SANS

Analyst Program

Survey

Frameworks, Tools, and Techniques: The Journey to Operational Security Effectiveness and Maturity

Written by **Dave Shackleford**

December 2023

expel

The Need for Benchmarking and Measuring Security Operations

There's an old adage in IT that says, "You can't manage what you don't know." This statement is particularly applicable to security operations: How can a security operations center (SOC) team respond to an event if they don't know it happened in the first place? Once the event has been detected, how effective can its incident response be if the cause of the problem is unknown or if the damage has been spreading undetected for weeks? To answer these kinds of questions, organizations need to aggregate and normalize thousands of security-related messages per second into an intelligent management engine, or engines, with carefully tuned rules and alerts. The SOC manages and monitors all of the relevant systems and alerts on them when necessary. A SOC watches for anomalies and ensures that the appropriate parties are called into action when an incident occurs. Today, most mature organizations have some sort of SOC defined and established.

Lack of insight into problem areas is a major challenge in many SOCs, however, along with a need for more detailed metrics and reporting to inform and help refine strategy. Organizations often try to automate many types of security controls and processes but fail to recognize that many more complex tasks (especially in detection and hunting activities that require context) don't lend themselves to simple automation. Those tasks may consistently remain immature or lacking over time. To develop a working baseline of security practices and processes, and measurably improve SOC capabilities, organizations need to focus on benchmarking and measuring SOC functions, ideally in line with industry frameworks.

In this survey, sponsored by Expel, we analyzed a wide range of SOC practices and reviewed the current state of the SOC within many organizations. In assessing staffing approaches, frameworks, tools, and techniques, this study sought to:

- Determine if frameworks are used to define, measure, and assess SOC functions, and which frameworks are preferred.
- Assess SOC metrics in use and the presence of policies and training, as well as respondents' sentiment regarding efforts to improve cybersecurity.
- Capture respondents' self-assessment for their organization's security program maturity and examine the security program components that contribute to maturity.
- Learn if benchmarking is performed and whether KPIs are useful and effective in driving improvements in security processes.

Some of the key takeaways include:

- **Over 48% of respondents' organizations take a hybrid SOC approach, employing an in-house team of cybersecurity professionals and outsourcing some SOC functions, with another 10% fully outsourcing their SOC.**
- **Sixty-nine percent of respondents' organizations use a cybersecurity framework to define, measure, and assess SOC performance, and a whopping 74% of those respondents are leveraging the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) as their cybersecurity framework of choice.**
- **The most popular metrics for measuring security operational performance include security incidents, vulnerability assessments, and intrusion attempts.**
- **Forty-three percent of respondents do not have a formal cybersecurity training program for IT/security professionals.**

Demographics

To gather data for this report, SANS conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations across industries and geographies between August 2023 and September 2023.

An interesting demographic in this survey is the range of different roles represented. The top job roles responding include security administrators, security analysts, security architects, and security managers and directors, which was expected. However, a number of executive roles are well-represented, too, including CIOs, CTOs, VPs, CSOs, CISOs, and even some CEOs and CFOs! Given the increasing focus on cybersecurity and security operations in particular, it's telling that senior leadership is weighing in and providing insights into how security operations are functioning and where these teams and core capabilities are heading in their organizations. With increasing pressure from auditors, regulators, partners, and customers to improve cybersecurity capabilities, this trend is likely to continue.

Organizations range from small to very large in size and mostly represent North America, Europe, and Asia. (Other regions had smaller numbers of responses.) See Figure 1 for a breakdown of the survey demographics.

