SANS

A SANS Survey

The Definition of SOC-cess?

SANS 2018 Security Operations Center Survey

Written by **Christopher Crowley** and **John Pescatore**

Sponsored by:
Awake Security

August 2018

SANS Analyst Program

Introduction

The SANS 2018 Security Operations Center Survey is intended to provide a community perspective on what security operations centers (SOCs) look like within organizations across the globe, as well as data and guidance to enable organizations to build, manage, maintain and mature effective and efficient SOCs. The pace of change in vulnerabilities, threats and business technology is much faster than many organizational cultures can deal with. However, real-world experience has long demonstrated that the existence of defined SOC processes backed by skilled personnel using effective security tools is a key differentiator between companies that see high levels of business damage due to attacks and those who avoid or minimize that damage.

Overall responses in the survey show limited satisfaction with current SOC performance, and the lack of a clear vision of excellence or a pathway to excellence. The overall view of this year's survey respondents is that most SOCs are not fulfilling expectations, although there is consensus overall on what key capabilities must be present within a SOC. Respondents also indicated consensus on which SOC functions are more likely to be outsourced to external service providers.

As in almost all security surveys, lack of skilled staff was listed as the top barrier to improving SOC performance and effectiveness. Two other survey findings directly relate to this barrier:

- **Only 54% of respondents collected SOC metrics, and most of the metrics were quantity metrics—not business-relevant effectiveness metrics.** Unclear (or absent) metrics make it difficult to convey to management why to continue to fund the SOC or to invest in increasing staff headcount and skill sets.
- **Lack of automation/orchestration, integrated toolsets and processes/playbooks were the next most commonly referenced barriers.** These three areas are critical to providing "force multipliers" to allow limited staff to identify issues, keep up with vulnerabilities and threats, and prioritize action and response.

Three other survey findings indicate critical areas where SOC processes and tools need prioritized improvement:

- **Asset discovery and inventory tool satisfaction was rated the lowest of all SOC technologies in use.** You can't protect what you don't know is there. Current and accurate hardware and software inventory is key to the entire protect/detect/respond/restore SOC mission.
- **Despite procurements of SIEM and big data products, most event correlation continues to be manual.** There has long been overpromising of meaningful event correlation by security product vendors, but the lack of integrated tools and effective processes/playbooks reduces the effectiveness of even the best of products.
- **Effectiveness of SOC/NOC integration was rated as low.** Many organizations have built and staffed NOCs for many years, and there are many areas of duplication or overlap between NOC and SOC functions. More effective integration between the two can be key to overcoming resource shortfalls.

Key Takeaways

- Metrics are used in only about half (**54%**) of SOCs.
- Only **30%** had a positive depiction of the coordination between the SOC and NOC.
- Asset discovery and inventory tool satisfaction was rated the lowest of all technologies.
- Most meaningful event correlation continues to be highly manual.
- **54%** of respondents did not consider their SOCs a security provider to their businesses (internal or external).
- The most common architecture is a single, central SOC (**39%**); **29%** have "informal/not defined" SOCs.
- **31%** of SOCs are staffed with 2–5 people, **36%** of SOCS are staffed with 6 to 25 SOC personnel, while 11% had 26 to 100 SOC staff members.
- **62%** cite lack of skilled staff, **53%** cite inadequate automation/orchestration as the most common self-identified shortcomings.

The survey also pointed out that SOCs are most often centralized into a single support organization working as security service providers. While they are centralized, these SOCS are not large: The most common SOC size (31%) is two to five people. For capabilities, 48% of survey respondents say their SOCs also include internal responders for incident response.

If you, reader, are like our respondents, you should focus on a few things to drive improvement: better recruitment and internal talent development; better metrics to be sure you're providing value to the organization; better understanding of the environment being defended; and better orchestration both with the NOC and internal to the SOC, using orchestration tools to drive consistency.

Compared with last year's survey, there has been minor improvement and no quantum state changes through technology improvement, staffing or clarity of purpose from the organization. The reality of security operations is that the winners understand "the grind," with marginal improvements being hard to win and a pace of change within organizations impeding SOC evolution. This is certainly a pessimist's perspective, with the optimistic outlook to keep fighting the good fight to demonstrate value through metrics so the organization can see what the SOC can and should do for it.

Survey Respondents Overview

In addition to the raw response values provided throughout the report, there are several graphs that compare the response values of certain questions to the industry or to organizational size. With the knowledge that we're seeing a somewhat limited view of SOCs present worldwide, we'll explore the size, composition, capability and self-assessed shortcomings of the SOCs.

Who Has a SOC?

A common question is, "What percentage of/how many organizations have a formal SOC?" This survey was not designed to answer that question, as we solicited information only from organizations that do have SOCs. Also, it is important to start with an agreed-upon definition of what a SOC actually is. Without that, many organizations will respond, "Yes, we have a SOC" to a survey.

About the Respondents

- **75%** are based in North America and Europe with worldwide operations.
- **16%** are from cyber security-related companies, 14% from finance/banking, 13% from technology and 12% from government sectors.
- **65%** are security analysts, architects, administrators and security managers.
- **43%** of respondents are from companies with workforces of less than 2,000; **39%** with workforces of 2,001 to 50,000; and the remaining **17%** from companies with workforces greater than 50,000.

The size of the organizations that took this survey varies widely, as shown in Figure 1.

Organization Total Size—Employees and Contractors (n=569)

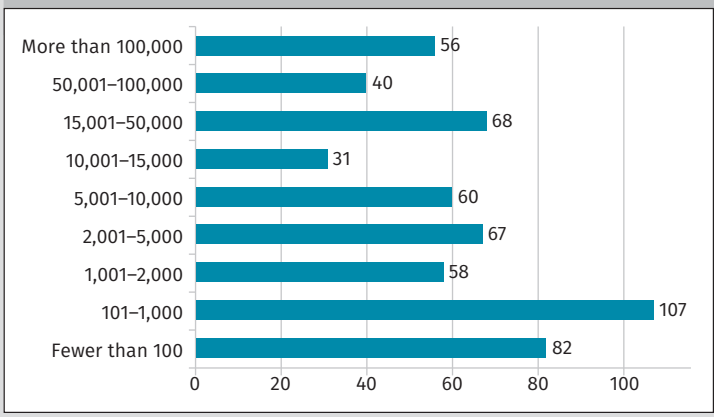

Figure 1. Workforce Size

SANS defines a SOC as: **A combination of people, processes and technology protecting the information systems of an organization through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects.**

A more meaningful question is "How many organizations have a successful SOC?" We define the success criterion for a SOC as: **when it intervenes in adversary efforts to impact the availability, confidentiality and integrity of the organization's information assets. It does this by proactively making systems more resilient to impact and reactively detecting, containing and eliminating adversary capability.**

This survey focuses on identifying the areas of SOCs that need improvement to reach consistent levels of success, but there are some data points on how common SOCs are in businesses.

One reference point on penetration of SOCs comes from Ernst & Young: Its survey of approximately 1,200 organizations (mostly large and well-funded) found 48% do not have a SOC.[1] Those figures seem in line with SANS' experience for large companies.

Another way to estimate is to consider the 285 million entities tracked by Dun and Bradstreet. If the guesstimate is that one company per 1,000 has an actual SOC, then 285,000 SOCs exist worldwide.[2] The large number of small companies drives this estimated low-penetration rate. Focusing on the largest 10,000 global companies, a SOC presence assumption of 52% (from the aforementioned Ernst & Young survey) would indicate there are approximately 5,200 SOCs in operation in medium to large companies.

SOC Capabilities

There are a lot of marketing terms in use that SANS has collapsed into the usage of the term SOC: "Fusion Center," "CIRT," "CERT," "CSIRC," etc. The title is less important than the collections of protection, detection, response and restoration activities performed. Toward this end, the survey asked respondents what their SOC does. We also asked whether they outsourced any SOC functions and/or had areas where both internal capabilities and external capabilities were used. See Figure 2.

We Do What We Do; They Do It Too

Outsourcing to external service providers is often considered when staffing and skills shortfalls exist. Outsourcing SOC functions is generally least likely to be successful when the activity requires deep knowledge of internal business flows or processes or active modification of internal systems. This is why security administration, security road map and planning, and remediation show the highest levels of internal services only.

[1] "Cyber Security Regained: Preparing to Face Cyber Attacks: 20th Global Information Security Survey 2017–18," 2017, www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf, p.14

[2] www.dnb.com/about-us/our-data.html

Externally focused services are the most likely to be outsourced, with penetration testing, red teaming and threat research having the highest levels of complete or partial outsourcing. It's worth noting that a lot of SOCs perform threat research in some form (87%) and a lot of them support penetration testing in some form (86%). Purple teaming, another poorly named and often misused term in our industry, is the least common, but is surprisingly present in the responses (70%).

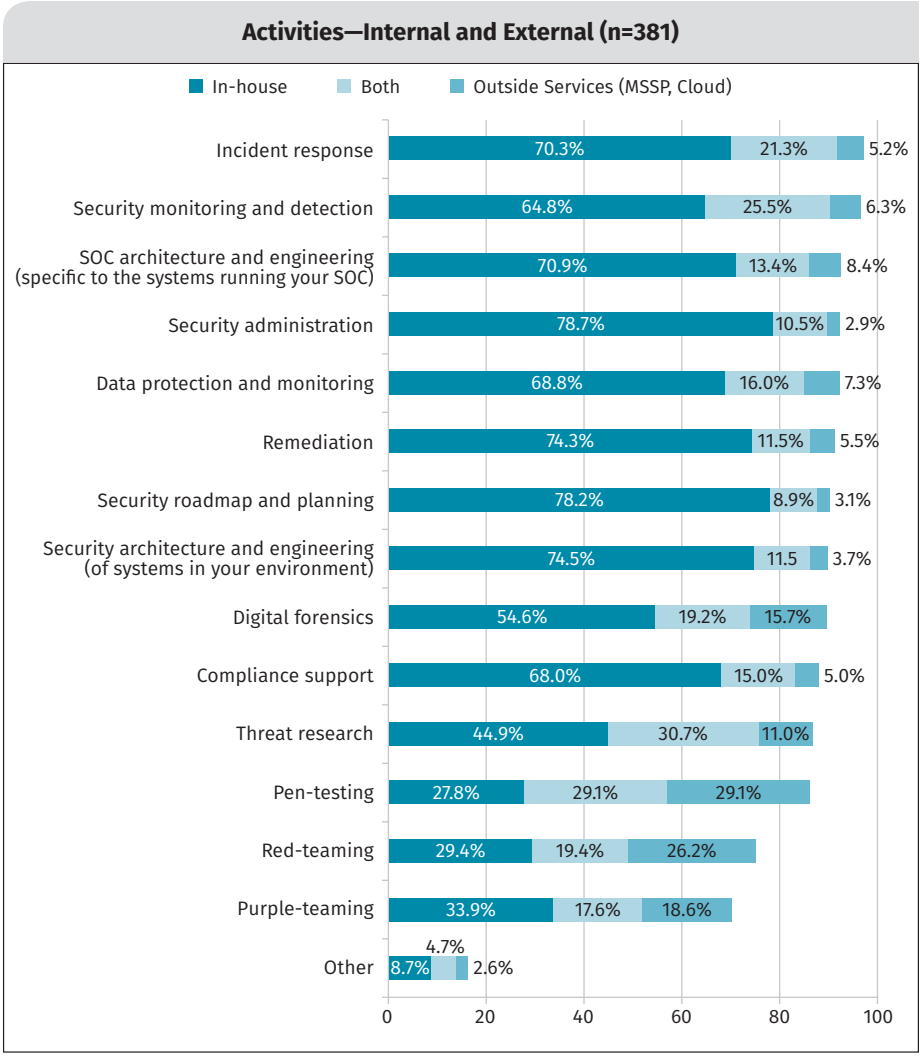

Figure 2. Internal and External SOC Activities

The purple team strategy is a combination of the red team (pen testers) and blue team (network defenders) in a hands-on assessment and detection strategy. The intention is to show the defenders all the details of the attack to verify that the attack was detected. This usually helps to assess the skill sets of the defenders as well as the most effective detection methods in the defenders' toolkits.

