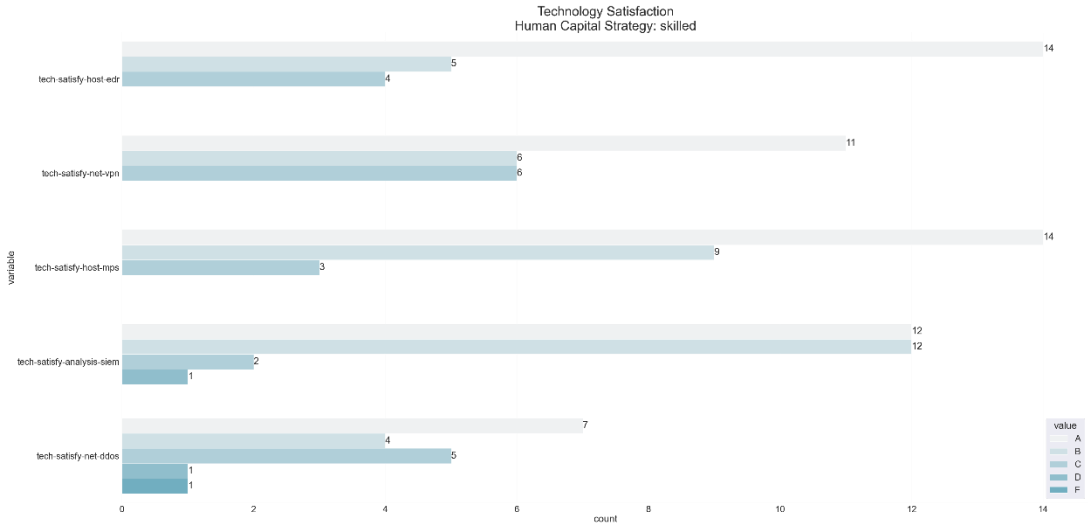

Figure TwoCities-10. Top 5 satisfied technology overall, skilled workers strategy (columns=142-181, inclusive)

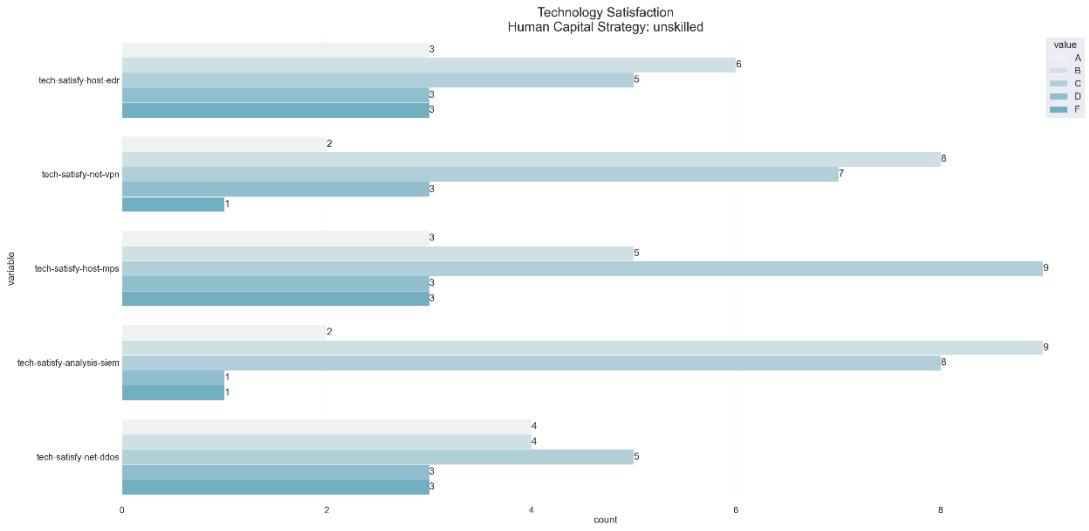

Figure TwoCities-11. Top 5 satisfied technology overall, unskilled workers strategy (columns=142-181, inclusive)

There may be any number of explanations as to why this is the case, and these survey responses don't seem to hold adequate information to allow us to explore the underlying reasons why.

Hypothesis 3: Is This Real Phenomenon or Perception?

There are certainly more opportunities to explore this apparent dichotomy further. It's important to consider if it is worth it. After considering Hypothesis 1 and Hypothesis 2 above, the notion that this might be a fruitless path of inquiry was strong.

That is, does this split actually exist, or are the responses simply targeting "management" as the convenient recipient of blame while the true nature of the issue rests elsewhere?