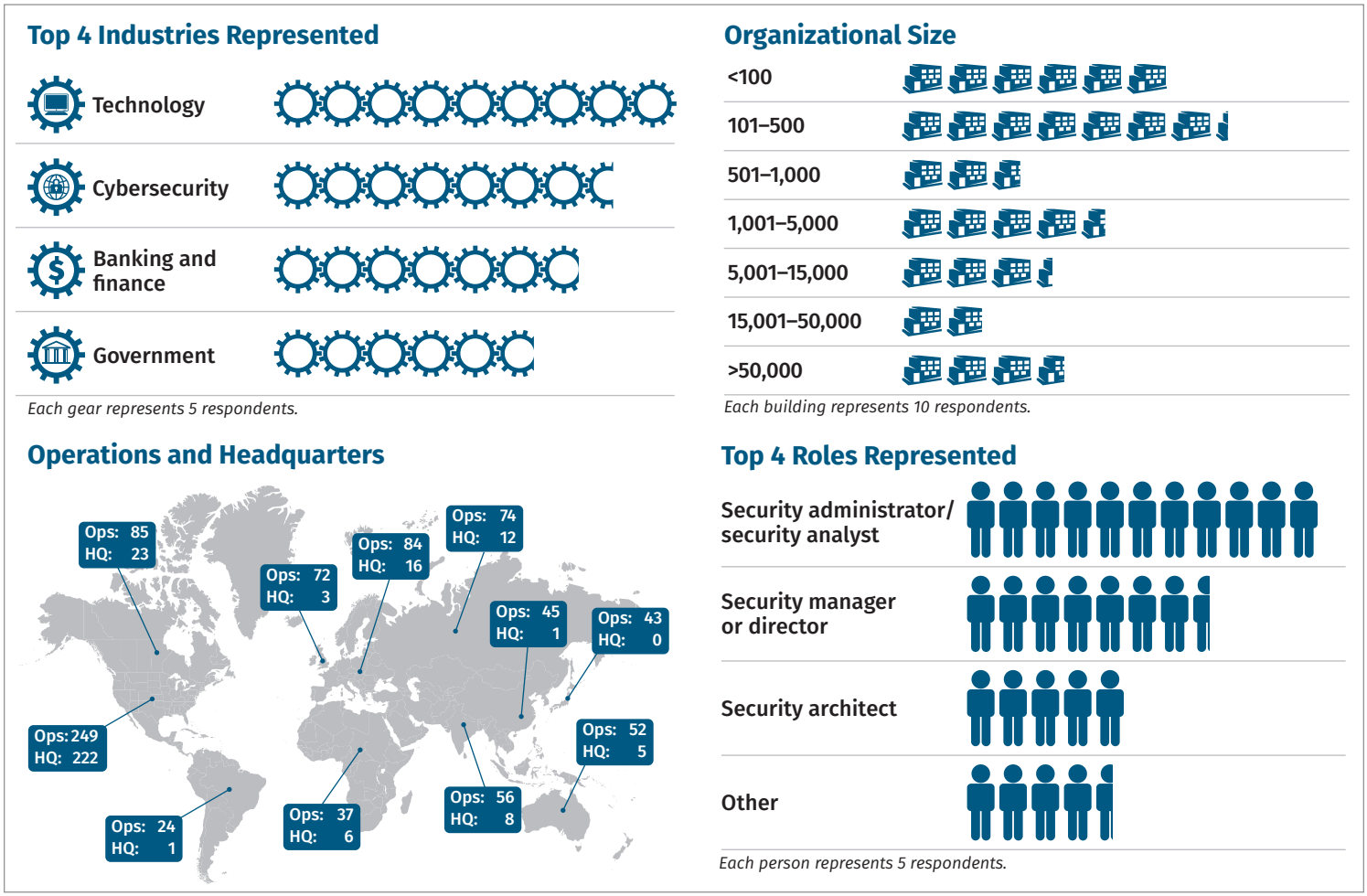

Figure 1. Key Demographics

Organization Security Operations Breakdown

One of the most common challenges SANS sees in security organizations is attracting and retaining skilled SOC analysts, largely because there aren't enough to cover the increasingly pressing needs of many organizations. Whether due to recruiting challenges, budget shortfalls, or both, many organizations are weighing the type of SOC approach they take both now and in the future. Not surprisingly, only 39% of respondents are managing their own SOC with internal staff. Nearly half (48%) have adopted a hybrid approach, which involves managed security services and outsourced SOC operations in addition to some internal detection and response capabilities. Often in these environments, a managed SOC team performs most or all tier-1 and tier-2 monitoring and escalation, with selective escalation to internal staff. About 10% of respondents have completely outsourced their SOC, and a very small number (3%) state they have no SOC capabilities now (see Figure 2).

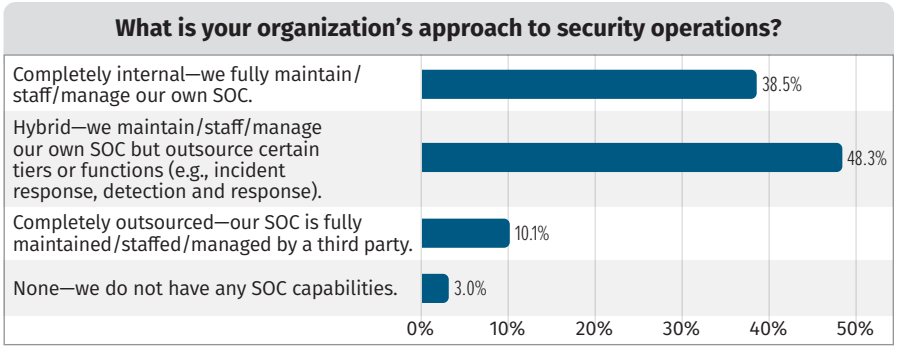

Figure 2. Security Operations Approaches

For respondents who leverage managed cybersecurity services, quite a few (41%) did not increase or decrease use in the past 12 months, but almost half (47%) increased their managed services usage—with about 16% increasing their use significantly. This trend is definitely one that we have watched for several years, and it's no surprise that organizations are increasingly outsourcing and relying on third-party services to help fill the gaps in operational coverage (see Figure 3).

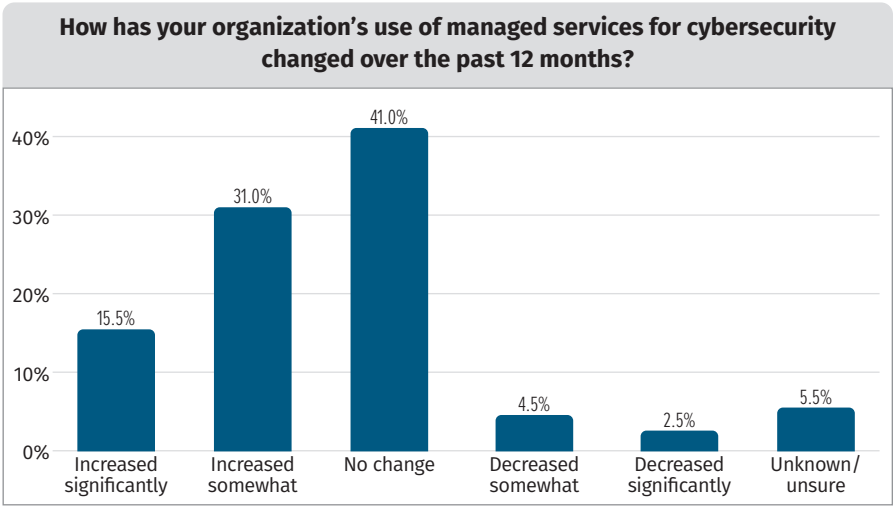

Figure 3. Changes in Cybersecurity Managed Services Use

For many organizations, using a cybersecurity framework to define, measure, and assess SOC functions makes sense. This survey found that 69% of respondents currently use a framework to help define and measure policies, processes, and controls, whereas only 22% do not. The remaining 9% are unsure whether they currently use frameworks.

Naturally, the follow-up question for those using frameworks is, "Which ones?" Overwhelmingly, almost three quarters (74%) of respondents employ the NIST CSF as their framework of choice—almost twice as many as the next top contenders (ISO 27001, NIST 800-37, and MITRE). The full breakdown of frameworks in use is shown in Figure 4.