That ongoing assessment and integration with known breach/failure/compromise/manipulation scenarios of concern to the organization (often called *use cases*) have proven to provide high value and will continue to expand. They do two things: First they check to see whether analysts and systems are capable of doing what is expected. Second, they provide a hedge against uncertain circumstances by giving the SOC management the opportunity to indicate that the SOC was addressing all of its agreed-upon obligations. This moves the SOC out of being a catchall for uncertainty, unpredictability (nonetheless, it is the author's opinion that SOCs are responsible for handling the unexpected) and more to a deterministic machine for handling the expected but unwanted. Removing unpredictability makes the SOC easier to manage, but ultimately does not address everything an organization needs from security operations.

Pretty much everyone's SOC can and does perform response (97%) and monitoring (97%), as well as architecting and engineering security of its own systems (93%). Many architect and engineer security solutions for the systems in the environment as well (90%).

SOC Size Matters

A frequently asked question about SOCs is, "How many people do I need to run a SOC?" Hiring skilled security staff is challenging and expensive. The business culture at most companies is focused on reducing labor costs and shifting to consuming services.

In keeping with the rationale that has long been used for IT headcount, a correlation is made between the number of nodes/systems or users in the network and the number of staff required to run the SOC. However, several key things should be considered when determining the size of SOC staff:

- Threats to your market sector and targeting of your company due to regional or political alignment
- The maturity of IT operations and the resulting level of "basic security hygiene"
- Sensitivity to an impact on confidentiality, integrity and availability
- Legal, fiduciary and/or industry requirements for processing and protecting information
- Management and organizational expectations of speed and capability of the SOC
- Requirement to provide services to other organizations
- Frequency of changes occurring to the operating systems and applications running on the systems
- Funding realities

These factors can drive similarly sized companies to show widely varying metrics. For example, one company with management that has a low appetite for risk would invest in SOC skills training and tools, and would have an IT organization that minimizes vulnerabilities. It would require more full-time employees (FTEs) to do all this well. A similarly sized company with management that does not emphasize or invest in security would have fewer FTEs. Experience shows that the latter company is very unlikely to be able to meet the standard SOC success criteria, but without SOC metrics that is hard to demonstrate. The latter company is less likely to measure itself because it takes time, people and resources to do so.

The survey results indicate that the most common SOC size, with 117 responses, is between two to five people. But, when accounting for the relative organizational size, the number of FTEs goes up. See Figure 3.

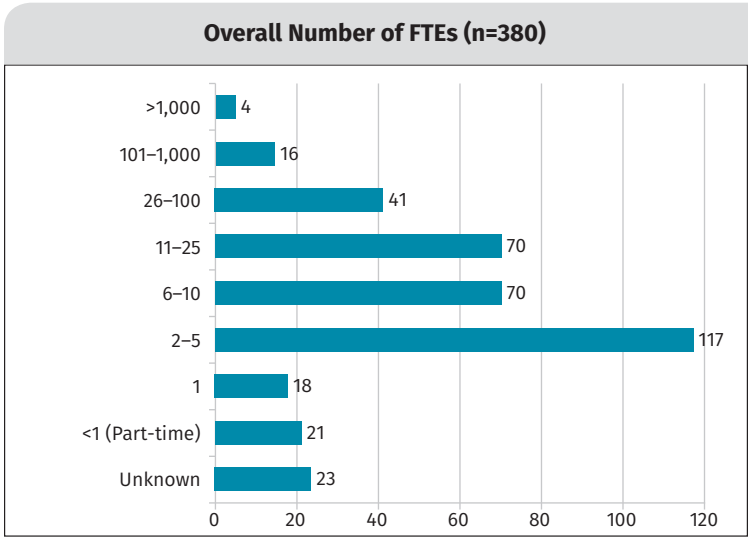

Figure 3. Number of Full-Time Employees

SOC Size—Relative to Organization Size and Sector

The SOC size relative to organization size is a decent indicator if your organization is roughly in line with other organizations your size. This doesn't account for market-specific challenges. It is one reasonable way to provide a comparison.

One obvious trend here is that smaller organizations tend to have fewer people in the SOC. The data don't show a clear answer to why this is so, but funding realities and actual demand may be strong candidates for an explanation, as is the reality that additional resources for monitoring require more staff. See Figure 4.

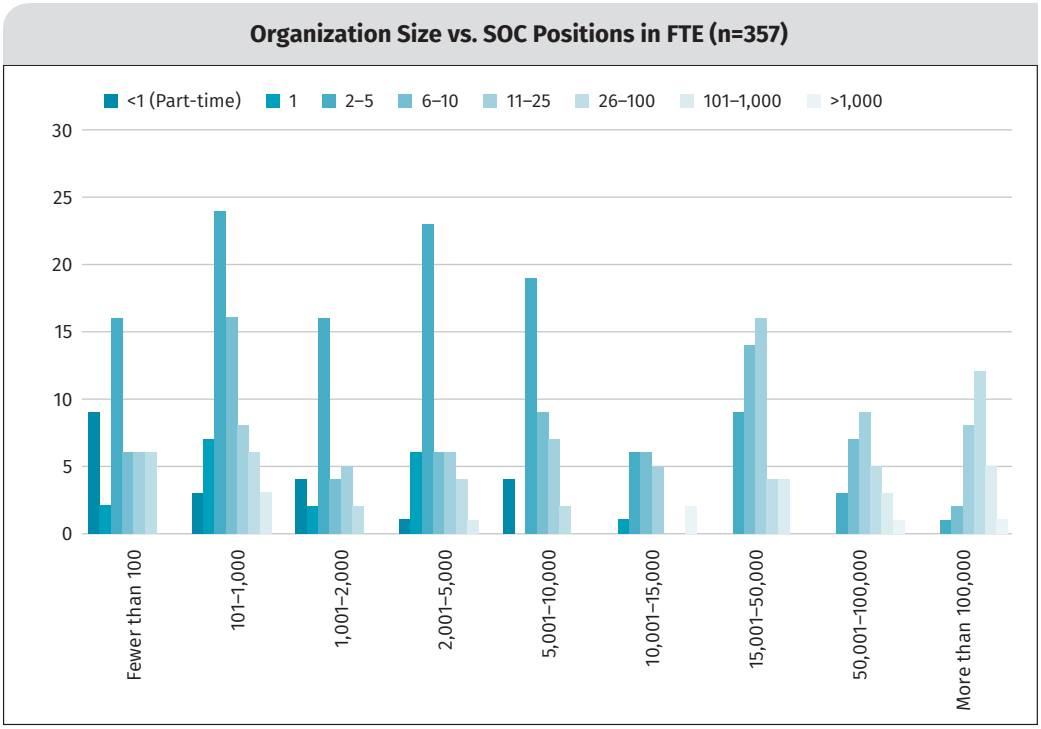

Figure 4. Organization Size vs. SOC Positions

The comparison between SOC size and market segment loses the sense of size of the organization, but helps to indicate the number of people that are being deployed to address specific threats within sectors. Larger doesn't imply more mature, however, and these values should not be used to determine what the right size is for your organization.

No clear trends in the responses indicate that a specific size is optimal for an industry. See Figure 5.

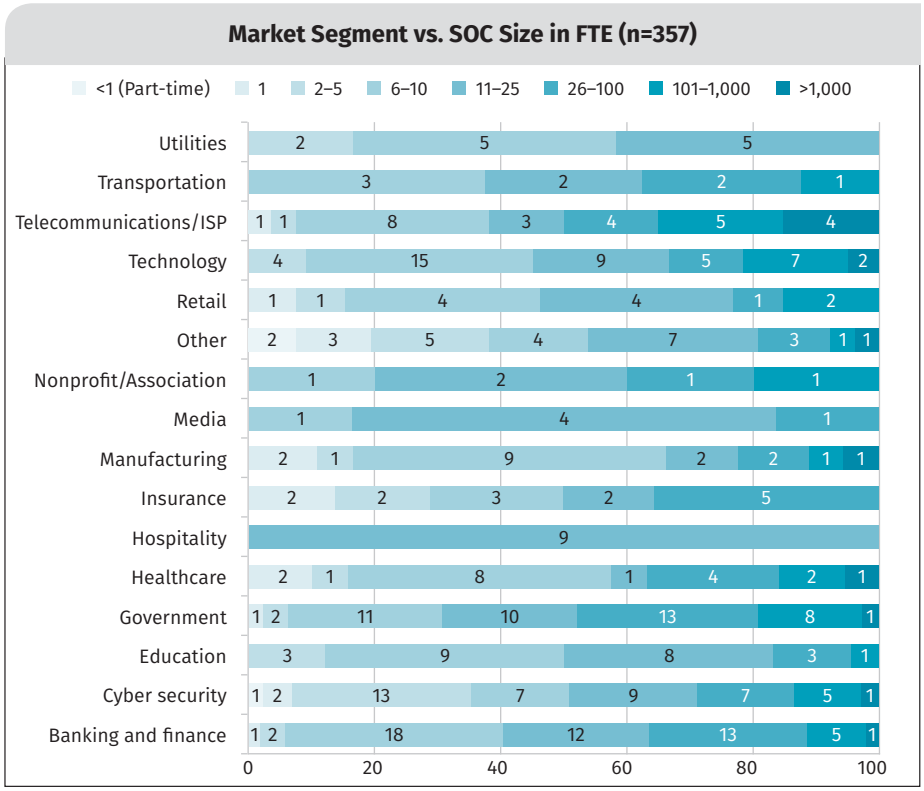

Figure 5. Market Segment vs. SOC Size

Service to the Organization

In today's business environment, internal services are often in competition with external service providers. Corporate management tries to limit direct employee headcount to core business areas, and often IT and IT security are seen more as

commodity functions. Security managers must determine how they will organize and architect SOC services with this in mind.