Null hypothesis expression is, "There is no difference between the capability, performance, satisfaction, or other attributes polled by this survey if the SOC management supports "skilled workers" or "unskilled workers" strategy."

This is left as an exercise for the reader, as it would consume substantial effort to assert this across this relatively small sample set.

One Additional Hypothesis: Management Support Removes Staffing Barrier

In examining the responses to investigate the three hypotheses above, there was another thought. Does the "top challenge" (column=79) change if there's management support for skilled workers? The full set of responses indicates "Lack of skilled staff" as the greatest challenge as was shown in Figure KeyFindings-10.

Null hypothesis expression is, "The top challenge of lack of skilled workers is not affected by management's reported attitude toward human capital."

The two plots below separate the responses into two sets, one which said that management supports a “skilled workers” or “unskilled workers” strategy. Figure TwoCities-12 shows the “skilled workers” responses for Top SOC Challenge (column=79).

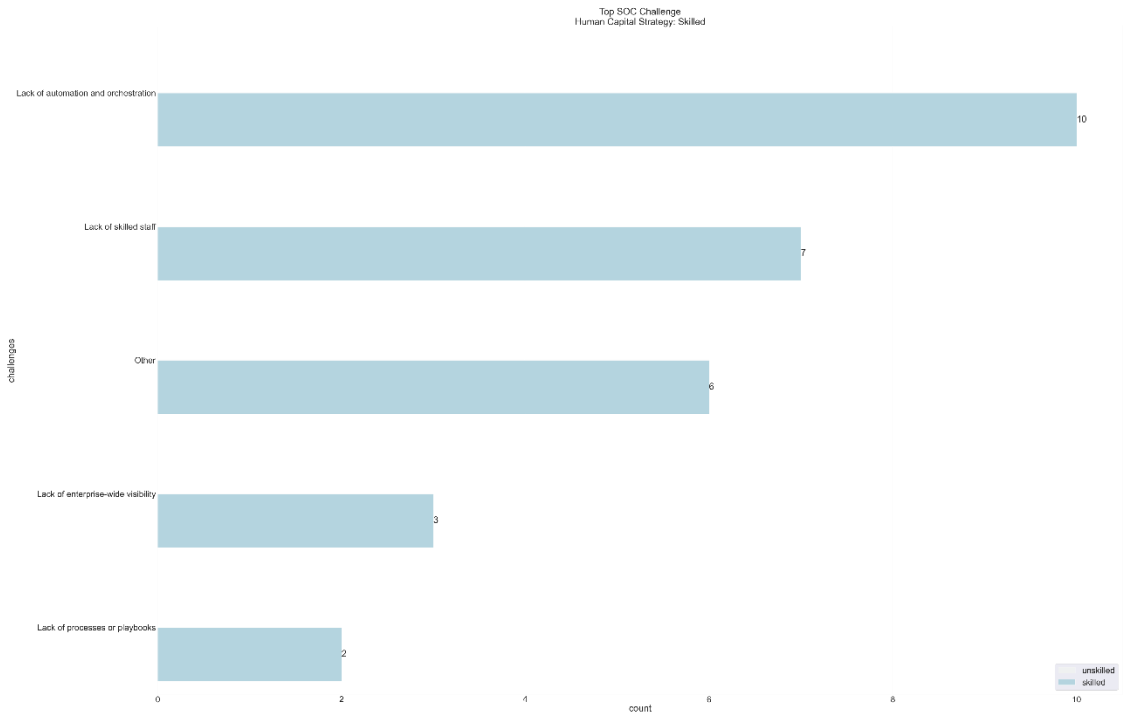

Figure TwoCities-12. Top Challenges (column=79) of “skilled workers” respondents

Figure TwoCities-13 shows the “unskilled workers” responses for Top Challenges.