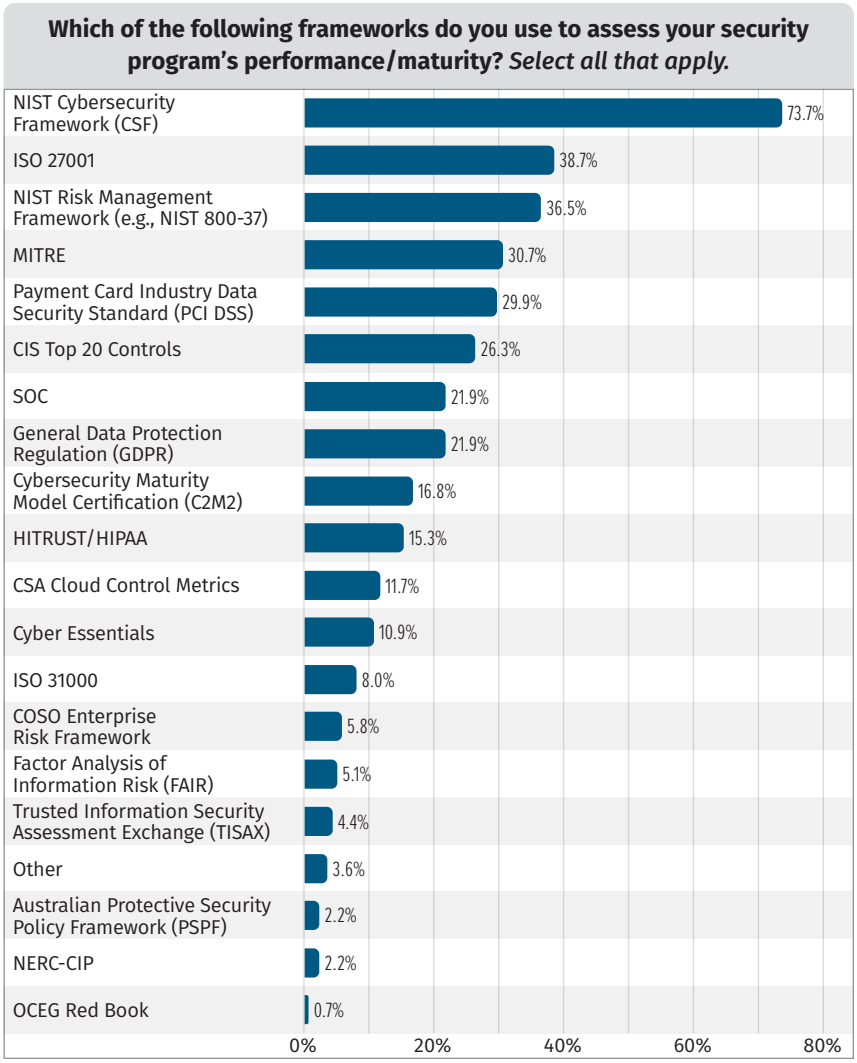

Figure 4. Cybersecurity Frameworks in Use

In many ways, this makes a lot of sense. Organizations that have definitive compliance requirements will naturally have some ties to compliance and regulatory frameworks like the Payment Card Industry Data Security Standard (PCI DSS), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP), and others. Organizations of all types find the NIST CSF to be a flexible, approachable framework that includes some definitive breakdown of measurement and maturity that can help organizations understand where they stand and where they need to develop.

NIST's update to version 2.0 is around the corner, and as we expected, a significant number of respondents plan to adopt that version. Just over 44% plan to use NIST CSF 2.0, and 10% are already starting to implement some of its new and updated controls and processes. Of the remaining respondents, 16.5% are not planning to adopt NIST CSF 2.0, and another 29% are not sure of their plans. These non-adopters may be weighing options to update at a later date or looking at alternatives. For those planning to adopt NIST CSF 2.0:

- Eighteen percent plan to adopt within 6 months of NIST 2.0 publishing.
- Nearly 44% plan to adopt within 12 months of publishing.
- About 20% plan to adopt within 24 months of publishing.

This feedback is immensely encouraging. Although SANS is neutral to one framework versus another, we believe that NIST CSF is approachable and rapidly becoming a widely used model that organizations of all types can quickly understand and begin to adopt. Additionally, we anticipate that as more organizations use NIST CSF, more users can compare notes and help to improve the level of security across industries and within the community overall. Truly, a rising tide lifts all boats, and a sound cybersecurity framework may just be that tide. We're encouraged by the use of *any* framework, because it demonstrates that the security organization is focused on optimization and improvement.

SOC Performance and Maturity

The next area of focus considers the respondents' views of their current state of security performance and the maturity of their security efforts. This includes their sentiments regarding their organization's reporting, metrics, policies, training, and more to support the overall effort to improve cybersecurity. Table 1 outlines those results.

Table 1. Security Maturity

	Strongly Agree	Agree	Neither Agree/Disagree	Disagree	Strongly Disagree
My organization recognizes that the right security policies, processes, and controls are critical to the success of its business.	43.1%	39.6%	9.6%	4.1%	2.5%
My organization actively reports on its security program using quantitative metrics/reports.	27.4%	39.6%	17.3%	9.6%	3.6%
My organization invests in training its IT/security teams at a level that meets or exceeds what is needed.	32.0%	32.5%	16.2%	13.7%	5.1%
Business leadership is accountable and active in managing cyber-risk.	24.4%	35.5%	19.3%	11.2%	6.1%

This breakdown reveals a few things:

- **Policies, processes, and controls—**Most respondents (83%) feel they have the right policies, processes, and controls defined, and the business acknowledges this. This is a good sign that more alignment between cybersecurity and business leaders is happening.
- **Quantitative metrics and reports—**Although a good number of respondents (67%) feel that they have actual metrics and reporting on their cybersecurity programs, there's a bit more hesitance. This is a maturing area that will likely see improvement in the future, but it's clear that metrics and reporting are important and in place to some degree.
- **IT and security training—**Although roughly two-thirds of respondents (65%) agree that IT and security training is meeting the needs of the organization, we'll soon see that training is not a mature area for quite a few. The more, the better, but lots of work is still to be done.
- **Accountable business leadership—**Nearly one-fifth (17%) of respondents do not believe that business leadership is accountable, which means we're still contending with business leaders denying that cybersecurity is a mission-critical element to how businesses function today. Fortunately, close to 60% agree overall—let's hope this number goes up.