Overall, 54% of respondents see their SOC as an internal service organization to their business. The SOC represented is considered a service provider by 102 respondents. Of these, 53% say use of the internal SOC is mandatory, and 29% say their organizations can acquire third-party SOC management services. See Figure 6.

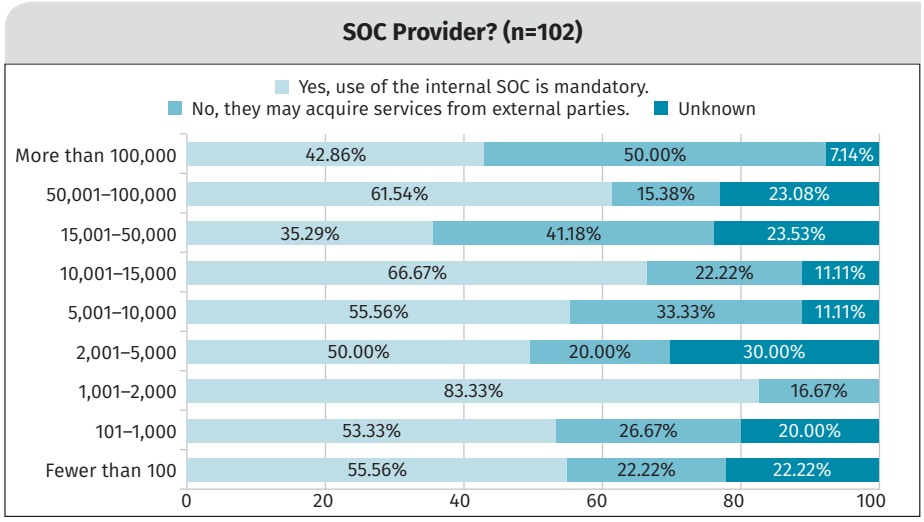

Figure 6. Internal SOCs vs. External Parties

The key to being an effective service provider is to first have stable, repeatable operations of the SOC information systems themselves. The survey covered how organizations are managing systems, and it will be discussed later.

Fundamental SOC offerings of device and network monitoring, threat intelligence, response and forensics, and system assessment are necessary. These offerings might be passed through services from other providers. The customer should be shielded from the complexity of what company is delivering the service. The customer interfaces via a single entry-point to the SOC. There should be a clear portfolio of offerings to constituents or customers with an understanding and expression of exactly what can and cannot be done. The flexibility of offering tailored services is exceptional, because it is difficult to accomplish while also providing needed stability.

Adaptability and resilience in the face of unexpected problems are other key components of what the SOC provides. Service providers with mature emergency response teams that have seen all manner of odd and unexpected situations bring calm and poise to bad circumstances. Few organizations can afford to have a staff of seasoned emergency response people. If the organization has this staff, it usually means that emergencies are happening frequently. The service provider performs drills and practices with customers to ensure that the unexpected is handled smoothly when it arrives, with the understanding that problems will arise, and the response actions will be effective but not graceful.

Service providers, internal or external, tend to develop a higher level of maturity in specific capabilities because they are selective and restrictive about what they offer for capability and technology. So general guidance is that if the organization needs faster change and more customization, the service provider model is the lesser option. In addition, if the organization wants to achieve maturity rapidly, a well-selected service provider is a jump-start to that maturity. That provider's shortcomings, identified as pain points over the time of using the provider, represent an opportunity for the provider to expand its service portfolio or for the organization to selectively change to in-house capabilities.

SOC Architectures

The architecture of a SOC can be fully centralized, fully distributed or anywhere in between. The choice of architecture should be driven by how IT and business services are delivered and managed. From an efficiency and effectiveness perspective, the worst choice is to have no formal architecture, and almost 30% of respondents indicated they have only an informal SOC and no defined architecture.

Of respondents who did cite a defined architecture, 39% reported having a single centralized SOC, and 13% reported having both centralized and regional SOCs. These numbers are very close to what the 2017 survey reported. See Figure 7.

Over the next 12 months, 7% will include cloud-based SOC services, with a predicted 1% growth in regional SOC distribution. Of those indicating changes, 47% say they'll implement a single central SOC architecture, and 7% anticipate that their architectures will be "informal with no defined architecture." These percentages are the raw numbers of respondents divided by the total number of respondents to the question. See Figure 8.

Figure 9 shows the planned change between current and in one year. Clearly the move is away from the informal. But, there's also a movement away from a single, central architecture.

The respondents' projections show strongly that ad hoc/informal SOCs are on the decline and that more cloud-based SOC services will be deployed, increasing the percentage of full SOCs distributed regionally and decreasing the dominance of single, centralized SOCs. To make this move successfully, any organizations with informal or undefined SOC architectures will

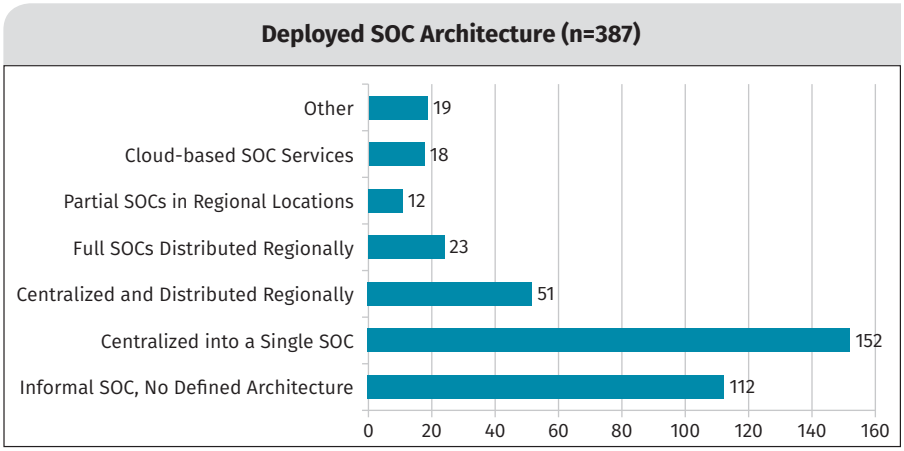

Figure 7. Current SOC Architectures

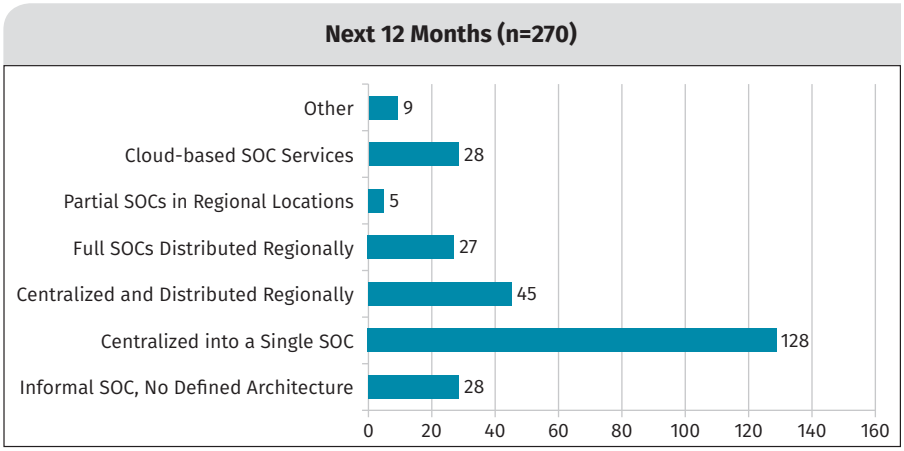

Figure 8. SOC Architecture Evolution in Next 12 Months

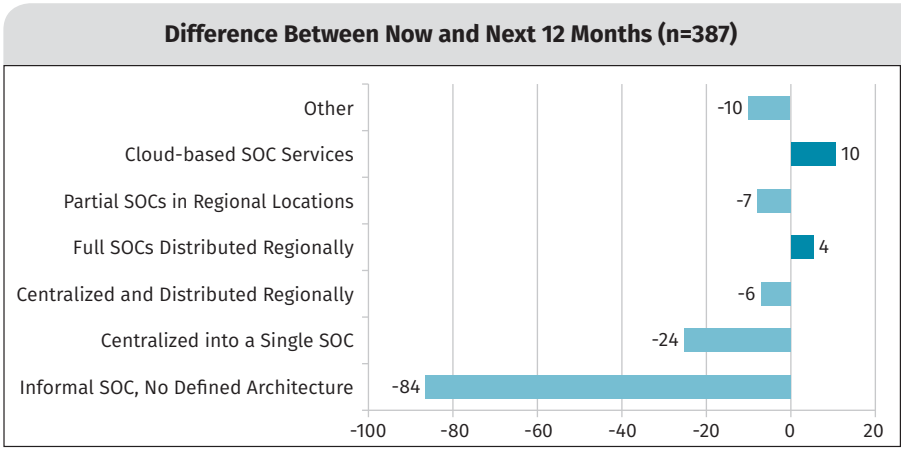

Figure 9. Planned Change in Next 12 Months (n=387)

be forced to develop a formal strategy and defined processes that will work across the distributed architecture.

As they move more toward cloud services, perhaps organizations are considering that their architectures will become more formal in the next 12 months because using cloud-based services requires formal contracts and service level definitions.

SOC and NOC Relationship

The SOC monitors the normal operations of the information systems on a near-constant basis, and there are many common or overlapping functions between operations and security. Synergy between the NOC and SOC in terms of shared information and shared goals can be a driving force for SOC efficiency and effectiveness.

However, the survey demonstrates SOC/NOC integration is a point of substantial frustration for many SOC managers and analysts. In the survey, only 14% of respondents who have a NOC report fully integrated SOC/NOC functions and workflow. At the far end of the spectrum, organizations either don't have a NOC, or the SOC and NOC are entirely separate with no relationship between them. See Figure 10.