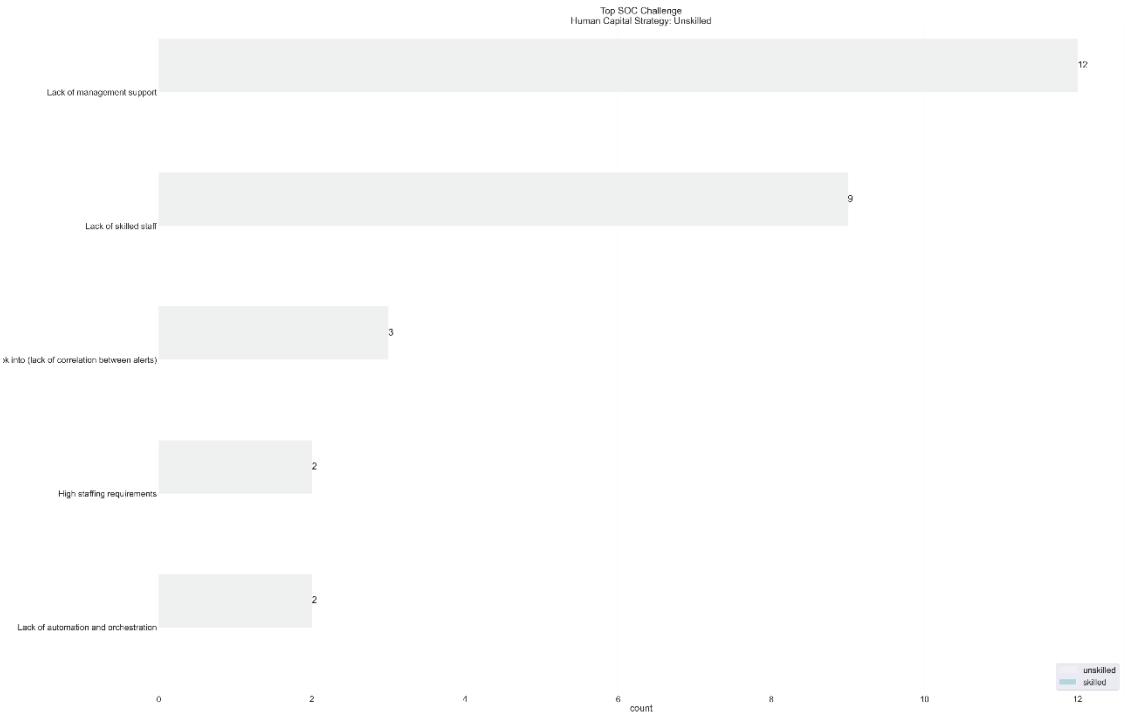

Figure TwoCities-13. Top Challenges (column=79) of “unskilled workers” respondents

This suggests that the “skilled workers” management support has enabled those respondents to move on to the next challenge of implementing SOAR tools despite “Lack of skilled staff” still being an obvious sore spot, where the skilled group reports that issue second most commonly (count=7).

The skilled group reports SOAR implementation most commonly (count=10) as the top challenge in Figure TwoCities-12, whereas the unskilled group reports that issue in the middle range (count=2) of its responses in Figure TwoCities-13. There were more than five options to the question, only the top five are depicted in Figures TwoCities-12 and TwoCities-13. Again, the full response set is available for your review or additional analysis.

Shown in Figure TwoCities-13, the unskilled group is more focused on the sense that management doesn’t support them, exceeding the lack of skilled staff (count=9) as the top response (count=12) but “lack of support” doesn’t even make top five in the skilled group’s responses.

Oddities and Unexplained Items

What Do You Want to Know?

There are lots of directions that analysis of these responses could be taken. If you perform analysis and want to share it with the world, please do so. If you suspect there are errors or miscalculations in this report, please send to soc+2020erratta@montance.com.

Boring Lists

There are approximately two hundred (200) graphical plots that were created from the responses with Jupyter notebook, python, pandas, and seaborn. If you don't see something in this report that you're interested in, take a look to see if the plot was already created in the images-output folder in the google drive repository https://mgt517.com/2020-survey-download or on https://soc-survey.com.

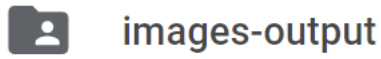

Figure Boring-1. Images-output folder in Google Drive share

Staff Composition

We already know the most likely size is 2-10 (column=81) full time equivalents (FTE). The survey asked in a little more detail how that gets broken down into specific staff roles.

The gist of this breakdown is general-purpose staff are the most common (count=63, column=89). It is most common that there are zero (0) dedicated monitoring (count=39, column=90); incident response (count=47, column=91); threat intelligence (count=49, column=92); or support (count=50, column=93) staff. Most responses said it took 2-10 FTEs to do the system administration for the SOC (count=47, column=94). Just "keeping the lights on" is what a lot of SOCs spend their time doing, essentially just running security systems as opposed to dedicated analysis using the security relevant data in those systems.

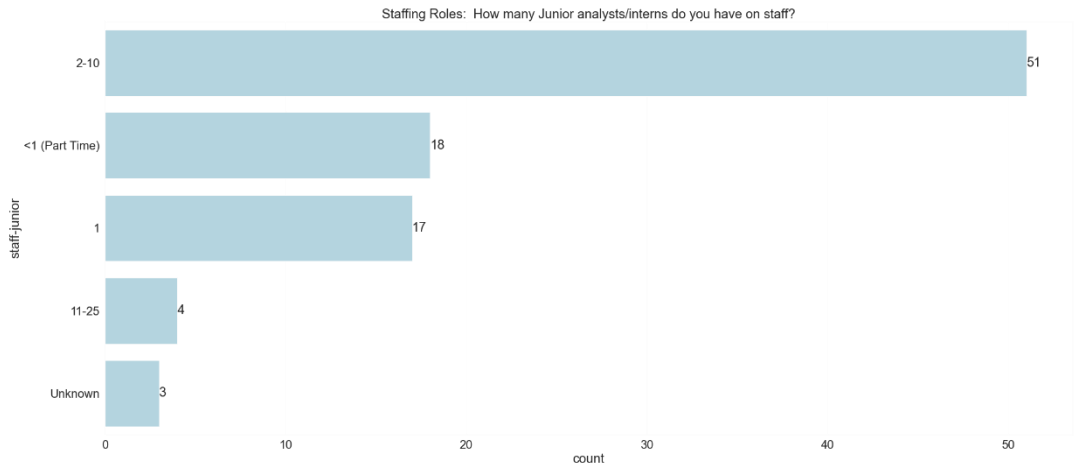

Figure Boring-2. Junior staff (column=88)

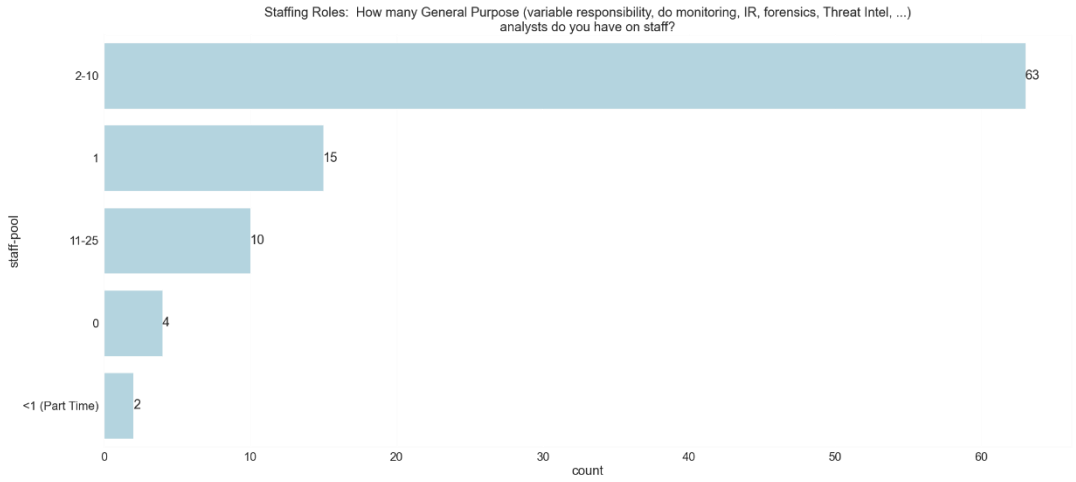

Figure Boring-3. General purpose staff (column=89)

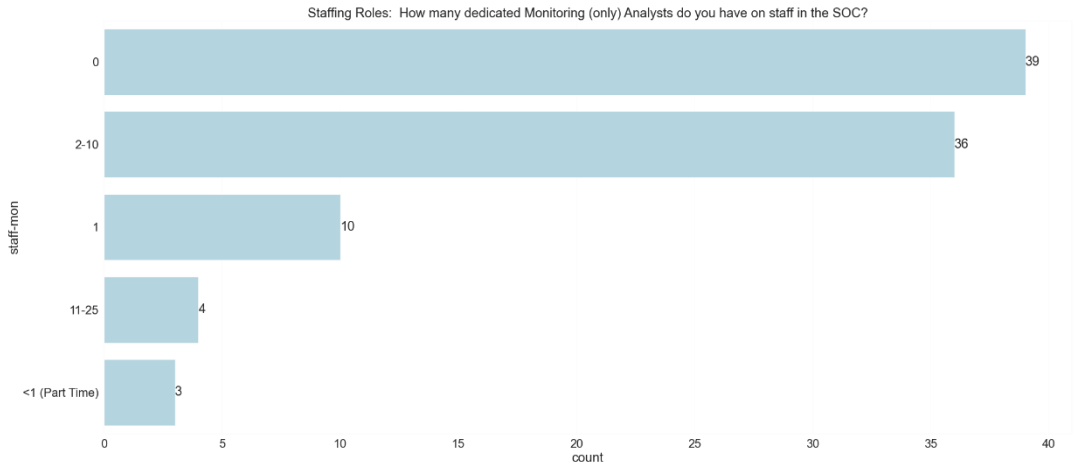

Figure Boring-4. Monitoring staff (column=90)

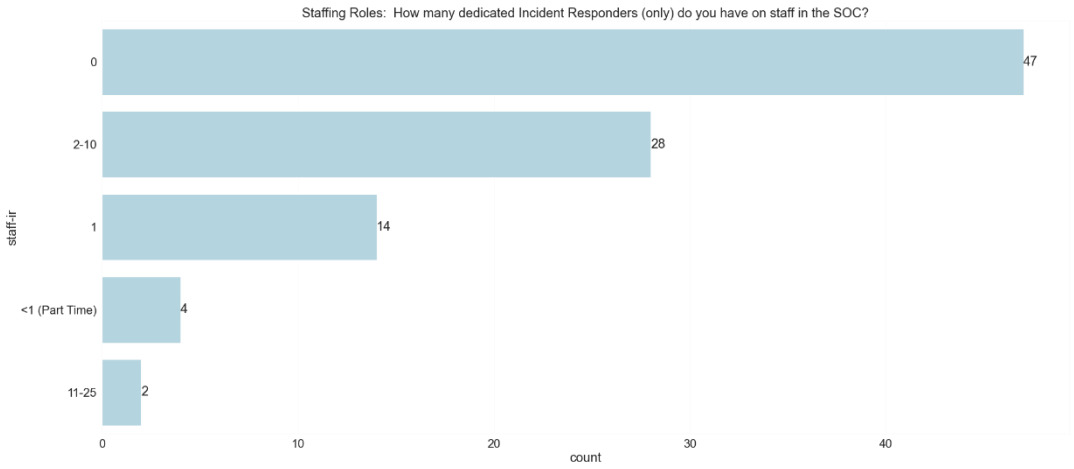

Figure Boring-5. Incident Response staff (column=91)

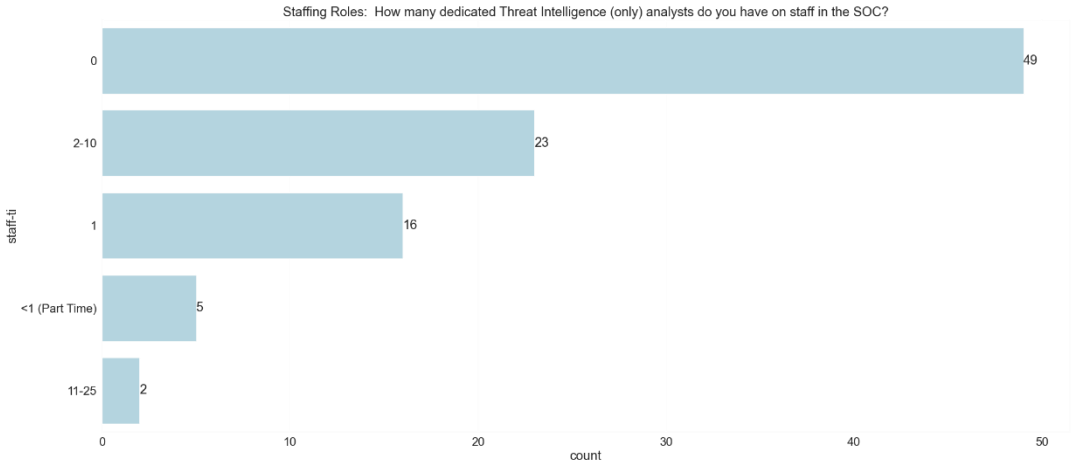

Figure Boring-6. Threat Intelligence staff (column=92)

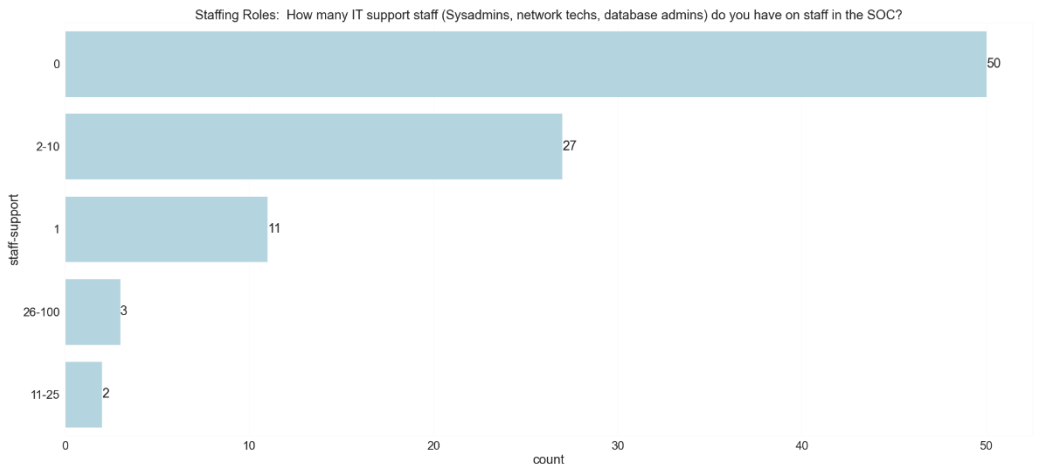

Figure Boring-7. Support staff (column=93)

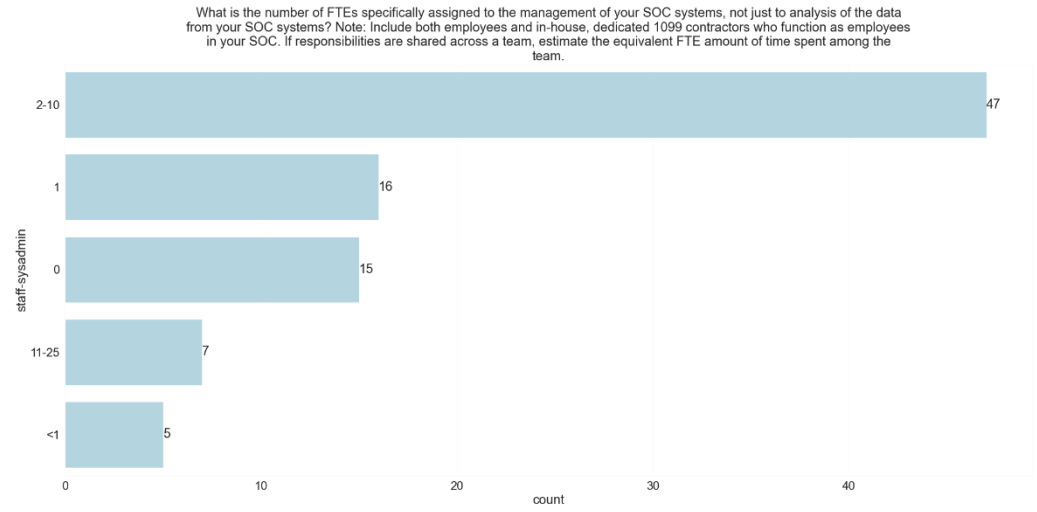

Figure Boring-8. System administration staff (column=94)

What are these systems that they're spending all this time system administrating? I'm glad you asked!

Tech and Tech (Dis)Satisfaction

The "Most As" award in technology goes to the endpoint detection and response (EDR) tools.