We asked respondents to rate their SOC's maturity, and the responses are encouraging—although with some room for improvement. Almost 16% of respondents report the highest level of SOC maturity, with another 38% stating that SOC maturity is "somewhat mature." The rest of the responses are either neutral (21%) or generally pessimistic (24%), as shown in Figure 5.

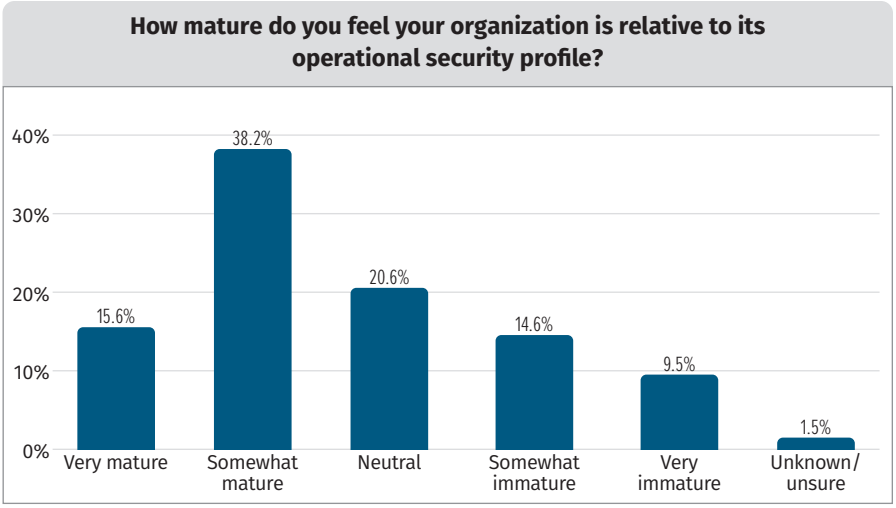

Figure 5. Operational Security Program Maturity

To get a better sense of why respondents feel their security programs are mature or not, we followed up with an open question about which key indicators would impact their opinion. Although we got a broad array of answers, there are some consistent themes:

- Most respondents feel that "tone at the top" and establishing governance play major roles in building and maintaining a strong SOC program.
- Rapid containment of threats and coordination across sites and services, including cloud environments, is pivotal to SOC maturity.
- Well-developed playbooks for detecting and responding to a variety of threats is a sign of SOC maturity.
- Ensuring the SOC has the right skills and capabilities to handle a variety of attacks is a requirement.
- High levels of maturity require the development and consistent use of SOC metrics to measure performance and effectiveness.

One area where we performed some additional analysis is around investments in managed security services based on the overall maturity of the organization. We found that mature organizations were investing in managed security services more than those that considered themselves less mature overall (see Figure 6).

These are all themes that we resonate with, leading into the next section of the survey.

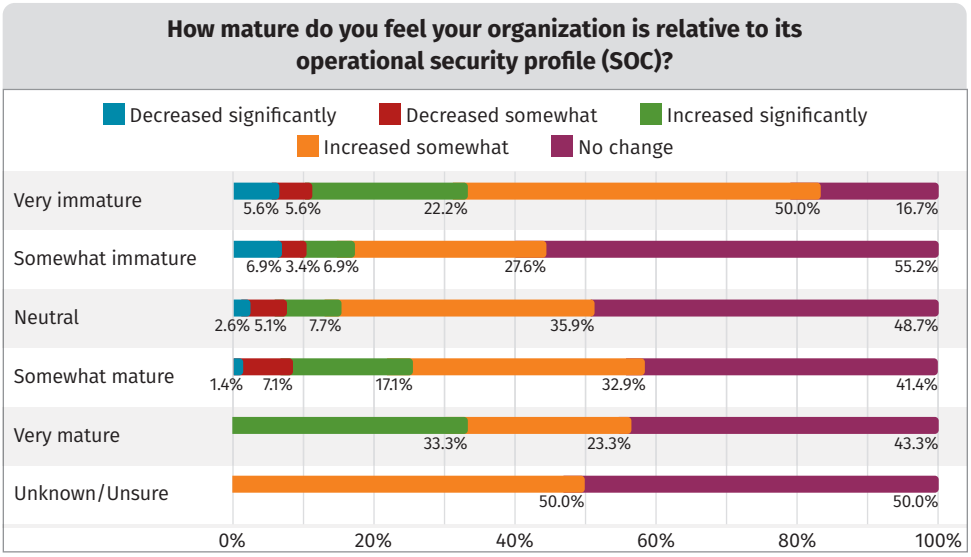

Figure 6. Changes in Managed Security Investments, Based on Maturity

Assessing the SOC and Security Maturity

Given the feedback we received relating to what many teams feel makes for a mature SOC organization, it's fitting that we followed this up with a set of questions focusing directly on those themes and others. It's always helpful to ask ourselves, "What does good look like?" when evaluating SOC capabilities, and the answers have traditionally proven somewhat elusive.

We began this series of queries with a critical topic—governance. Using a definition of *governance groups* as "a team responsible for providing organizational oversight to ensure that risks are adequately mitigated and that controls are implemented to mitigate risks as needed," we posed the question:

Does your organization maintain one or more security-focused governance groups?

Fortunately, roughly two-thirds of the respondents indicate that governance groups are effectively in place. However, of that number, only 31% of these groups consist of a cross-functional team of IT, cybersecurity, and line-of-business leadership. The rest (35%) include only cybersecurity and IT representatives. Ideally, cross-functional groups are in place to ensure that cybersecurity controls and initiatives are tightly tied to business goals, too. Unfortunately, more than 24% of respondents note that no dedicated governance groups exist, with only ad hoc or informal governance. Advancing security and SOC maturity is significantly more challenging without a sound governance structure in place, in our experience. We then asked respondents how well-defined they find cybersecurity processes to be (see Figure 7).