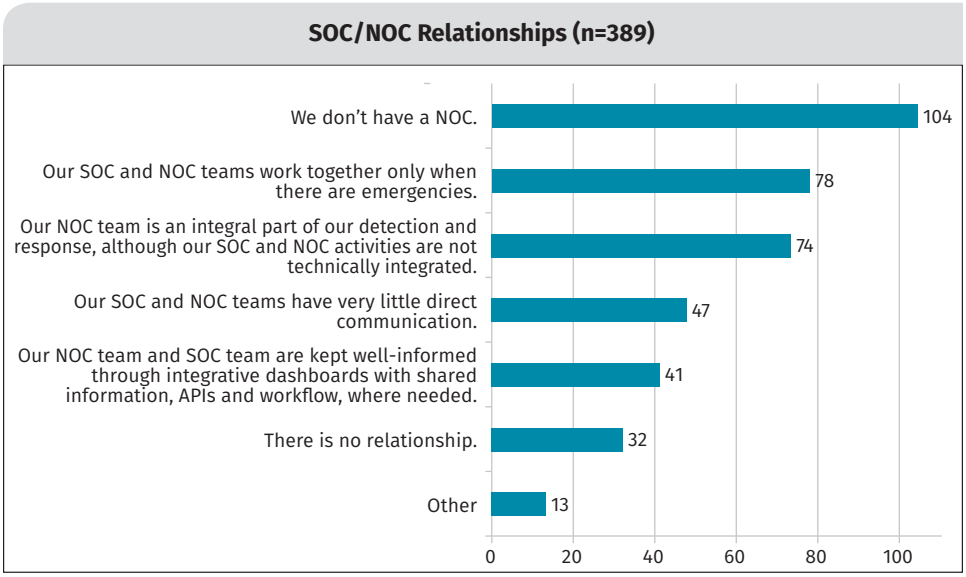

Figure 10. SOC/NOC Relationships

Of those who responded "other," five write-in responses indicated that the SOC and NOC are the same team.

Looking at the responses by industry verticals, we see that government agencies, followed by banking and finance, have the highest rate of integrated shared dashboards and information. Government agencies typically have little or no separation between IT and security operations. Because it has long been a prominent target of both cyber criminals and auditors, the banking and finance sector is typically where security best practices are found.

Measuring SOC-cess

Some people contemplate life, the universe and everything. Some people check their stock market portfolio every hour or so. Slightly more than half measure something. Only 54% of respondents stated they provide metrics that can be used in reports and dashboards to gauge the ongoing status and effectiveness of their SOC's capabilities. See Figure 11.

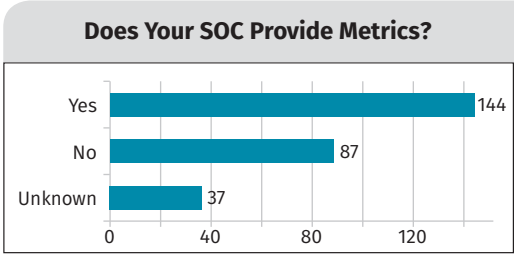

Figure 11. Use of Metrics (n=268)

That's not a good start. While security managers complain about management not providing resources for security operations, CEOs and CIOs complain about security programs always asking for increased funding but never being able to define how

much is enough or how well past investments in security have performed from a business perspective.

SOC processes and controls collect much volume-related data, such as quantities of vulnerabilities, alerts, attacks, incidents, closed trouble tickets, etc. However, these numbers have little business relevance unless connected to avoidance or minimization of business damage.

Only 54% measure whether they're SOC-cessful.

Of those that measure success of their SOC operations, the top three metrics include: Number of incidents handled, time from detection to containment to eradication, and number of incidents closed in a single shift. The second metric—time to detect, contain, eradicate, restore—can be a highly effective metric when shown over time and correlated to reductions in downtime or other business impact.

The "other" items included a couple of good ideas, including: time to act upon high/medium severity issues, phishing incident count and threat hunting-related statistics. Also, there was a little comic relief: "I'm stealing these metrics, btw," wrote one respondent. See Figure 12.

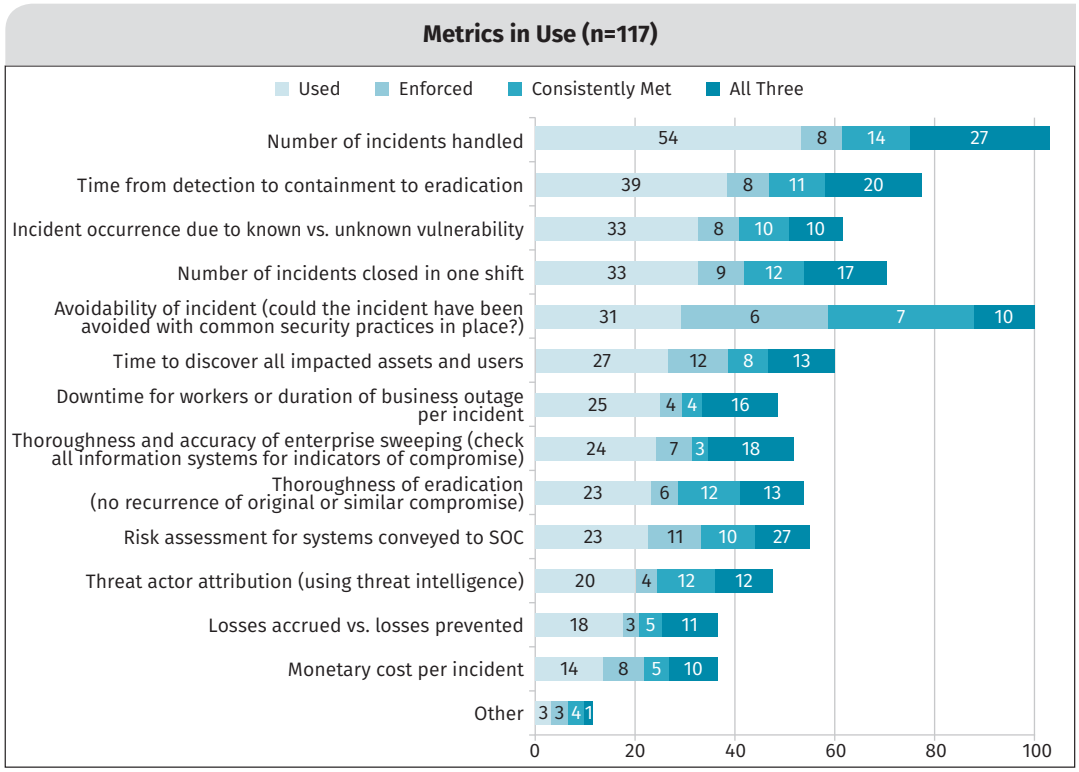

Figure 12. SOC Performance Metrics

Mostly Manual

Of these, there are not many measurements that are ranked as consistently met. But, measurement and striving to meet is at least one maturity level above not measuring at all. Furthermore, most of the respondents were stuck doing this assessment manually. To paraphrase Andrew Jaquith from *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, metrics should be derived from data that is readily available and computed in an automated fashion.[3] See Figure 13.

The good news is that it is, in fact, possible to produce a largely automated dashboard to provide ongoing visibility. How is this accomplished? Identify your data sources: ticketing system, SIEM, automation tool, customer performance feedback and evaluation, and the dashboard/reporting

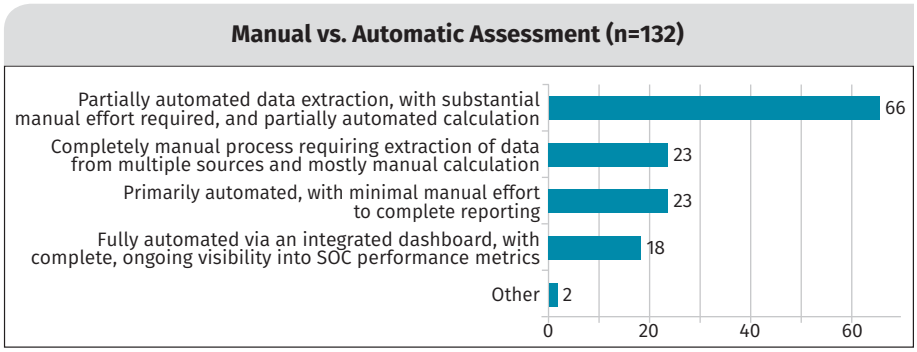

Figure 13. Manual vs. Automatic Assessment n=132

[3] Jaquith, Andrew. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Upper Saddle River, NJ: Addison-Wesley, 2010.

system that you'll integrate into. If an automation tool is in use, there are usually reports within it that can be leveraged straight away.

Start with easily quantifiable metrics that can be used as good examples of what you're trying to accomplish and have no ambiguity or need for analysis. For example, the application of patches once approved via change control within the organization. Patch release data, change approval data, software inventory control and vulnerability scan data can all be combined to show a timeline of release, approval, distribution and verification of needed change in the organization.

For something more difficult to automate, let's consider "time to detection." This is the most important metric for SOCs currently. It is considered most important by the author because it triggers a cascade of investigative and responsive actions and is a serious deficiency in most SOCs. This has been validated by the respondents of this survey, in community literature and by firsthand observation. Calculation of time to detection depends on thorough analysis of the incident. To arrive at a meaningful metric, the root cause analysis must produce data of the initial compromise time entry. The calculation could be automated if the data derived from analysis was available as part of the SIEM or ticketing system. The "initial compromise" is a specific reference to the Vocabulary for Event Recording and Incident Sharing (VERIS) schema.[4]

Artisanal, Handcrafted Snowflake Machines

SOCs are not all created equal, and many require customization and tailoring to deliver business-valuable security services. In addition to writing their own tools, respondents are also using commodity tools to perform their tailoring and customization. This effort is error-prone, labor-intensive, frequently changing, and without a clear consensus on what the tools can and should do. Furthermore, the tools must be frequently updated, repaired and patched.