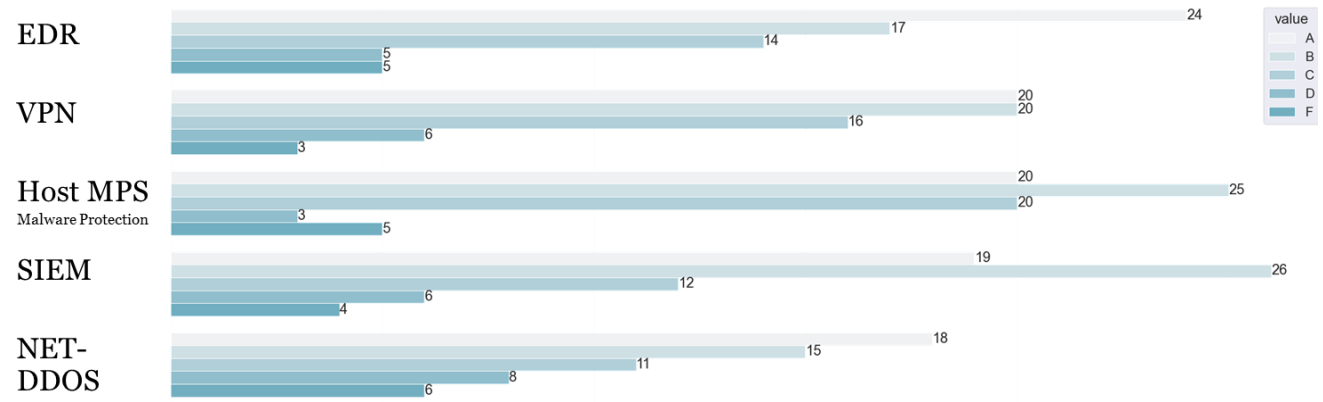

Figure Boring-9. Technology Satisfaction. Ranked by most As (columns=142-181, inclusive)

Whereas, the unwanted “Most Fs” mark goes to Full PCAP technology.

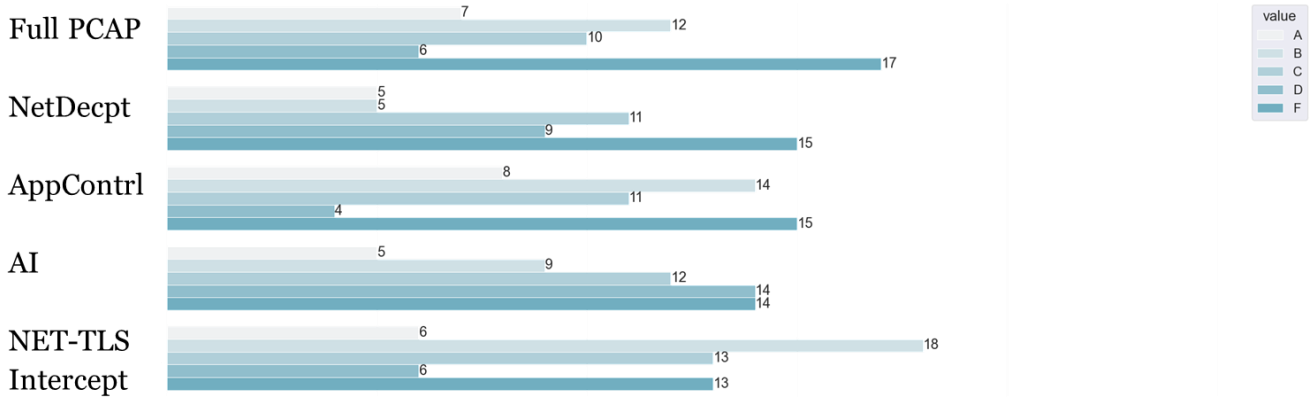

Figure Boring-10. Technology (Dis)Satisfaction. Ranked by most Fs. (columns=142-181, inclusive)

We conclude with one last plot of technology, that which is used most frequently (regardless of satisfaction with it).

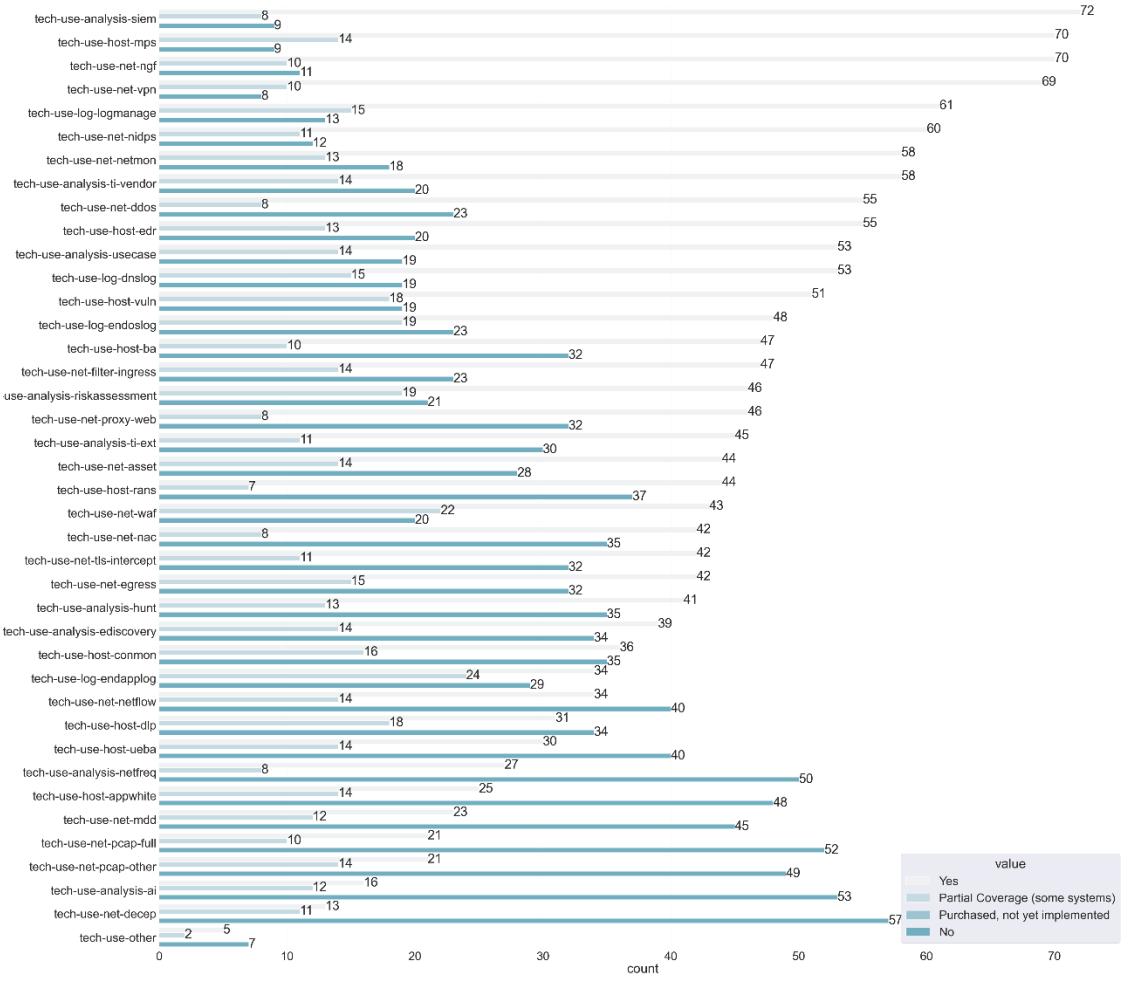

Figure Boring-11. Technology used. (columns=102-141, inclusive)

A way to use this last chart may be to assess if the SOC you work in is at least keeping up with the technology the majority of your peers (who responded to this survey) are using.

Conclusion

It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other

way—in short, the period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or for evil, in the superlative degree of comparison only.[3]

This quotation was selected to carry the theme of this report because there seems to be both aspiration and opportunity for security operations centers to accomplish massive change (in the Bruce Mau, alignment of form and design sense) for information systems globally, but are frequently resource constrained and never seem to accomplish their full potential of centers of analysis.

This paper was intended to share insight into the SOC through analysis of community contributed responses to a survey. If you read this paper, but didn't take the survey, please be sure to take the survey in 2021.

The report took a distinctive "split" in the counts of one response, and used it to pivot through the rest of the responses to see if this split made a difference. It seems to, but there isn't an absolute distinction found in the inquiries performed.

On the Cover

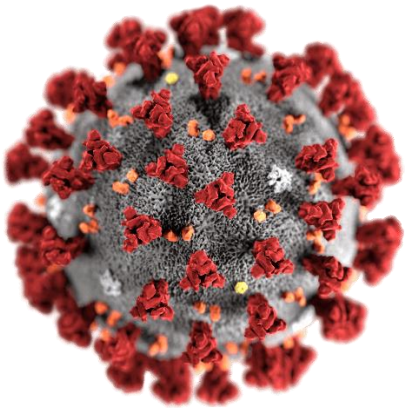

Figure OnTheCover-1. US CDC Released Rendering of SARS-CoV_2[4]
URL: https://commons.wikimedia.org/wiki/File:SARS-CoV-2_without_background.png

On the cover is a word cloud of the words in this report, using this public domain rendering of the novel coronavirus responsible for hundreds of thousands of deaths globally in 2020 as the image map. This virus influenced everything we did this year, and what we will do going forward.

Thank you to the United States Center for Disease Control and Prevention, and everyone in the safety and medical communities who have exerted tremendous effort to do everything in your power to save lives and prevent the spread of disease in 2020. You were likely frequently feeling you are operating without management (or public) support or adequate resources, but tirelessly doing your best nonetheless. Thank you.

---

[3] Charles Dickens, A Tale of Two Cities, Book the First, Chapter I. Also, https://archive.org/stream/adventuresofoliv00dickiala#page/n401/mode/2up

[4] https://commons.wikimedia.org/wiki/File:SARS-CoV-2_without_background.png