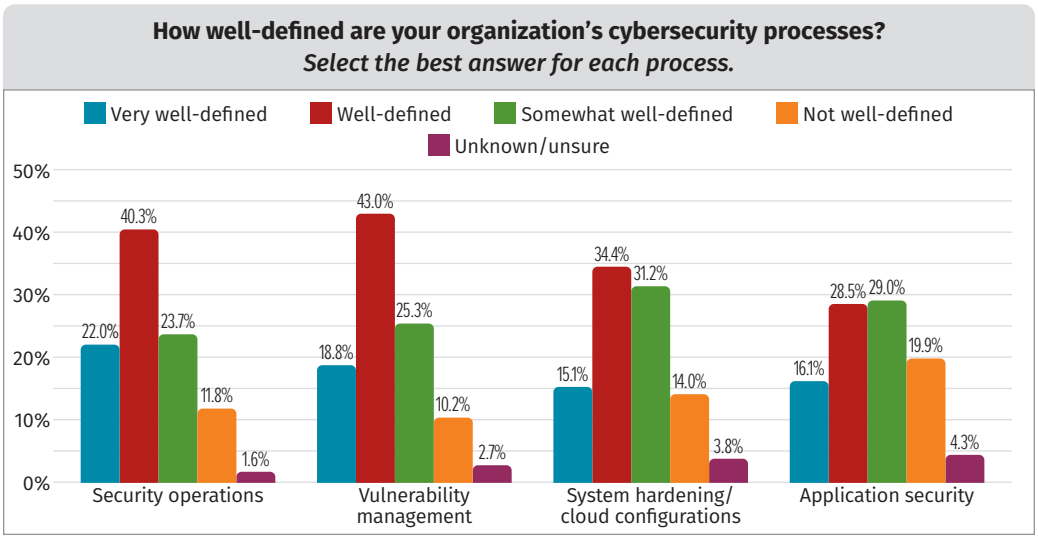

Figure 7. Cybersecurity Process Definition (1 of 2)

It's clear that many respondents feel relatively confident that security operations and vulnerability management (both at about 62%) are very well-defined or well-defined today. Given the challenges we see in the industry with configuration management (especially cloud service configuration), it's not surprising to see a bit less confidence in system hardening and cloud configuration capabilities and maturity. To be fair, these are hard. The same lack of confidence is also expressed with application security, which had the highest response rate for "not well-defined" at close to 20%.

The second set of core security processes is shown in Figure 8. Of this second group of security control and process areas, it seems there's general confidence in network security (62%) and identity and access management (IAM) (60%) being well-defined or very well-defined, with a more mixed response on pen testing and controls validation (49%). The area with the clearest lack of confidence is third-party supply chain/risk management (41%), which we see widely echoed in the community today. Given the number of recent incidents and breaches related to third-party organizations (e.g., Okta, SolarWinds, Progress Software, and so on), it's not surprising that many security and IT teams are focusing on this area.

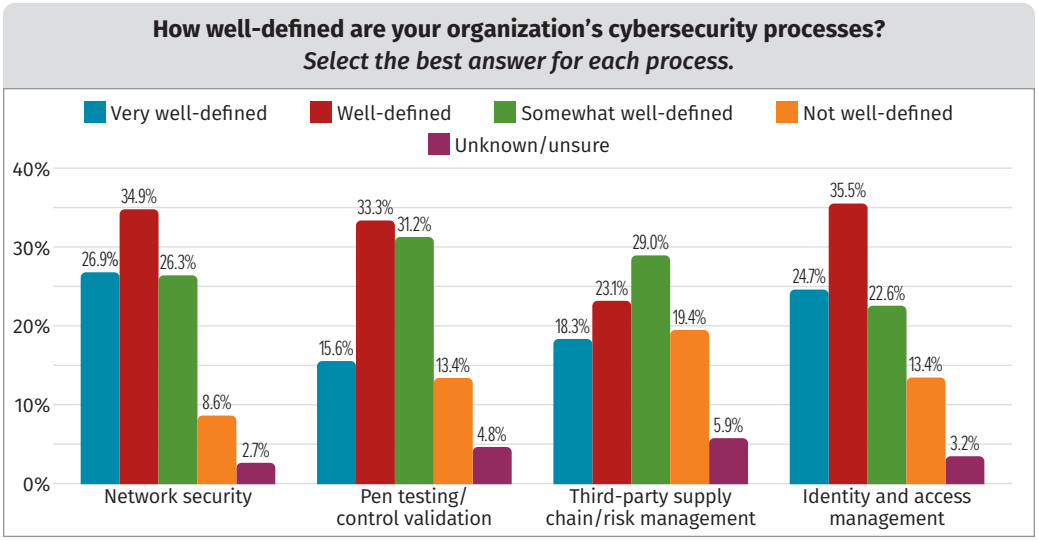

Figure 8. Cybersecurity Process Definition (2 of 2)

Currently, the majority of respondents' organizations are regularly performing some types of assessments to enhance and improve operational security capabilities. Some only perform internal assessments (21%), but most use a combination of internal and third-party assessments (54%). Just over 13% only leverage third-party assessments, and only 7% don't do any type of assessments. (This is still 7% too many, truthfully.) Those respondents that do perform assessments have done a wide variety of them in the past 12 months. Most have done risk assessments (73%), security testing (67%), and internal security audits (66%)—these are usually the most common types of assessments performed by teams, and often these are mandated by compliance and regulatory requirements. Following these leading three types of assessments, third-party risk assessments and technology vendor risk assessments are the next most cited at close to 48% each. The full breakdown of assessment types is shown in Figure 9.