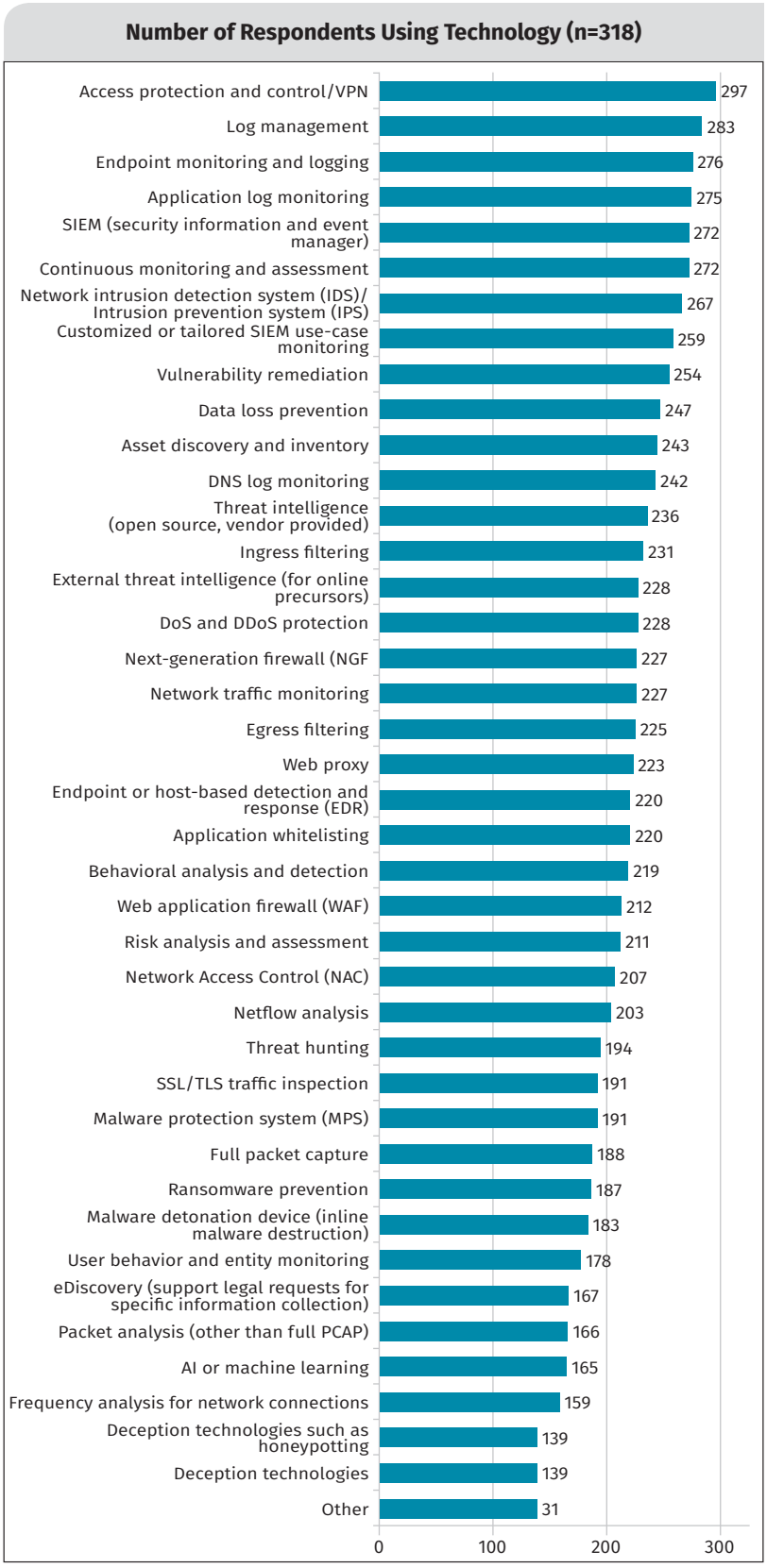

Figure 14. SOC Tools and Their Uses

[4] More information is available at http://veriscommunity.net/index.html

Organizations are using a lot of technologies in their SOCs, most of which have both preventive and detective capabilities.

If you are reading this and don't have a SOC, you can consider this an ordered list of tools that are most popular among SOCs. If you already have a SOC, you could look at the list to see if there's something you're not deploying that everyone else seems to be using. In either case, it doesn't mean the average mix is right for you. See Figure 14 to determine whether you have good risk, threat or business reasons for diverging from the norm.

(I Can't Get No) Satisfaction

No analyst in the SOC will tell you that the tools are perfect, that the tools never make mistakes, and that the tools frequently adjust themselves to account for the changing threat landscape and learn from the constantly changing business environment. Yet, marketing pitches and advertising quite often make those exaggerated claims. In SOCs, success requires a mix of skilled analysts, skilled administrators and tool curators, repeatable processes, and effective security tools.

Survey respondents indicate that a lot of room for improvement exists in the security tools they are using in SOC operations. Across the board, most respondents were, at best, somewhat satisfied or not satisfied with the various tools used to prevent, detect and respond.

Next-generation firewalls and web proxies are mature protection areas that had the highest reported overall satisfaction (B+) of those using them. However, another very mature area (asset discovery and inventory) fared the worst (F) at 59% (number of respondents: 278). This indicates an enormous problem with currently used products—the highest priority Critical Security Controls (#1 and #2) are discovery and inventory. Figure 17, a little later in this paper, addresses the methods employed to perform asset discovery.

A few other highly hyped technologies received very low satisfaction scores: data loss prevention, artificial intelligence (AI)/machine learning, and deception technologies. While many organizations are able to get security value from these technologies, the level of hype created unrealistic expectations, and there was no recognition of the skills and SOC processes required to make these technologies provide value. See Figure 15.

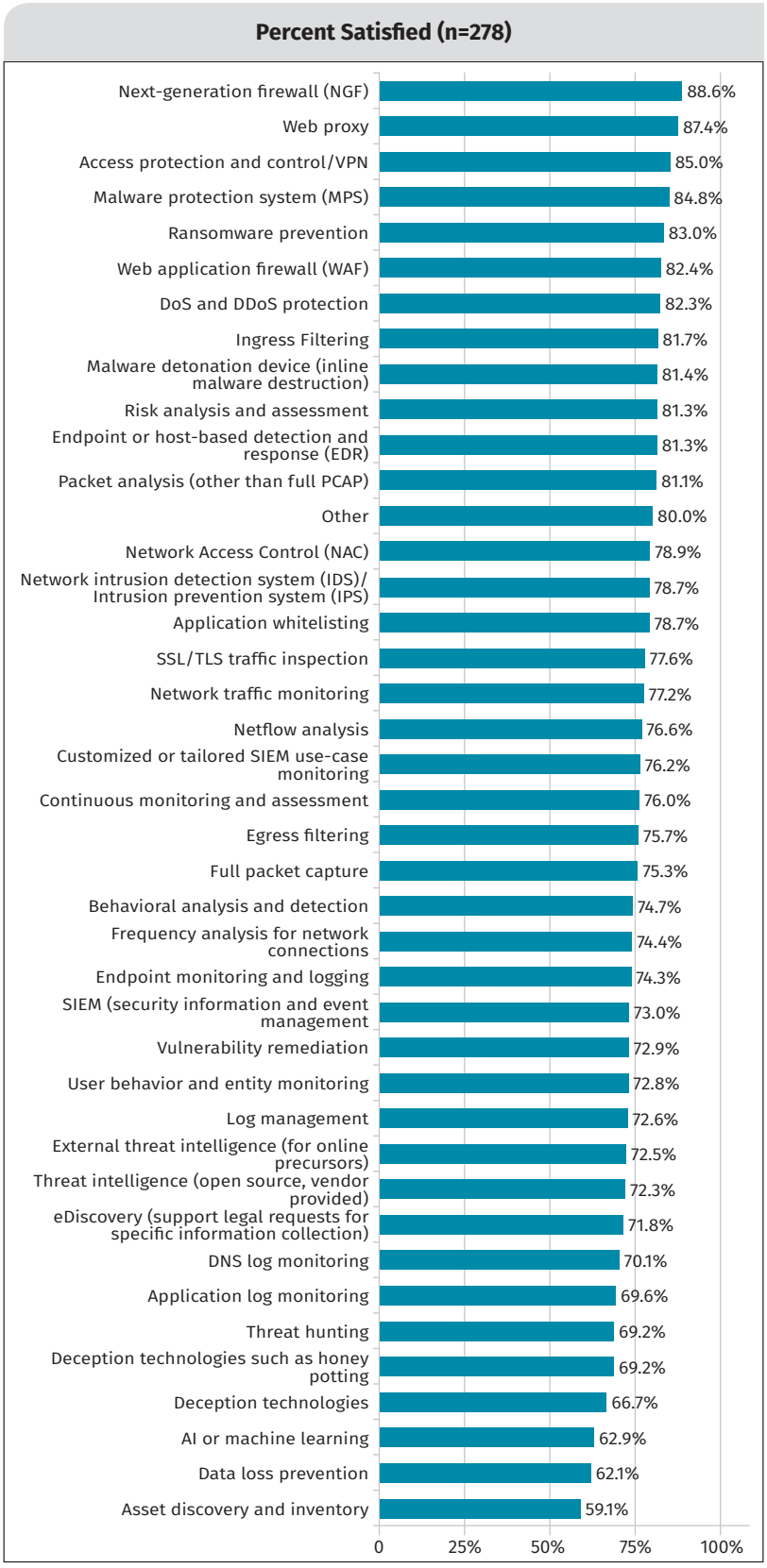

Figure 15. Technology Satisfaction Levels[5]

[5] (n=278, sort= sum(Very Satisfied+Satisfied)/sum(Very Satisfied+Satisfied+Not Satisfied)

Drill Down—Visibility and Awareness

Know thy network and software are the highest priority controls listed in the CIS, because they provide a clear boundary of defense. Enumeration of assets gives the SOC an opportunity to quantify resources and develop strategies and procedures for detecting and dealing with issues, as well as observing normal and anomalous behaviors.

The survey asked respondents how well they ranked their SOC's knowledge, including inventory of endpoints, specific IP addresses, user and responsible party. The largest group maintains such inventories on 76–99% of their assets, as shown in Figure 16.

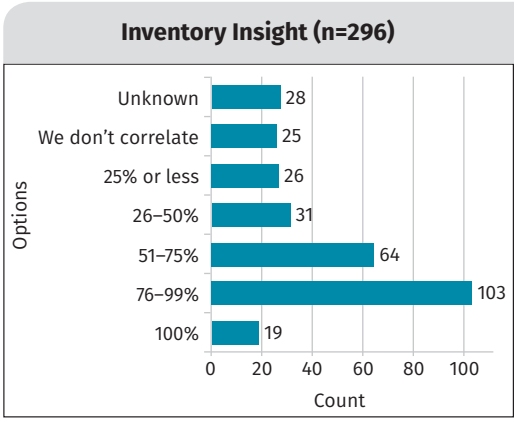

Figure 16. Inventory Insight (n=296)

Mostly, however, they managed this correlation between asset and ownership with manual methods (looking up IP addresses, checking logs, etc.) This approach is time- and resource-intensive and makes it impossible to keep up with the rate of change of hardware and software on the typical business network.

The fact that 20 respondents indicated that they have full integration between physical badging, authentication and the SIEM is impressive. This is technically feasible, but expensive and complicated to implement even in a fully enumerated network environment. The visibility and control opportunities available as a result are substantial.

The 55 responses having full integration between the authentication system and SIEM show movement in a positive direction as well. However, the high level of manual responses shows that both the capabilities of the products and the skills of the analysts using them must dramatically increase to support more automated, more repeatable maintenance of accurate hardware and software inventories.

This is an opportunity for scripting to prepopulate tables with relevant information for lookup, or integrating into SIEM or correlation engines if the SOC doesn't have full integration yet. An additional opportunity exists for real-time asset discovery and classification based on network traffic analysis. A great deal of information about every device on a network can be gleaned quickly from observed communications, which represents a large improvement in speed and fidelity of asset inventory maintenance over old-school configuration management database (CMDB) and manual approaches. Ninety-seven of the respondents have made that headway and have things primarily automated. There were two comments for "Other": One consisted of homegrown methods using available data resources such as logs and switch information, and the other considered its method undefined magic. See Figure 17.

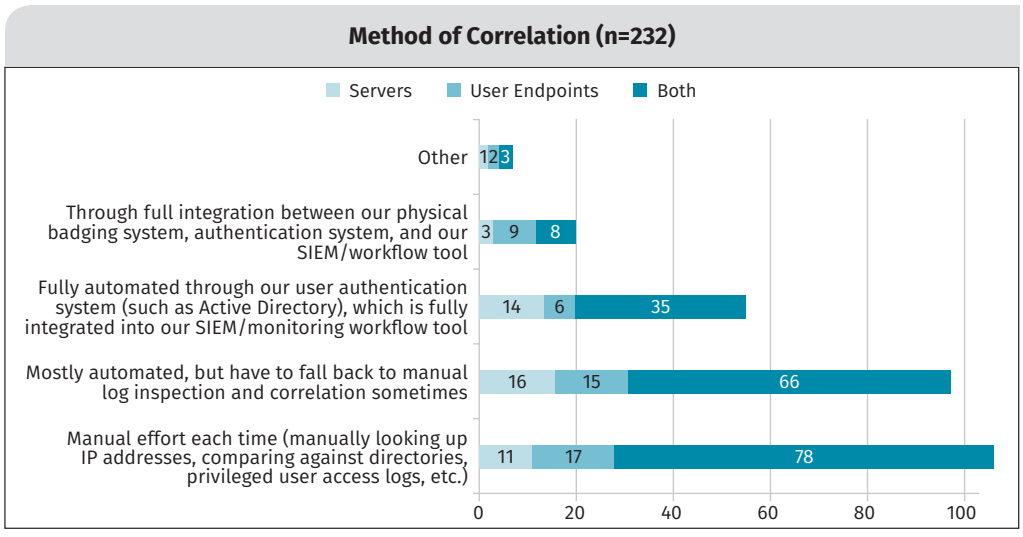

Figure 17. Asset/Ownership Correlation

Response in the SOC

Our definition of SOC success requires the SOC to take proactive steps to reduce risk in making systems more resilient, as well as using reactive steps to detect, contain and eliminate adversary actions. The response activities of a SOC represent that reactive side of operations.

What Triggers a Response

Actions that trigger the response more often start at the host (number of respondents: 192); however, triggers from the host are barely more likely than actions on the network (number of respondents: 187) with three of four respondents (number of respondents: 251) saying they would respond to either sort of alert. What's interesting here is that one of four respondents stated that an alert from the endpoint security alone isn't adequate to trigger response. See Figure 18.

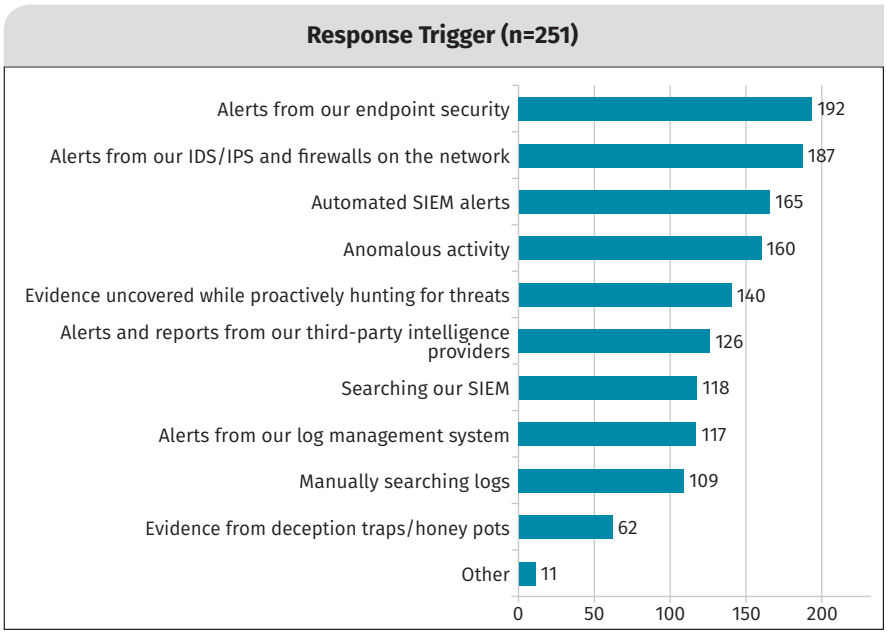

Figure 18. Response Triggers

Our hypothesis, based on other survey data, is that respondents are relying more on their SIEMs to alert them to breaches and respond to them. This is driven by the high level of noise from individual endpoint security agents, which leads to high levels of false positives. SIEMs are effectively used to filter out low-level endpoint alerts or to perform simple time/IP address correlation with network alerts before triggering a response.

Alerts from SIEMs

To correlate and analyze event data, indicators of compromise (IoCs) and other security- and threat-related data, respondents primarily rely on their SIEMs, as shown in Figure 19.

SIEM and automation/orchestration tools have improved their capabilities via enrichment from threat intelligence data sources that allow increasing the fidelity and priority of alerts that match known attack indicators. However, the low level of satisfaction from asset discovery and inventory tools indicates that large blind spots still remain.

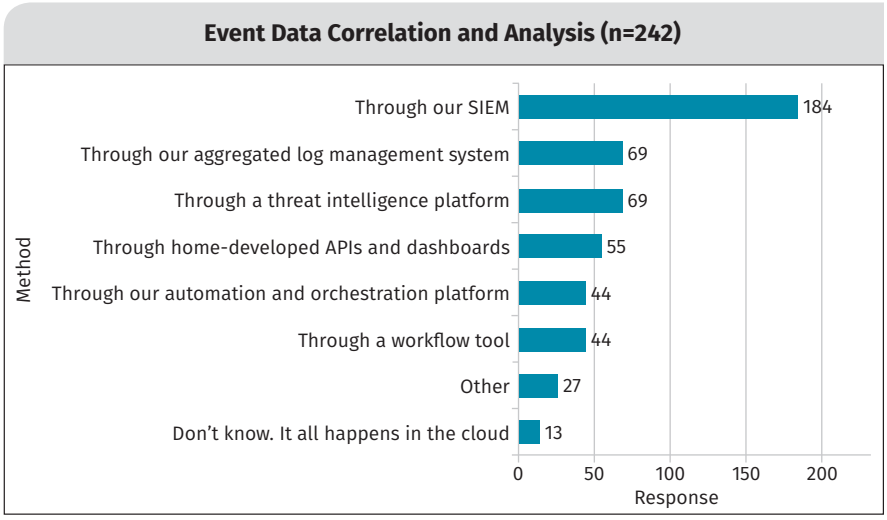

Figure 19. Event Data Correlation and Analysis (n=242)

Integrated Response

By a wide margin (2.4 times more common), respondents included incident response as a fully integrated SOC function, as shown in Figure 20.

Figure 20 also indicates that IR services are not taking off as widely as industry reports indicate. Instead, we are seeing a mix of mostly internal with some outside services used.

Satisfaction with IR Capabilities

Overall, respondents are "satisfied" but not "very satisfied" with their response capabilities. The response capabilities satisfaction fared worse than the technology satisfaction. Network forensics, which has the largest "very satisfied" and the largest "satisfied" responses, would still get a C. Malware reverse engineering, hardware reverse engineering and the use of adversary deception would get an F on the grading scale. The order of these on Figure 21 is based on the percentage of satisfaction of those using response capabilities.

At its essence, response is about bringing something out of control back under control. Response has both an investigative aspect and an ad hoc change aspect to it. To develop maturity in incident response, it is useful to separate the tasks into two categories by asking: What should I be doing to investigate the situation? What should I be doing to change my environment to stop or minimize damage right now and in the near future? Ultimately, effective response evangelizes long-term, proactive change.

Increasing response satisfaction is largely about practicing for the most feasible scenarios where control of sensitive assets will be lost or degraded. Tabletop exercises have proven to be an effective way to do this.