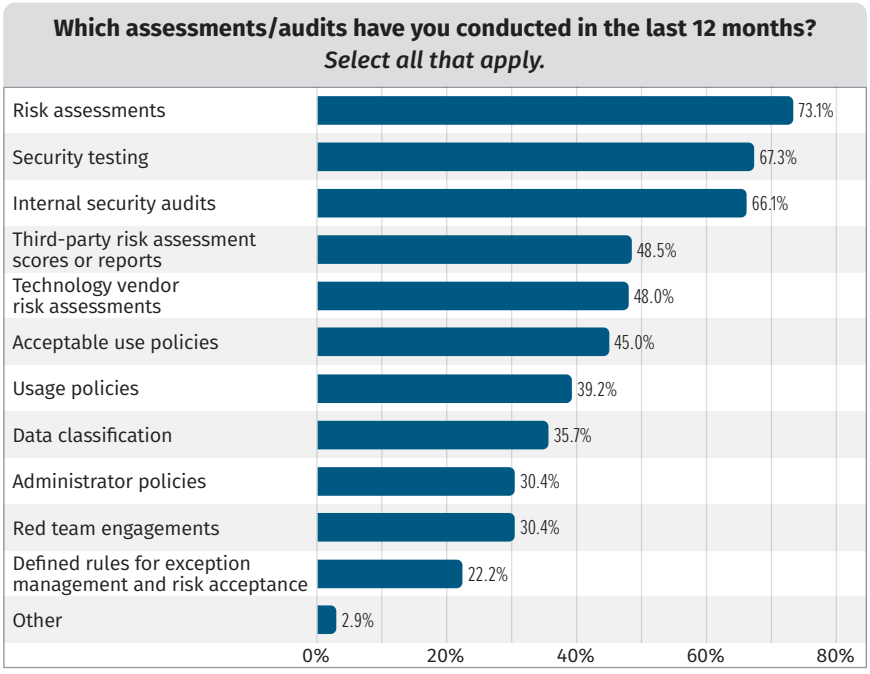

Figure 9. Assessment Types Performed in the Last 12 Months

It's somewhat interesting that policy updates of all types (e.g., acceptable use, data classification, usage, etc.) are less frequently performed than other assessment and audit types. Although policies are not frequently updated in many organizations, we expected at least some policy types to be reviewed by more organizations.

Two-thirds (66%) of respondents are currently using metrics to assess operational security performance. Just under 22% are not, and another 12% aren't sure, likely due to job roles with little to no exposure to them. For those that are using metrics (fortunately, the majority), the top three metrics collected and measured are security incidents (74%), vulnerability assessments (59%), and intrusion attempts (44%). The full list of the metrics in use is shown in Figure 10.

Let's consider some of these. It's common for organizations to track incidents, so seeing this at the top of the list isn't surprising. Intrusion attempts rank higher than expected, and this could essentially be anything—port scans, phishing emails, failed login attempts, blocked endpoint detection and response (EDR), anti-malware and/or firewall/IPS events, and so on. We had hoped to see MTTD/MTTR/MTTC a bit higher in the rankings, but these take time to develop; hopefully they'll be more prevalent in the future as organizations focus more on SOC maturity and measuring effectiveness. Threat hunting also appears lower in the rankings than we'd hoped, but again this is a developing and growing discipline that many organizations are just starting to integrate into SOC models.

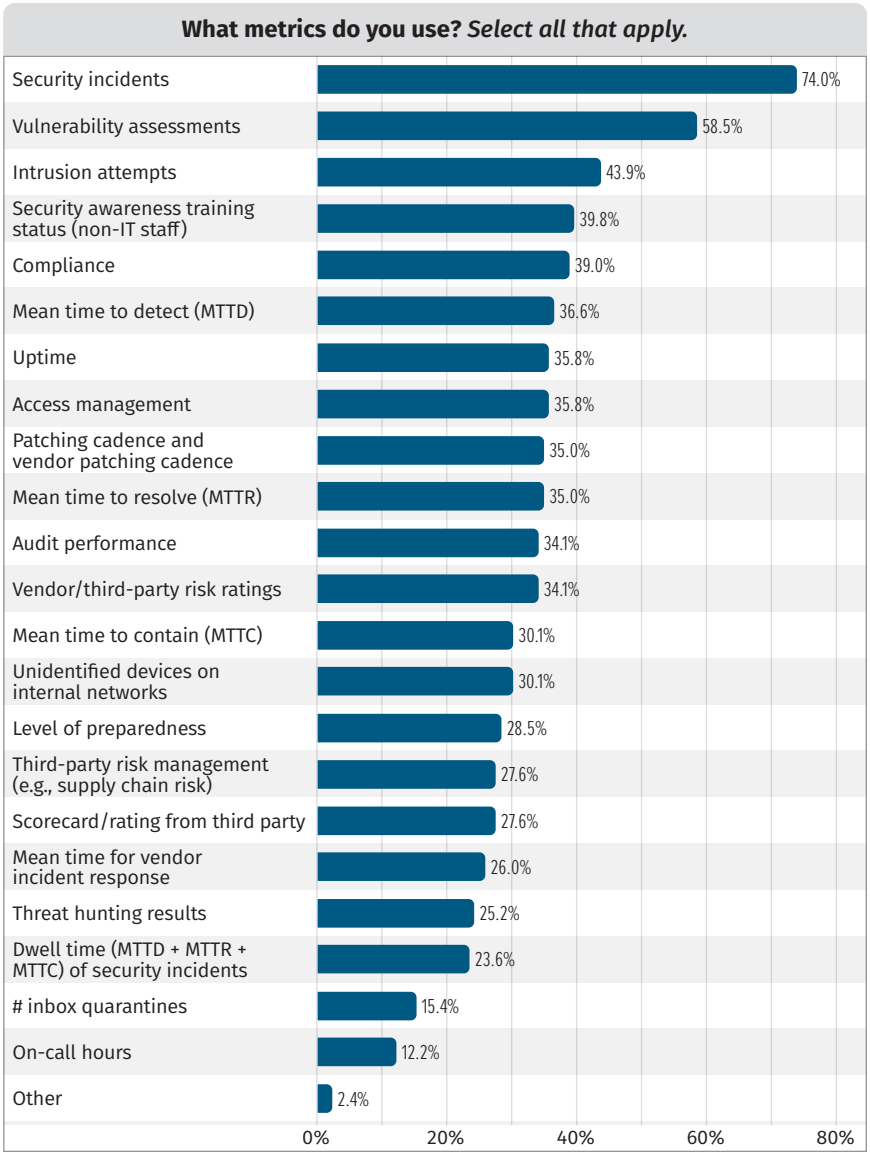

Figure 10. Top Metrics in Use

One of the more disturbing results we see is in response to whether respondents have a formal IT/security training program in place. Although 56% said that they did, 43% said "no." When almost half of respondents' organizations don't have a defined training regimen for IT and security—especially in an environment where technology is changing rapidly—it's not a good sign. For those that do have a training program, most focus on phishing and interactive self-paced training (roughly two-thirds each). However, we also see a good percentage of respondents attending training at industry events (57%), doing hands-on training with more senior cybersecurity staff (48%), and taking instructor-led training (46%), as shown in Figure 11.

Figure 11. Training Types in Use

Aligned with training formats, we asked what kinds of training materials organizations supplied to IT and security teams, as well. Most respondents note they are supplied relevant video content (73%), which correlates with phishing testing and training and interactive self-paced training. Almost 60% of respondents cite taking third-party certification exams; other options include email-based educational content (55%) (likely from subscriptions to industry and community sites) and maintaining wikis and internal knowledge centers (34%), as shown in Figure 12.

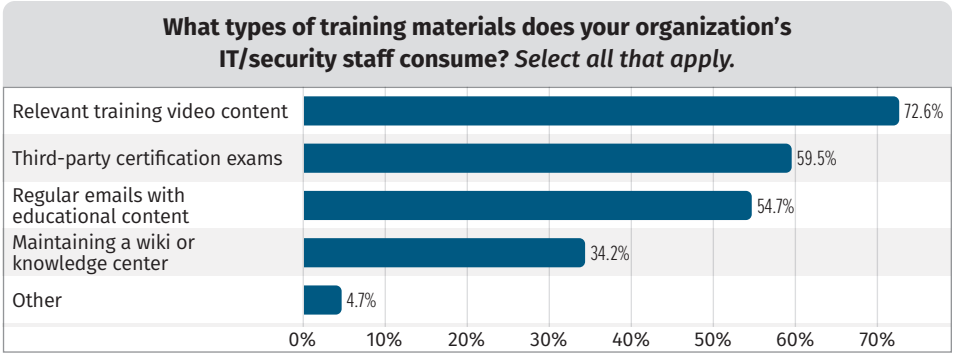

Figure 12. Training Material Formats

As everyone knows by now, one of the biggest challenges we face is educating nontechnical staff and groups. These stakeholders, who may hold extensive privileges or access to highly sensitive information, are top targets for adversaries today. Most respondents, sadly, note that their organizations conduct IT/security training for these professionals only once per year (46%). Over 21% cite this kind of training quarterly or more, almost 11% perform training for nontechnical staff twice per year, 6% do it less than once per year, and almost 9% don't train at all. Needless to say, this could be improved as well.

Along the same lines, we asked respondents whether they perform cyber-readiness exercises on a routine basis. Although 61% indicate that they do, roughly 30% said "no," and the rest aren't sure. Most respondents that do perform these kinds of cyber-readiness exercises rely on penetration tests and tabletop exercises (tied at 74% each) along with incident response testing (72%). Disaster recovery tests (56%) and red/blue/purple team exercises (39%) round out the responses. Many of these types of cyber-readiness tests are mandated by regulations and compliance, and many tabletop exercises are somewhat ad hoc—we'd like to see this number increase and more prescriptive testing be performed on a regular basis.

Although we'd like to see more cyber-readiness exercises performed, those that do perform these generally see positive outcomes, with improvements to the organization's security posture. Over 26% see security posture improvement with executive sponsorship and follow-through, and another 36% see improvements within IT and cybersecurity (but perhaps lacking in executive-level governance). Sadly, another 23% see more ad hoc improvements without prescribed follow-through, and the rest don't do this or don't know. What does this mean? Ultimately, organizations need more realistic and frequent cybersecurity readiness exercises and measurable outcomes; however, given the need for governance and operational commitment of time, it will likely be an area that sees slower growth (see Figure 13).

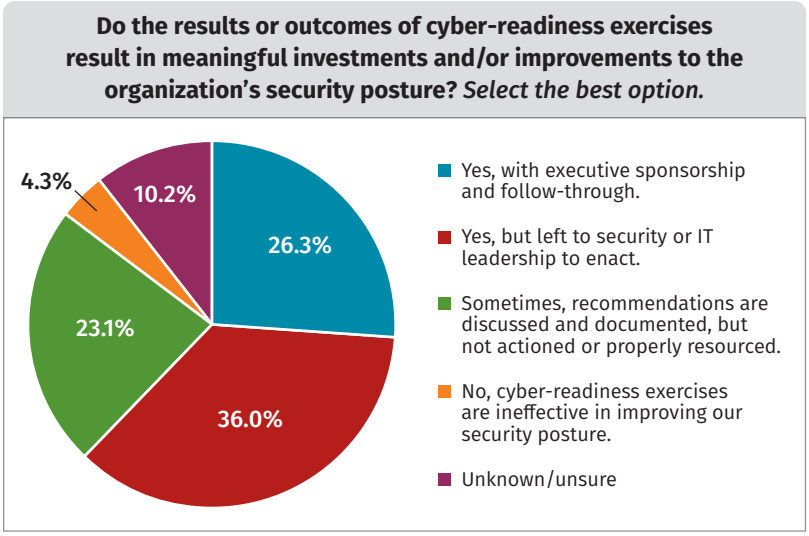

Figure 13. Cyber-readiness Improvements

We delved into the different responses to this question by role and outcome and found some interesting insights. First, the IT managers/system admins/system analysts/ etc. group and the security/ admin/security analyst/ SOC analyst/etc. group both seem less confident that cyber-readiness exercises are effective. This could be due to internal politics or a lack of cohesion between those "in the trenches" in both IT and cybersecurity. In addition, the CIO/CTO/VP group sees themselves as helping drive the outcomes, which naturally ties back to sound governance and program execution. The business manager/CEO/CFO/COO group generally feels confident in these exercises, as well (see Figure 14).

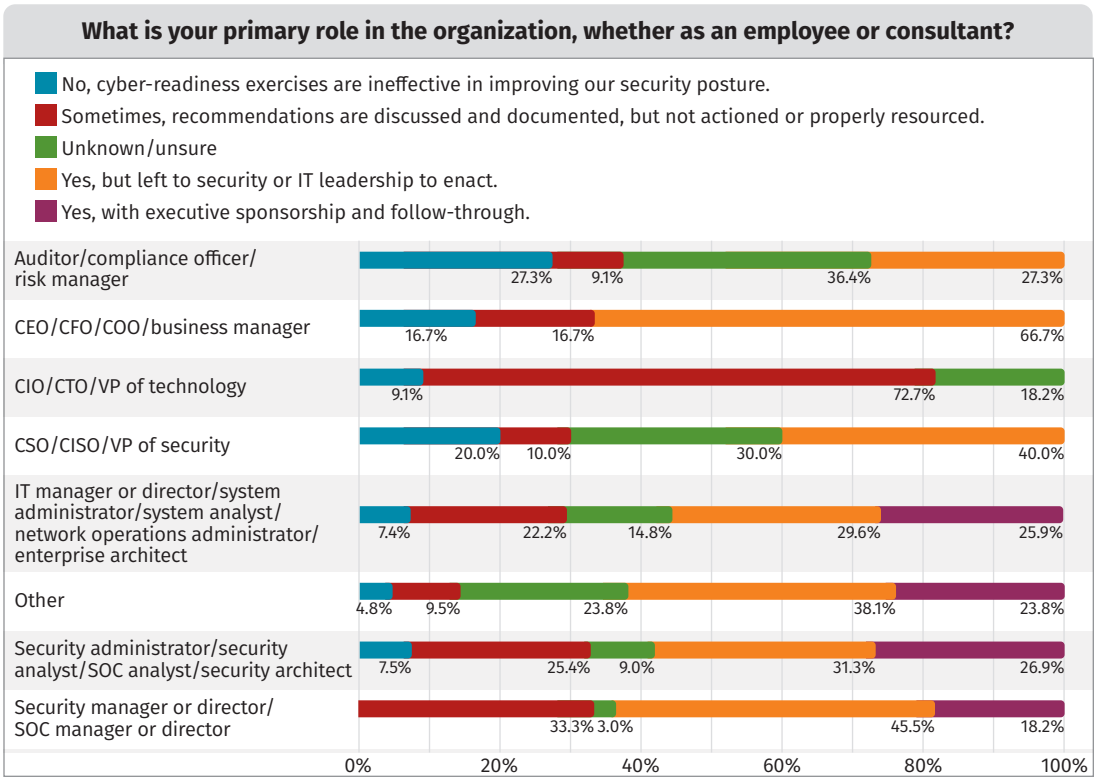

Figure 14. Cyber-readiness Outcomes by Role

Security Measurements

When we asked whether respondents benchmark operational security performance, results are fairly evenly split. Slightly more indicate that they do perform benchmarking (45%) versus those that don't (41%). Respondents citing that their organizations do perform benchmarking employ a variety of tools to get it done, including automated vulnerability scanning (78%), open-source security tool testing (54%), commercial security tool testing (49%), and others (see Figure 15).

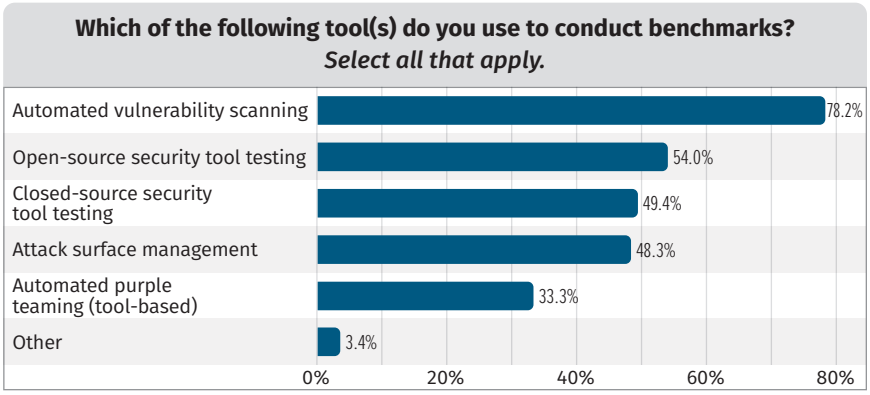

Figure 15. Tools Used for Security Benchmarking

Similarly, most respondents' organizations that perform benchmarking use penetration testing and vulnerability scanning services (33% each), along with managed purple teaming (13%) and other external assessments (16%). This makes sense, because vulnerability assessments and pen tests are relatively mature offerings today and are often required by compliance and regulatory frameworks.

Overall, most respondents state that security metrics and key performance indicators (KPIs) are useful and effective in driving improvements in security processes. Roughly 8% indicate that KPIs and metrics are very effective, with close to 33% noting KPIs are generally effective. Nearly 27% are neutral, perhaps because they're just getting started with metrics and KPIs and haven't had a chance to put them to use; 22% note that KPIs and metrics aren't effective to varying degrees.

Conclusion: Trends and Measuring Security and SecOps

This survey shed some light on the state of security operations governance, framework use, and benchmarking. It's clear that most respondents' organizations are currently leveraging a variety of frameworks to help define their programs and the maturity measurements they put in place, as well as benchmarking their security operations with metrics and KPIs. We still have some work to do—not enough respondents' organizations have executive-level governance and involvement or well-defined training programs, which are both major gaps. As we continue to evolve and mature security operations, it's likely we'll see all these areas improve over time—and with better metrics, we'll be able to track and compare organizations' security operations maturity much more effectively, too.

Sponsor

SANS would like to thank this paper's sponsor:

expel®