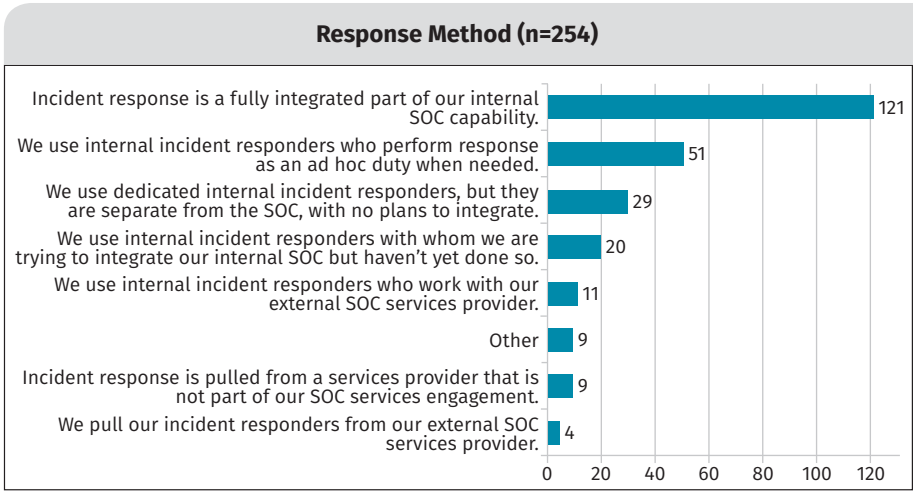

Figure 20. Incident Response Handling

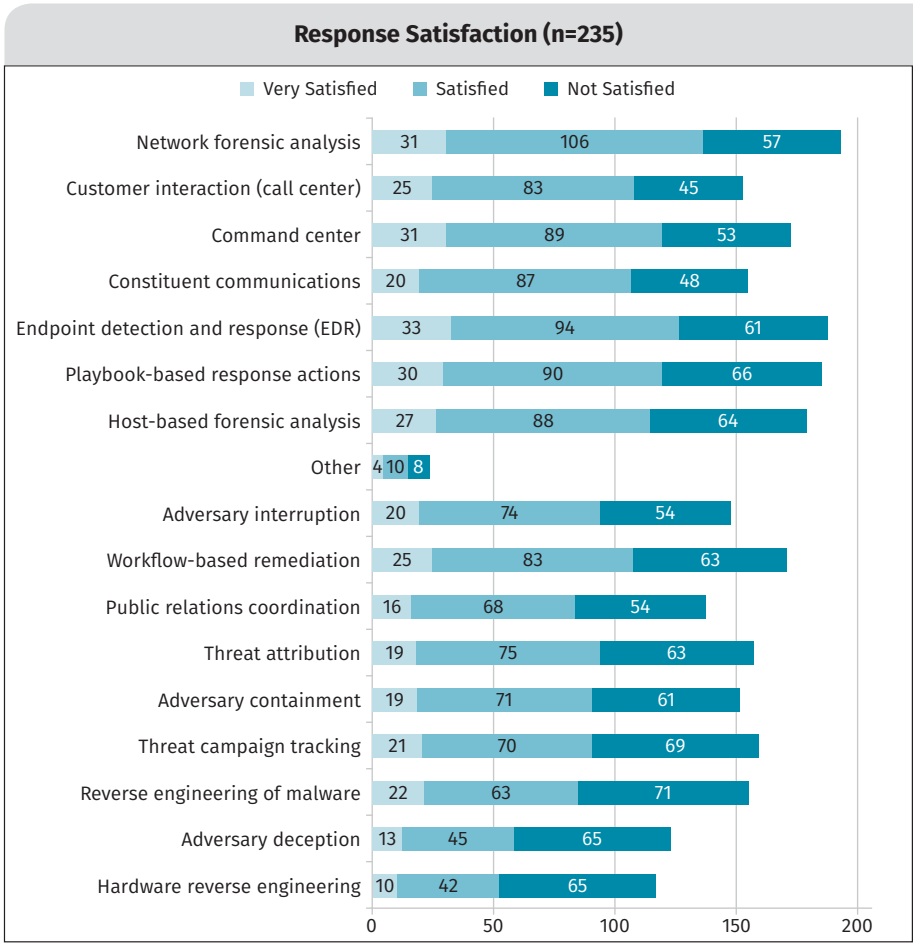

Figure 21. Response Satisfaction[6]

[6] (n=235, sort=sum[Very Satisfied+Satisfied]/sum[Very Satisfied+Satisfied+Not Satisfied])

Shortcomings

Lack of skilled staff is the most common (number of respondents: 148) reason respondents felt was hampering SOC capabilities. And of those who responded "other," three specifically mentioned lack of skilled staff.

One respondent confided it is "VERY difficult to teach green people how to rapidly synthesize volume of data to yield actionable information." Another said she was working in a SOC where, "Current staff lacks any relevant or useful SOC skill set." See Figure 22.

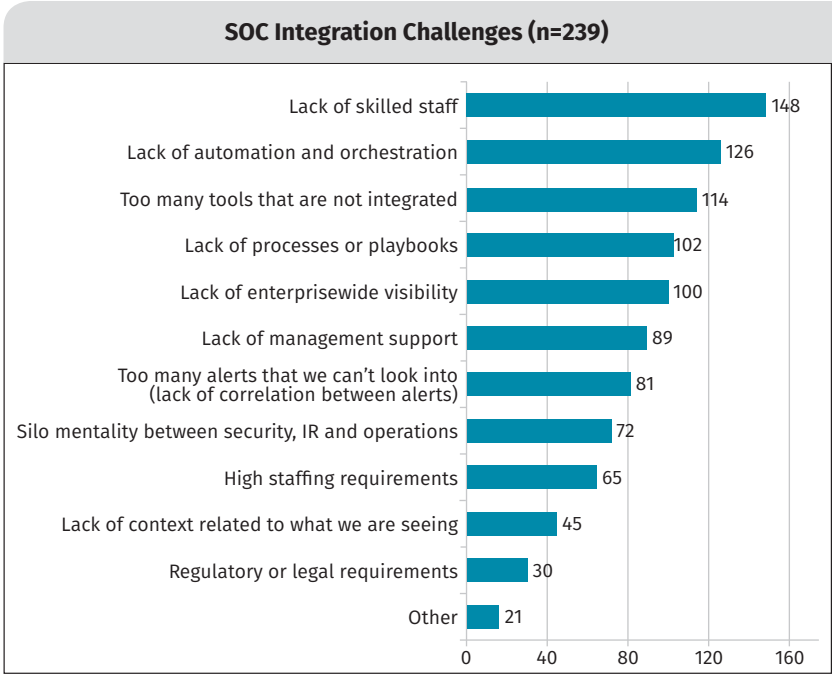

Figure 22. SOC Challenges

What's the source of the problem with finding competent and skilled staff? The difficulty is that the role of a SOC analyst requires a large amount of background knowledge and adjacent expertise to derive actionable insights from the data collected into SIEMs and other security tools. Further, human behavioral and business context is necessary to make a determination that something is unauthorized.

It is the author's opinion that most junior security staff are thrust into the role of SOC analyst with training only on what "security" is. This usually entails basics of networking, security concepts, cryptography, operating systems and a history of attacker methodology. What often isn't included is analytical methodology, such as the diamond model, or analysis of competing hypotheses. There's little training on outlier detection methodology, such as least frequency of occurrence or more complicated techniques such as isolation forests. There is rarely time dedicated to developing and honing a common analytical methodology among analysts in a single SOC. Further, there is little time allocated to trying hunting techniques, where the presumption is that the automated alerting has failed and something bad was missed and is still present.

Tier 1 SOC analyst positions are often introductory positions in the security realm. These tier 1 staff have the responsibility of looking at the information in a system and making a critical decision: "Do we need to care about this or not?" If the analyst decides the item warrants no further inspection, it receives no more attention. The analyst often has only minutes to make this determination due to the large number of items to inspect. Yet, there's rarely a clear parameter of accuracy for each decision. We hope there is a set of known cases by which the analyst can be educated on what matters and what doesn't. Very "green" staff need simple examples to develop the capability of synthesis.

A sequence of increasingly difficult challenges should be in place with known outcomes and rationale for why the organization cares about some combination of the information available. If this is done, performance can be assessed. If there is assessment capability, a drive toward improvement can be undertaken.

Some organizations have a specific hunt team. It is the opinion of the survey author that hunting is a process rather than a team. Use of a specific team to do that work is one approach to completing what is considered to be a required task for the SOC. While the data in this survey didn't specifically address this, we implore SOC owners to hunt, because the automated tools that are in use don't always turn up issues that are present. The presumption of compromise, and the failure of the tools to identify this compromise, is an important reality in the SOC. Happy hunting!

The companion to trained people is usually an automation tool, and the second most common complaint (number of respondents: 126) was a lack of automation and orchestration. These tools are available currently, with vendors at the ready to install and configure them. But the tools are infrequently combined with the right set of data, procedures and business impact, and risk information to produce effective SOC operations. Too many tools that are not integrated (number of respondents: 114), lack of process or playbooks (number of respondents: 102) and lack of enterprisewide visibility (number of respondents: 100) are complaints that exemplify this issue.

The complaints reveal something very interesting, and it is an important takeaway that most security vendors have tapped into: There's a delicate balance between human decision making through effective analysis, capture of analytical effort into the automation and orchestration, and the continued maintenance of flexibility and resilience in the face of persistent change. In our opinion, the gamification of the SOC via simulations, exercises, training or any other form of target practice is becoming the standard operating procedure for providing a SOC skill set and an effective way of retaining skilled staff. Many employees are willing to stay for the long term, even in the same job position, if professional growth and development are offered.

Who Manages the Tools?

In addition to the aforementioned trained analysts, someone (or something) needs to manage the systems that are used by the SOC analysts. This support role also consumes funding and requires difficult-to-hire-for skill sets.

The author thinks several respondents were confused by the wording of question 13: "What is the total internal staffing level (i.e., all related positions) for your SOC, expressed in terms of full-time equivalents (FTEs)? What is the number of FTEs specifically assigned to the management of your SOC systems, not just to analysis of the data from your SOC systems? Note: Include both employees and in-house, dedicated 1099 contractors who function as employees in your SOC. If responsibilities are shared across a team, estimate the equivalent FTE amount of time spent among the team."

For example, it seems odd that there are greater than 1,000 FTEs specific to system management for the SOC. That might have been interpreted as system management across the organization, but the intention of the question was to ask whether this consisted of management specific to SOC systems. See Figure 23.

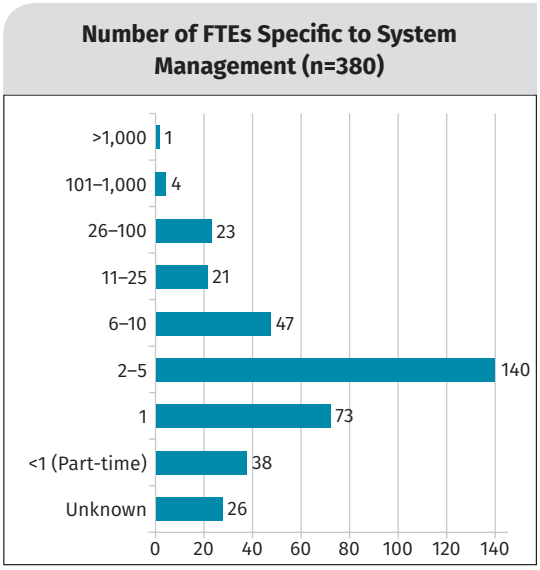

Figure 23. Management-Specific Full-Time Employees

Wicked Smart?

Smart systems hand decision making over to the machine, but hopefully only with an appropriate measure of control, so the SOC can identify and contain any missteps by the fledgling intelligence.

About 62% of the "No" answerers (**Partly, No, Not Assessed, Unsure**) say they're not monitoring smart systems. The "Unsure" answers are added to this group, because "if you have to ask, you don't know." See Figure 24.

Does your SOC support nontraditional computing devices such as smart sensors, building devices, building monitoring, manufacturing, industrial control systems, and other items considered as part of the Internet of Things?

So how does a SOC get a little peace and quiet with the smart systems running amok? There are a couple of approaches: First, smart systems usually don't have a lot of patches to be applied. So, change monitoring is a very effective way to identify compromises. Even simple scripts that take hashes of files and compare against a known baseline will detect unauthorized change. Attackers frequently change something to accomplish their objectives. Second, smart systems are predictable and fairly straightforward to provide normal baselines of activity. For example, establishing a network behavior baseline with restrictive network firewall rules is a requirement of deployment for these sorts of systems. Blocks on network firewall rules can be investigated on a daily or weekly basis in bulk using anomaly-detection methodology with the available data. It's true that anomalies may be authorized changes of the baseline that can be safely ignored after investigation, but this data shouldn't be ignored without investigation.

TAKEAWAY

Smart systems are like children: Unsupervised, they are typically able to find mischief faster than the fatigued adults thought was possible. A good SOC team also focuses on minding the "kids."

Does your SOC support nontraditional computing devices such as smart sensors, building devices, building monitoring, manufacturing, industrial control systems, and other items considered as part of the Internet of Things?

	Now	In the Next 12 Months
Partly. Our SOC supports some of our connected, at-risk smart systems.	16.8%	10.7%
Yes. Our SOC supports all of our at-risk smart systems.	9.1%	9.3%
No. We have no plans to support smart systems.	25.3%	7.7%
We haven't assessed and inventoried smart systems yet, but we plan to.	5.9%	15.2%
Unsure	12.0%	12.0%
Other	1.1%	1.1%

Figure 24. Support for Nontraditional Computing Devices Chart (n=375)

TLS Inspection

Transport Layer Security (TLS) is the standard protocol for encrypting network communications between any two nodes. TLS inspection is a means of looking into inbound and outbound communications, as well as internal communications inside the network. Inspecting TLS traffic is important, because attackers can use uninspected, encrypted traffic to secretly communicate with infected systems, conduct internal reconnaissance, and pull sensitive data from an organization. There are two deployment approaches for achieving TLS inspection: interception and out-of-band monitoring.

Interception of TLS traffic requires the network owner to install a device (hardware or software) through which all network communications between any two nodes will pass. The device receives the communications, decrypts them for inspection, then re-encrypts the communications before delivery to the final destination. This is often called a "man-in-the-middle" approach. Because interception devices must decrypt, inspect and re-encrypt communications before the final destination can receive them, they may cause a delay in communication. They often also use a less secure encryption standard than the original device, therefore introducing security risk. However, interceptor boxes can also prevent known malicious traffic from being transmitted.

Out-of-band monitoring also requires a device, but instead of intercepting communications, the network owner provides the device with a copy of the traffic via network tap or port mirror. The device can then decrypt the data for inspection, but does not slow down the transmission of the message the way a man-in-the-middle device does.

Each security organization must choose for itself whether the risks inherent in the man-in-the-middle approach are worth it, or whether an out-of-band solution is preferable. Often, the answer is some combination of the two. TLS interception via next-generation firewall can be an excellent practice for preventing dangerous connections between a corporate network and the public Internet. However, many SOCs are focusing more attention on traffic inside their own network, seeking signals of advanced attackers who have already bypassed the perimeter undetected.

Why Hackers Love TLS

Because technical implementations are difficult to conceptualize, here is an analogy for nontechnical people that explains why TLS inspection is a good idea, even though there are technical and legal hurdles to implementation. The analogy goes something like this: You're designing defenses for a physical campus. The isolated campus is ringed with a large fence that has video monitoring, with on-duty responsive guards making it essentially impassable. There are two roads into the campus. One is Cleartext Road and the other is TLS Street. On Cleartext Road, there's a guard station. Every vehicle entering the station undergoes inspection, and IDs of the people entering the facility are verified against a central repository of authorized individuals. On TLS Street, vehicles and people are free to pass without inspection. In fact, the guards may not be able to see inside the vehicles even if they wanted to!

If you were an attacker, would you travel in or out on Cleartext Road or on TLS Street? Attackers will find and exploit all available means for hiding their activity, both as they cross the perimeter and as they move about inside the campus (network) seeking valuable data to steal or destroy.

Challenges Inherent in TLS Interception

This survey's questions about TLS inspection focused mainly on the interception method, so we'll dive a little deeper into the challenges of that decision. TLS interception—a relatively mature technology—is missing from most SOCs, according to results. In the survey, only 13% had TLS interception fully working, while 43% are not using TLS interception to see inside encrypted communications. See Figure 25.

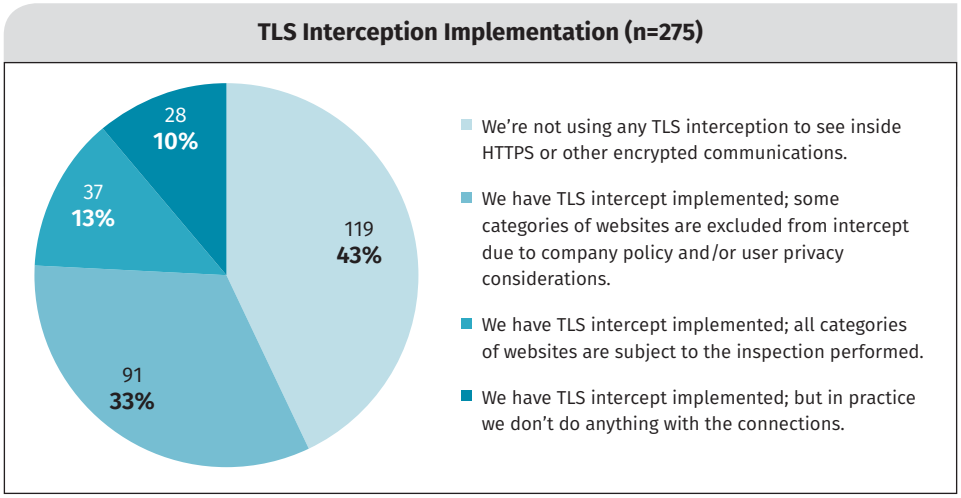

Figure 25. TLS Interception Usage

Implementing TLS interception isn't frequently performed because there are multiple pitfalls. The first issue is a legal one. Organizations may not have the legal authority to perform TLS interception due to prevailing laws. Even if an organization has the legal authority, it may not have confidence or inclination to defend that legal authority.

The second issue is cultural. An organization may choose to avoid TLS interception because it gives employees the impression that information isn't private. There will be questions about organizational inspection of private communications. In an environment where the prevailing sentiment is that everything done from organizational

assets is monitored, this isn't an issue. But consider a mixed network such as a university campus where some communication is private in nature and some is specifically related to the organization. The university might choose to avoid the effort altogether because of the perceived complexity and issues regarding how to distinguish private from organizational electronic communication.

Finally, there is technical difficulty. In short, any system connecting to the network needs a certification authority included in the certification authority repository so that it can vouch for every single website that exists. That is what allows TLS interception to work. Whatever tool (usually a web proxy or next-generation firewall) is going to implement the interception is the authority and will terminate the TLS connection, then create a second connection out to the correct website. See Figure 26.

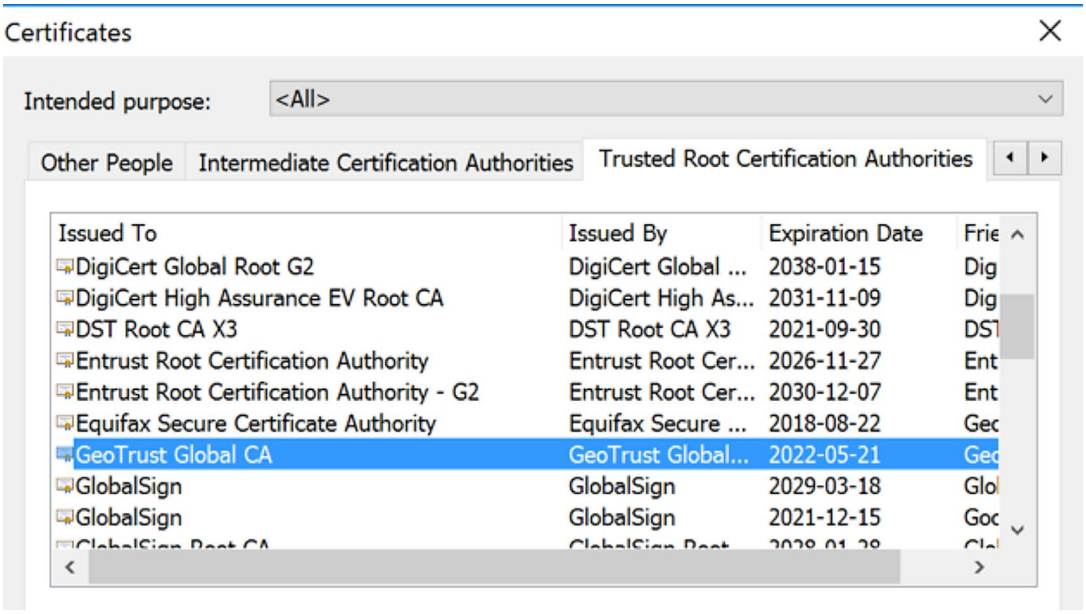

Figure 26. Certification Authority Repository

This is effective, but also technically challenging to maintain for organizations with many different types of devices, or devices that change frequently. This challenge is much less relevant when using out-of-band decryption and analysis for TLS inspection, because the out-of-band box does not need to decide whether to allow a connection. Some out-of-band solutions may still report upon invalid certificates. Another part of the technical challenge is what to do when the user's browser has a satisfactory connection to the intercepting device (web proxy, for example) but the external resource requires some interaction based on the certificate presented. There are two basic options: fail open or fail closed. Failing closed is the more conservative and secure approach, but it will anger users who don't understand why the connection isn't working. Failing open is frightening, with the intercepting device blindly accepting any certificate that might be presented on the Internet. These challenges are primarily relevant when using TLS interception at the network perimeter. Decrypting and analyzing internal traffic for signs of hidden hackers has separate challenges and benefits not addressed in this survey.

Getting the legal, cultural and technical details right takes a lot of effort and is frequently complex enough that organizations decide to forgo the implementation of TLS interception and end up with the scenario described at the beginning of the section: an unprotected and uninspected avenue of ingress and egress.

Conclusion

A leading indicator of a security program's capability to effectively and efficiently protect the business is the existence of a functional and mature security operations center. The SANS 2018 Security Operations Center Survey identified a number of obstacles security managers face in deploying and maintaining SOCs:

- Lack of effective and integrated tools
- Lack of effective asset and inventory tools
- Organizational silos and barriers
- Lack of staff and key skills
- Ineffective automation, particularly in correlation
- Unclear or nonexistent definition of SOC-cess

A key finding of the survey was that only about half of the SOCs are using metrics. Not only are meaningful metrics critical to running an effective SOC, but they are absolutely mandatory to have any chance of persuading management to provide the resources needed to overcome the barriers identified in the survey. Hopefully we'll see more SOC-cess in next year's survey!

About the Authoring Team

Christopher Crowley is a principal SANS instructor and course author for SANS courses in Managing Security Operations and Incident Response Team Management. He received the SANS 2009 Local Mentor of the Year award for excellence in providing mentor classes to his local community. Chris is a consultant based in Washington, D.C., who has more than 15 years of experience in managing and securing networks. His areas of expertise include network and mobile penetration testing, mobile device deployments, security operations, incident response and forensic analysis.

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, 11 years with GTE, and service with both the National Security Administration, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and voice systems "and the occasional ballistic armor installation." John has testified before Congress about cyber security, was named one of the 15 most-influential people in security in 2008 and remains an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this survey's sponsor: