Commissioned by

Siemplify

The Road to Security Operations Maturity

A CYENTIA INSTITUTE RESEARCH REPORT

Introduction

> **ONLY THREE THINGS HAPPEN NATURALLY IN ORGANIZATIONS: FRICTION, CONFUSION AND UNDERPERFORMANCE. EVERYTHING ELSE REQUIRES LEADERSHIP.**
>
> **– PETER DRUCKER**

Friction, confusion and underperformance. Managerial mastermind Peter Drucker was almost certainly not referring to modern security operations (SecOps) when he uttered this piece of timeless wisdom, but he sure could've been. Friction among SecOps people, processes and technologies breeds silos of confusion that cripple performance and ultimately lead to losses of one kind or another. Testifying to this, a recent study found that only 5% of SecOps programs operate at recommended target levels of capability and maturity.[1] Numerous other studies have reached similar conclusions.

While there's widespread agreement that many SecOps programs aren't where they need to be performance wise, there's less consensus on exactly where they should be and how best to get there. To help break this stalemate, Siemplify commissioned the Cyentia Institute to examine where organizations are on their journey to SecOps maturity. What are the critical challenges? How are programs of different types and sizes addressing these challenges? Where are they finding success? What does success look like?

We posed these questions and more to over 250 qualified professionals from a variety of roles and responsibilities. Not surprisingly, they had a lot to say, and their responses helped paint a picture of modern-day SecOps programs.

A summary of what we learned from participants is found below, and the pages that follow unpack those lessons in more detail. Our goal is that this research supports SecOps leaders looking to overcome the forces of friction, confusion and underperformance in their organization.

[1]Source: Micro Focus, 2018 State of Security Operations.

GENERAL PURPOSE

The study aims to understand the maturity of security operations and describe the roadblocks and roadmaps on that journey.

TARGET POPULATION

Anyone working in a role that supports the mission of cybersecurity operations.

SAMPLING METHOD

A combination of judgement, convenience, and snowball sampling along with paid "ads" (invitations) to qualified individuals via LinkedIn. See Appendix A.

SAMPLE SIZE

267 qualified respondents of varying roles and tenures from a wide range of organizations.

Overall, our analysis yielded one clear message: SecOps maturity is about robust, repeatable processes that tie teams and technology together to drive success.

Key Findings

Not all SecOps programs are created equal.

– For example, over half of financial firms report having 10 or more SecOps staff, but only 14% in the healthcare sector have that level of resources.

We see signs of change in SecOps team structure.

– Barely over half work in traditional 'tiered' SOCs comprised of different analyst levels. The rest form teams of mixed roles and experience.

The structure of SecOps teams influences strategy.

– Programs with a 'tiered' structure emphasize optimizing technologies. Those organized by 'teams' stress improving people and processes.

SecOps teams are busy and broadly tasked.

– The average staff member handles 3.5 major functions. Counterintuitively, those in larger firms wear more hats than their SMB counterparts.

SecOps functions are not evenly distributed.

– Basics like event monitoring, vulnerability management and incident response have the widest adoption. But specializations like threat hunting are 3X less common in smaller firms.

Functional maturity varies widely.

– The majority of SecOps programs are just starting their maturity journey or midway through it. Only 16% claim to have reached peak maturity.

SecDevOps may boost maturity.

– More mature programs tended to have a higher ratio of staff who could code or script.

Challenges span people, processes and technology.

– The most common challenge was lack of trained staff. Poor correlation and orchestration among processes and technologies was a close second.

Sample Demographics

Who participated in this study?

Using several different sources and methods to reach qualified SecOps professionals for this study, we received a total of 267 usable responses for analysis. We provide summary demographics for the organizations represented by those responses below and a fuller description of sample sources and methods in Appendix A.

Figure 1 shows industries with at least five respondents. A broad range of IT product and service firms sits firmly atop the list, but we see strong representation by a variety of sectors. One deserving special mention is managed security service providers (MSSPs). Such firms handle security operations on behalf of their clients, making them unique in many ways from others in the list.

The distribution of employee counts in Figure 2 is not at all reflective of the real business landscape (which is predominantly SMB), but this actually works to our favor. The focus of this study undoubtedly skews results to organizations large/mature enough to have SecOps teams. And the over-representation among larger firms sets up size-based comparisons later.

Respondents could select multiple regions of operation, accounting for the global sourcing and/or distribution of many SecOps programs. North America clearly sits on top, but it is far from exclusive. Four other regions were identified by at least 20% of participants, and none fell below 10%.

Our sincere thanks to all who shared their perspective with us.

FIGURE 1 SECTORS REPRESENTED

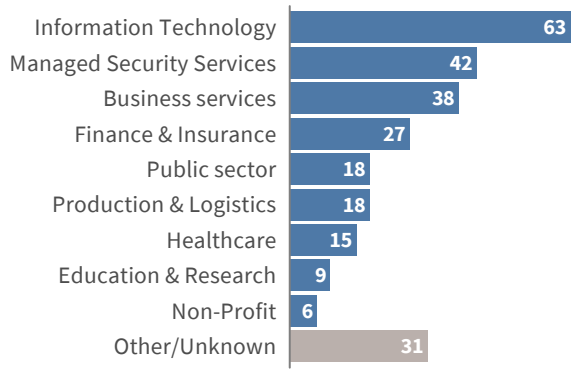


FIGURE 2 NUMBER OF EMPLOYEES

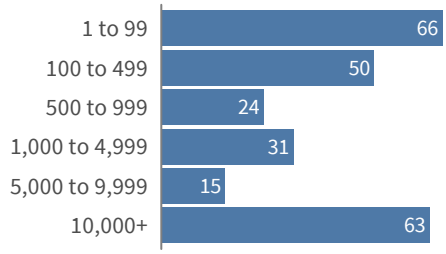
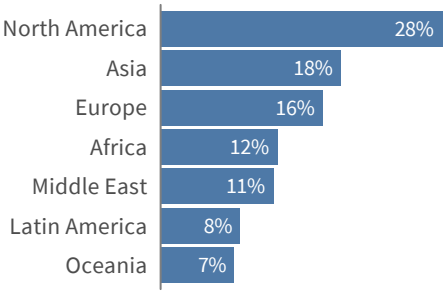


FIGURE 3 REGION(S) OF OPERATION



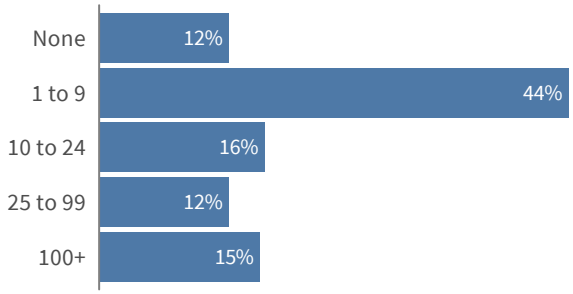
The Size & Shape of SecOps

Now that we know a bit more about the organizations represented in this study, let's take a look at the size and shape of their SecOps programs. This is a hot topic of late, with many questioning the tiered staffing models and rigid escalation processes that are so common.[2] Interest is growing in giving the traditional security operations center (SOC) a much-needed makeover. The drivers for this shift are myriad and include talent shortages, alert fatigue, shift burnout, tool fragmentation, ill-defined processes and more.

SECOPS PROGRAM SIZE

On the surface, Figure 4 doesn't tell us much other than the fact that we have some really small SecOps programs, some really big ones, and everything in between. We suspect, however, that most of you are wondering what's below the surface and thinking "yeah, but…" We're right there with you, so hold on to your "buts" for a moment.

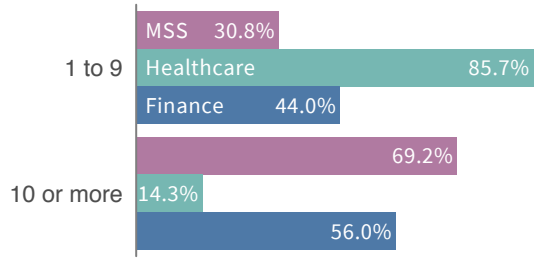
FIGURE 4 NUMBER OF SECOPS STAFF



One of those "buts" may arise from a hunch that certain types of companies—namely MSSPs—would employ more SecOps staff members than the typical enterprise in order to serve their customers. That does indeed check out with our data.

Given that, you may also suspect variation on this data point among industries. We tested that theory by comparing traditionally budget-rich financial firms to traditionally budget-strapped healthcare institutions. We don't have the sample size to assert precision here, but the overall pattern of Figure 5 aligns with our expectations. SecOps staff size maxes out for healthcare well before it does for financial services. Over half of financial firms report 10 or more SecOps employees, while only 14% in the healthcare sector make that claim. It's not shown here, but also noteworthy that no healthcare respondents reported staff sizes over 50, whereas multiple from the finance sector fell in the 100+ category.

FIGURE 5 NUMBER OF SECOPS STAFF



Another "but" might be forming at this point, possibly from intuiting that SecOps staff is a close reflection of the overall size of the organization. Indeed, Figure 6 on the following page suggests the larger the firm, the larger the program. There are, however, some notable exceptions to the rule. A few organizations in the lower right claim to support more than 10,000 employees with fewer than 10 in SecOps. We'd love to hear how that works out for them.

[2]For example, see https://www.darkreading.com/risk/the-soc-gets-a-makeover/d/d-id/1332744

FIGURE 6 SECOPS STAFF BY OVERALL ORGANIZATION SIZE

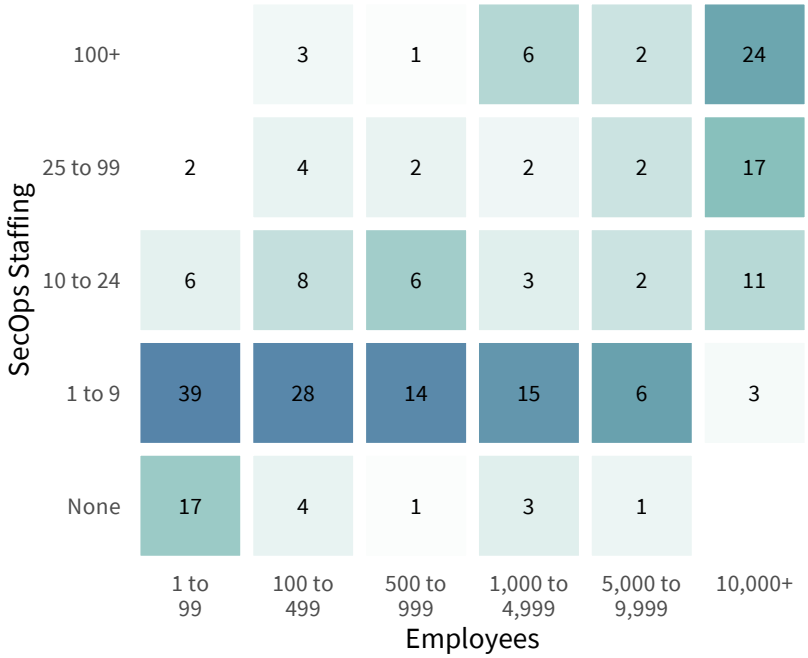


Figure 6 suggests the larger the firm, the larger the SecOps program. There are, however, exceptions to the rule. A few claim to support more than 10,000 employees with fewer than 10 in SecOps!

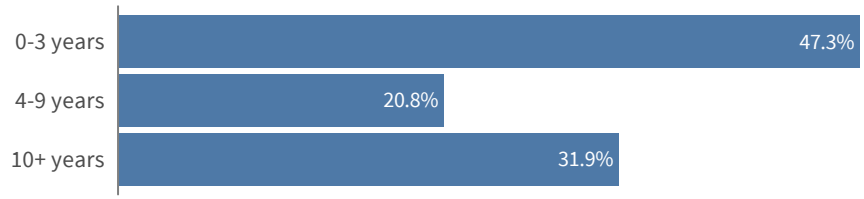
Going a layer deeper than overall size, we asked respondents about how SecOps teams were organized. Over 80% indicated that they were part of a group comprised of differing roles and experience levels. We'll return to these 80 percenters in a moment, but let's first raise a toast to that small, but sturdy cornerstone of the SecOps program: the Lone Hero.[3]

It's pretty much a foregone conclusion that SecOps programs staffed with one or fewer full-time employees are mostly relegated to SMBs. But that doesn't diminish the size of their heroic accomplishments; even the smallest programs are tough to carry when there's only one hero shouldering the weight. We'll examine how much weight that represents a bit later.

SECOPS EXPERIENCE

That last bit is a good reminder that organizations have vastly different resources at their disposal with which to get the SecOps job done. It also insinuates that whatever staffing resources they do have are not on equal footing in terms of experience. To help put some numbers around that, we asked respondents how long they've been in a SecOps role.

FIGURE 7 RESPONDENT EXPERIENCE



Keep in mind that Figure 7 does not supply a breakdown of staff experience within one SecOps program, but rather across many in our survey sample. So it's difficult to apply what we see here to the context of any particular organization. But it does provide some perspective relative to our explorations into the size and shape of SecOps.

[3] "This Bud's for you, Mr. or Ms. Lone SecOps Hero. You carry the entire program on your back with little help and no complaints..."

Across respondents, we find roughly half in the junior category with three years of experience or less. Given the efforts we've seen over the past few years to fill in the cybersecurity talent gap, this could be viewed as a positive sign. Of course, bringing all those new staff members up to speed presents a new set of challenges, as we will discuss later.

The solid contingent of seasoned respondents in Figure 7 is not only good for the SecOps program mission but represents valuable experience that can be passed along to the growing next generation. We find the comparatively low representation from mid-level practitioners rather odd; perhaps they're busy doing actual work while the n00bs and managers fill out surveys.[4]

SOC STRUCTURE

If your mind works like ours, you looked at the three bands of experience in Figure 8 through the subconscious lens of a traditional three-level SOC. Every one of us has either worked in this structure or been worked through it when calling technical support. In this model, junior analysts triage inbound events and escalate those they can't close out quickly to more experienced staff. It's a time-honored staple of IT and security operations.

That's why we were quite surprised to learn from Figure 8 that barely over half of respondents work in a tiered SOC comprised of different levels of analysts. The other (just under) half report being part of an operations team of mixed roles and experience levels. While we are aware of increasing momentum behind adopting this 'teams' approach, we did not expect to see it anywhere near on par with the more traditional 'tiered' SOC model.

FIGURE 8 SOC STRUCTURE ACROSS ALL FIRMS

One theory is that Figure 8 shows the strong influence DevOps has had on SecOps of late. If small teams with at least one individual responsible for security are less likely to produce insecure products, perhaps teams with mixed roles can be more effective in the SOC as well. We will pull on this thread later, but it's worth mentioning briefly here that respondents within the 'teams' model seemed to emphasize improving people and processes, while those in the classic 'tiers' model talked more about optimizing and managing tools.

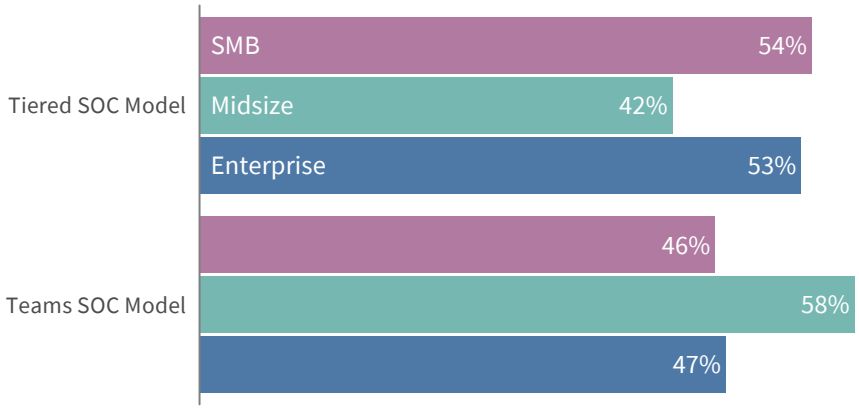
Overall though, respondents from both schools of thought reported having mature, successful programs. Are we seeing the big reveal of a widespread "SOC makeover," or just more options for structuring the emerging broader-than-the-SOC notion of SecOps? Could it be that both models have their place, depending upon the goals and characteristics of the organization?

> **"WHILE WE ARE AWARE OF INCREASING MOMENTUM BEHIND ADOPTING THIS 'TEAMS' APPROACH, WE DID NOT EXPECT TO SEE IT ANYWHERE NEAR ON PAR WITH THE MORE TRADITIONAL 'TIERED' SOC MODEL...OVERALL, THOUGH, RESPONDENTS FROM BOTH SCHOOLS OF THOUGHT REPORTED HAVING MATURE, SUCCESSFUL PROGRAMS.**

[4] Kidding! You know we appreciate what you do and that you took the time to share your thoughts with us.

In search of clues for this question, we first wanted to know if the choice of SOC structure is influenced by the size of the organization. That does not appear to be the case and, in fact, the evidence points to the contrary. Figure 9 shows virtually no difference between SMBs and enterprises in terms of the ratio of tiers versus teams. Both show a moderate preference for a tiered SOC. Midsize firms, however, break the pattern by preferring the teams model.

FIGURE 9 SOC STRUCTURE BY ORGANIZATION SIZE



Once again, we find these results counterintuitive. We suspect that MSSPs may be an underlying factor here. Many SMBs outsource SOC functions to MSSPs (and thus inherit their structure) and many larger enterprises model their SOCs after MSSPs due to similar delivery pressures (even if all the customers are internal departments). Figure 10 offers some supporting evidence for this hypothesis.

FIGURE 10 SOC STRUCTURE: MSSP VS IN-HOUSE PROGRAMS

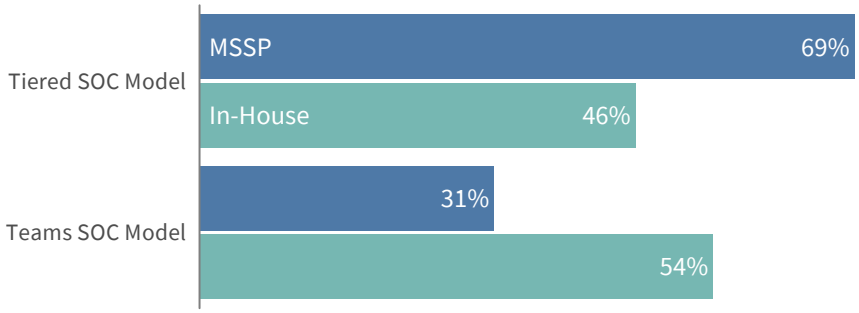


Figure 10 shows tiered SOCs are indeed over twice as common among MSSPs than their team-based counterparts. This structure is undoubtedly born of a need to handle a high volume of alerts with high efficiency on behalf of multiple customers. In-house SOCs, on the other hand, have more freedom to optimize size and shape according to internal functions. What are those functions, and how do SecOps programs mature capabilities to meet them? Keep on reading.

SecOps Roles & Functions

Armed with a better understanding of the structure of SecOps programs today, we're now ready to investigate what those programs actually do. In this section, we focus on 12 roles or functions that commonly fall under the bailiwick of SecOps. Respondents were asked to select three functions[5] that best represent their primary responsibilities. Table 1 provides a listing of these functions and how they were described in the survey.

TABLE 1 DESCRIPTION OF SECOPS FUNCTIONS INCLUDED IN THIS STUDY

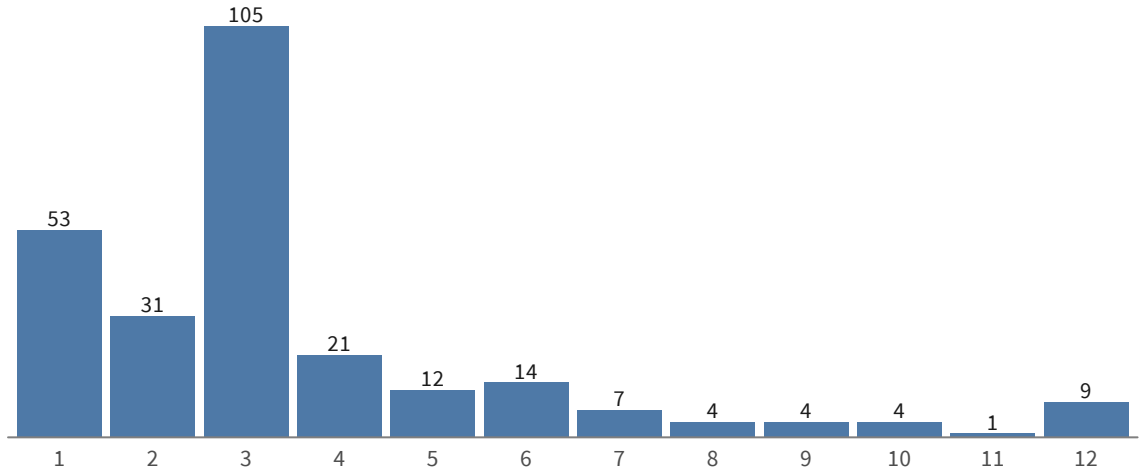
FUNCTION	DESCRIPTION	LABEL
SecOps director	Responsible for overseeing or directing all security operations for the organization. Those selecting this function did not choose additional functions but had some unique questions.	Director
Team management	Leadership of one or more SecOps teams/functions, including setting objectives, organizing resources, directing activities, measuring performance, etc. Those selecting this function were also asked to select the function(s) they managed.	Manager
Vulnerability management	Identifying, assessing, prioritizing, and remediating hardware and software vulnerabilities.	Vuln Mgt
Penetration testing or red teaming	Reconnaissance and attack scenarios conducted from the adversary's perspective to assess and stress test security posture and response.	Pen Test
Security event monitoring and triage	Monitoring ticket and event queues, triaging and classifying events, closing out tickets, escalating potential incidents, etc.	Monitoring
Network intrusion analysis	In-depth analysis of potential intrusions, information and artifact fusion, recommendations for further action, etc.	Intrusion
Incident response or digital forensics	Responding to confirmed incidents to determine scope, contain exposure, collect evidence, investigate root cause, facilitate recovery, etc.	Response
Malware or vulnerability analysis	Examining or reversing the properties, behaviors and capabilities of malicious code and vulnerabilities.	Malware
Threat intelligence and research	Collecting and analyzing the motivations, intent, capabilities, TTPs, indicators and activities of threat actors.	Intelligence
Advanced threat hunting	Proactively searching across networks and systems to identify signs of advanced, subtle and/or evasive threats.	Hunting
Engineering, system admin, or development	Designing, developing, deploying, tuning, administering, and maintaining systems, sensors, tools and content in support of security operations.	Engineering
Project or product management	Initiating, planning, executing and tracking projects and products relevant to security operations.	Project Mgt

[5]They were not prevented from selecting more than three, however, and some did just that.

You may get the impression that some functions in Table 1 fall at or even outside the edges of what many consider SecOps. This is by design so that we could study not only core SecOps responsibilities like event monitoring and incident response, but a range of SOC support roles as well. Plus, we wanted to set ourselves up to detect if, for instance, breakdowns were occurring within or between the core and support roles.

Before we get into which functions respondents perform, let's first get a sense of how many they selected. Figure 11 outs 76 respondents (~30%) for not following the survey instructions by choosing more than three functions. That's actually ok and reinforces our decision not to enforce that rule. From Figure 11, we can easily see that quite a few SecOps professionals wear numerous hats.

FIGURE 11 NUMBER OF FUNCTIONS PER RESPONDENT



Of the 50+ respondents who chose only one function, most were SecOps directors or other management roles. At the other end of the spectrum, nine respondents selected every function. Those poor souls. On average, respondents report handling roughly 3.5 functions each; slightly more than we asked them to select. We looked at that number by organization size and found something interesting: Respondents in larger enterprises actually wear more hats than their SMB counterparts (average of 3.9 vs. 3.5 for SMBs). That seems backward at first blush, but remember that those larger firms also have bigger programs. "To whom much is given, much is required," as the saying goes.

Oh, and remember the lone SecOps heroes from the previous section? They tackle an average of 5.5 functions. Give them a raise!

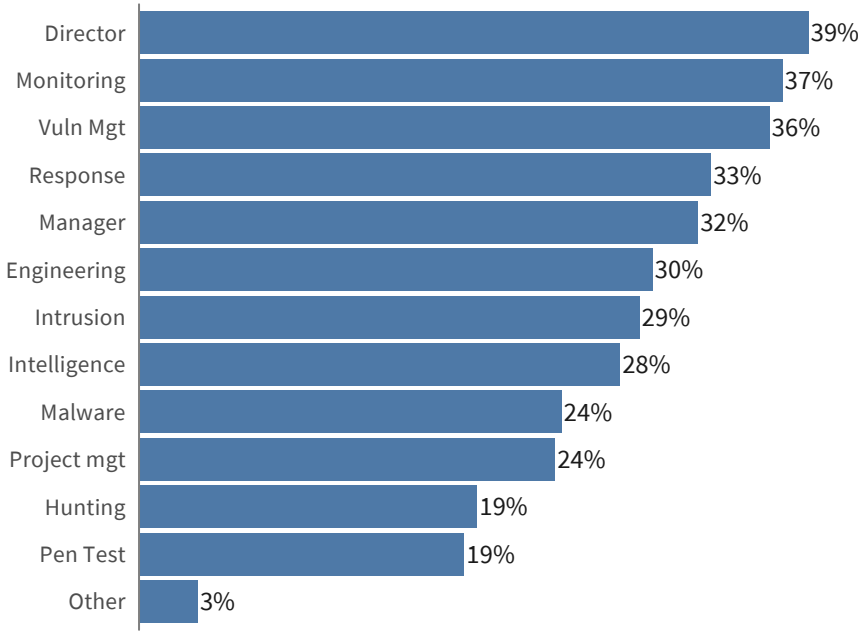
TOP SECOPS FUNCTIONS

Let's press on to what respondents told us about the specific functions they perform. Figure 12 tallies these from most to least common. Our first impression is that the results reflect a well-rounded list with no major imbalances. Sure, some functions are more common than others, but we don't see any that drown out everything else. It conveys the diversity inherent to SecOps.

It is also a good sign that respondents didn't feel the need to make heavy use of the "Other" option. We received only a few of those, including security audit, sales engineering, and policy and procedure development. This suggests our list of functions is fairly comprehensive in terms of the scope of responsibilities delivered by SecOps programs.

As we have cautioned with prior charts, Figure 12 does not give a breakdown of functions within a particular SecOps program. We would need large numbers of respondents from the same organizations to create that view, and we suspect it would be significantly more lopsided for roles like event monitoring. What we should have here, however, is a reasonable proxy of these roles across the SecOps profession. Let's explore why some of these functions fell where they did in Figure 12 and whether they line up with what we'd expect.

FIGURE 12 PRIMARY SECOPS FUNCTIONS PERFORMED BY RESPONDENTS



Charts in this section all sum to well over 100% because the calculation is based on the % of respondents, who could choose multiple functions.

Setting aside the director role, the top three functions fall in line with expectations. These, or some version of them, form the core "Prevent, Detect, Respond" pillars that undergird SecOps. These roles also align strongly with the prevailing tools and training available to aspiring (or practicing) cybersecurity professionals. It's where many cut their teeth before either broadening their skills or narrowing in on a specialty.

This is probably a good way to view the functions in the lower half of Figure 12. They are what SecOps programs and professionals expand into or focus on once they move beyond the basics. It's not the exact order of these that matters, but rather what they collectively represent—an organization that has the luxury of preparing for future fires rather than just fighting the current ones.

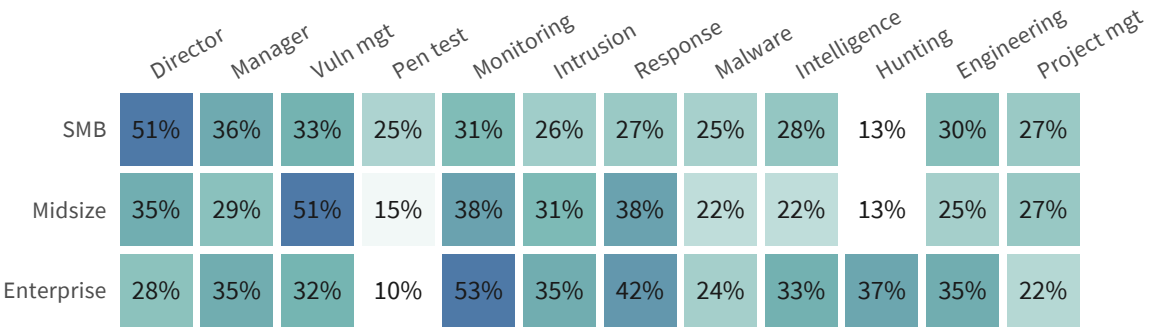
Threat intelligence, malware/vulnerability analysis, and threat hunting do indeed have that "future fires" outlook. At least that's the intent. And even though penetration tests are often part of a basic compliance checklist nowadays, the requisite skills don't come cheap. In fact, the mid-career salaries commanded by all of these roles rank among the highest in the cybersecurity field. Luxury taxes.

We think it fitting that engineering/development and intrusion analysis land in the middle of the core and advanced functional groupings in Figure 12. These can be seen as transitional roles for SecOps programs ready to kick it into higher gear. That transition will typically require deeper investigation of complex events (intrusion analysis) and finely tuned tools and processes to support those capabilities (engineering/development).

DIFFERENCES BY ORGANIZATION SIZE

We discovered earlier in this section that SecOps professionals in larger firms perform (slightly) more functions on average than those in SMBs. But do their mix of responsibilities differ as well? That's the question we have in mind here, and Figure 13 will help us answer it.

FIGURE 13 SECOPS FUNCTIONS BY ORGANIZATION SIZE



Smaller firms appear to rely heavily on SecOps directors and managers, who almost certainly juggle many of the critical functions for the program as best they can. Any opportunity to outsource, automate or otherwise simplify the other functions listed is likely music to their ears. Moving beyond these "leader-doers" (they lead, but they also do), smaller shops appear most likely to add staff for vulnerability management and event monitoring.

This general trend continues in midsize organizations, but vulnerability management, event monitoring and incident response begin to play a much bigger role. It's almost like you can see the SecOps hierarchy of needs taking shape in organizations of this size. You can also sense issues starting to form among these expanding tools and teams.

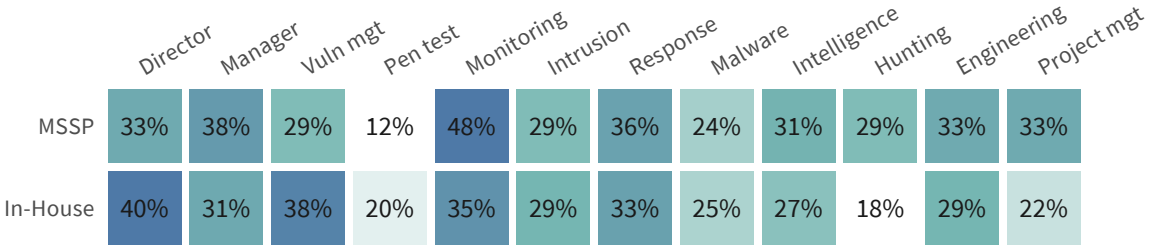
By the time we get to larger firms, we see the effects of the expanded resources and skills needed to defend more complex environments. This is evidenced by a high concentration of staff to monitor and respond to the constant barrage of threats. Backing up that first line of defense, the supporting and specialized functions are also well attended. None exemplify that more than threat hunting. It's the least common function among small and midsize firms, yet 3X higher in large enterprises.

MSSPS VERSUS IN-HOUSE PROGRAMS

Some readers may be skeptical about the results shown in Figure 13 because MSSPs are in the mix. It's conceivable that a smaller MSSP may have abnormally high numbers of specialty roles compared to traditional enterprises. That kind of expertise is, after all, why many smaller and midsize firms turn to MSSPs. Figure 14 should ease any holdover skepticism by making it abundantly plain what the data says on this topic.

> "IT'S ALMOST LIKE YOU CAN SEE THE SECOPS HIERARCHY OF NEEDS TAKING SHAPE IN MIDSIZE ORGANIZATIONS. BY THE TIME WE GET TO LARGER FIRMS, WE SEE THE EFFECTS OF THE EXPANDED RESOURCES AND SKILLS NEEDED TO DEFEND MORE COMPLEX ENVIRONMENTS.

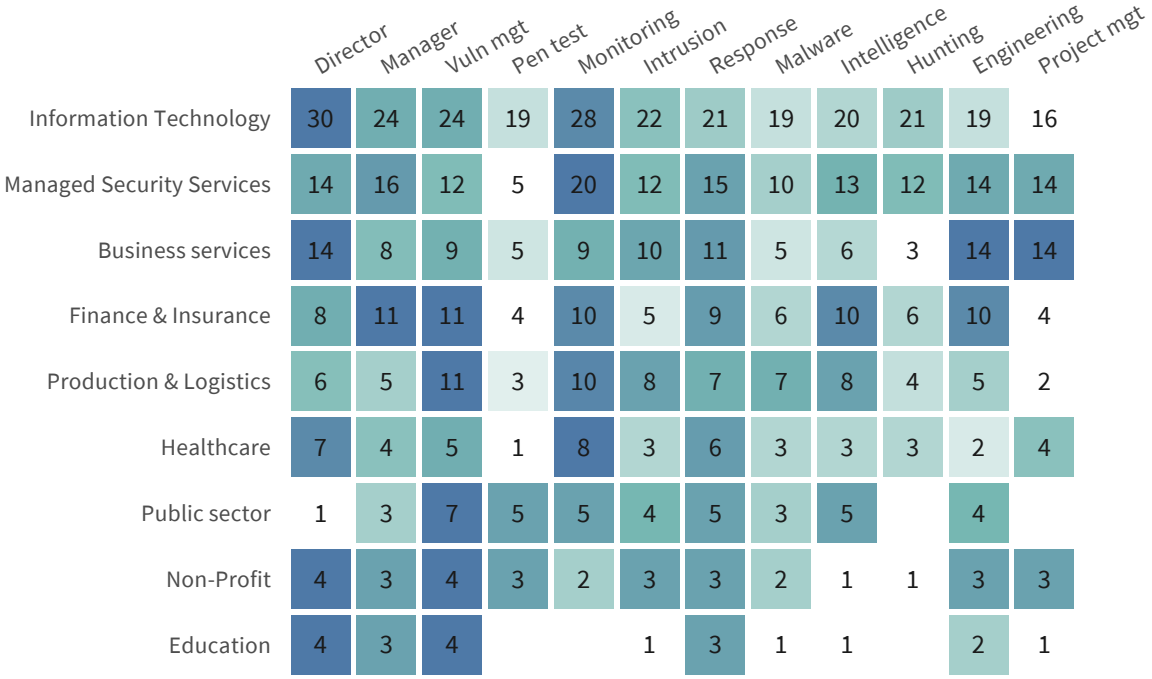
FIGURE 14 SECOPS FUNCTIONS FOR MSSPS AND IN-HOUSE PROGRAMS



Findings for the classic SOC role, event monitoring, will probably surprise very few: MSSPs staff a lot of those. Some specialty functions such as threat hunting rate substantially higher among MSSPs, but others like malware/vulnerability analysis show little difference. MSSPs appear to have more need for PM roles, whereas enterprises are more likely to own the vulnerability management function. But overall, we find the distinction less dramatic than anticipated.

Those looking for a more detailed comparison among industries are invited to peruse Figure 15 at your leisure. Expanded commentary seems like overkill, especially since we suspect many will glean a few insights on their specific industry and ignore the rest. And there's nothing wrong with that approach; that's why we included it. Take as long as you like, and we'll rejoin you on the flip side.

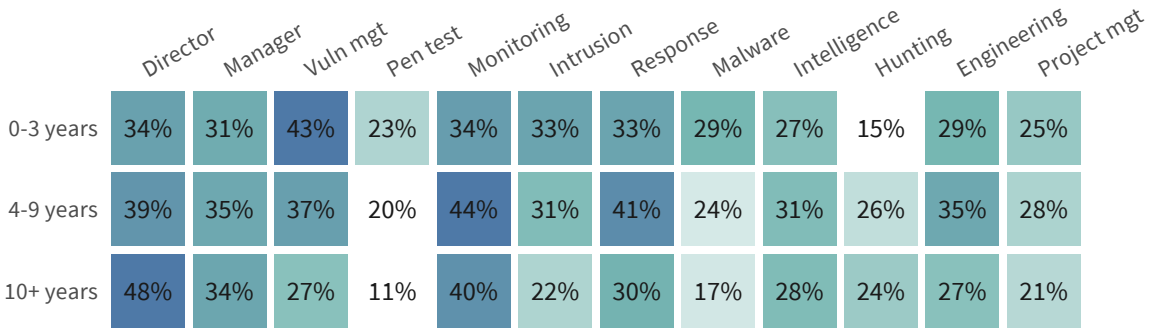
FIGURE 15 SECOPS FUNCTIONS BY SECTOR



DIFFERENCES BY EXPERIENCE LEVEL

One final aspect of SecOps functions we wanted to examine relates to experience. It makes sense that entry-level practitioners would have different roles and responsibilities than their more seasoned peers. Figure 16 provides what we need to make this comparison.

FIGURE 16 SECOPS FUNCTIONS BY EXPERIENCE LEVEL



We see the SecOps director is the No. 1 role among those with 10 or more years of experience. No surprise there; it's fitting for these veterans to take the reins of their own program. What is surprising is that the proportion of less-experienced directors is as high as it is. A quick peek under the covers reveals these to be those "leader-doer" roles we mentioned earlier who are prevalent in smaller organizations. While we're on the topic of leader-doers, we should call out the relatively equal proportion of team managers across experience levels. The classic persona here are those who want some management experience for career momentum, but still like to get their hands dirty.

Looking over the technical functions in Figure 16 prompts both "duh" and "huh?" reactions. Among the "duhs," vulnerability management tends to be an early career role, and threat hunting requires more experience. In the "huh?" category, penetration testing and malware/vulnerability analysis are purportedly n00b skills. We've **heard rumors that the pen test is dead**, but could it be that pen testers are actually dying off? In all seriousness, we're at a loss to explain several of these findings. So we will simply point out the dangers of reading big things into small differences and admit we don't have all the answers.

Assessing SecOps Maturity

In addition to asking respondents about their primary functions, we asked them to rate the maturity of those functions within their organization. This was done for each function selected according to the maturity scale defined in Table 2.

TABLE 2 DESCRIPTION OF MATURITY LEVELS USED IN THIS STUDY

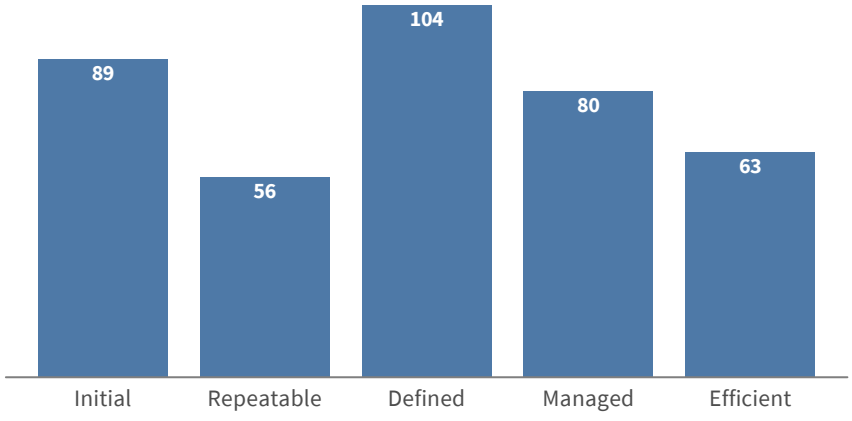
LEVEL	LABEL	DESCRIPTION
1	Initial	Chaotic, ad-hoc, reactive and reliant upon individual heroics
2	Repeatable	Loosely defined such that some institutional memory and consistency exist
3	Defined	Well understood, documented and standardized processes
4	Managed	Processes have been defined, stress tested, measured, refined and adapted
5	Efficient	Optimized through rigorous diagnostics and a focus on continual improvement

Notice from this maturity model that functions really don't get…well, functional until the fourth and fifth levels. In the early stages, things will only get done if forced, and the way they get done will vary each time. The middle level acts as a sort of 'hump' that aspiring SecOps programs must get over before becoming truly functional. Where do the organizations in our study fall along these maturity levels? Let's find out.

PROGRAM-LEVEL MATURITY

Starting off, we'll look at the big picture of maturity across the SecOps program. We're using an ordinal scale, so the rules of math won't allow the calculation of an "average maturity rating" within or across organizations. We can, though, tally the total number of functions rated at each level and summarize it with a chart like Figure 17.

FIGURE 17 COMBINED MATURITY RATINGS FOR ALL FUNCTIONS



The majority of SecOps programs are just starting their maturity journey or midway through. Only 20% claim to have reached peak maturity.

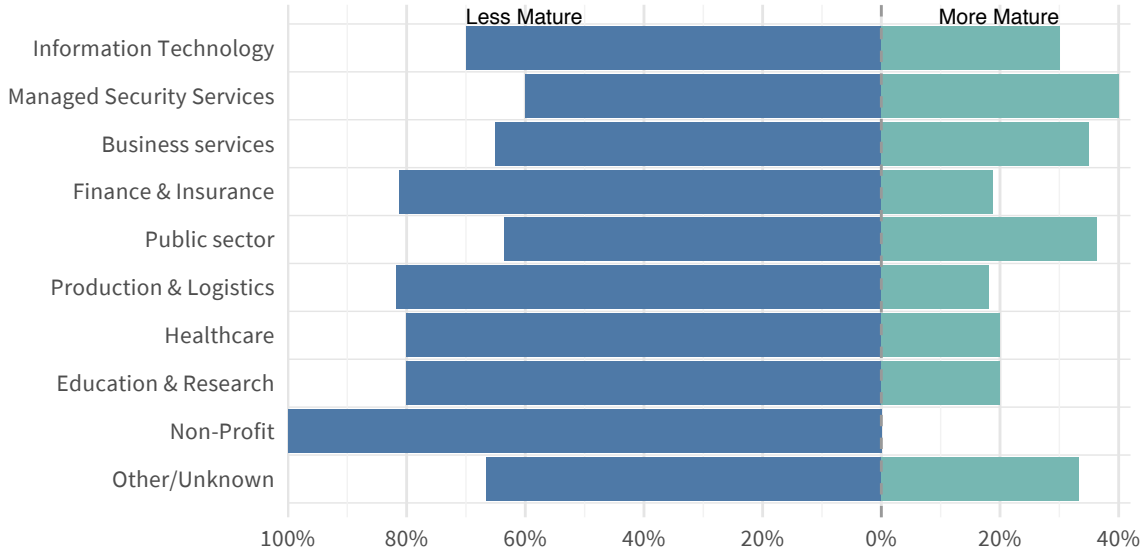
The first thing we notice is that the 'hump' mentioned a few paragraphs back does seem to be a thing. Many programs seem stuck in that maturity purgatory called 'Defined.' It's difficult to know what they did to earn this fate. What we do know is that the level of effort to get over the maturity hump is almost certainly much greater than what was required to get to the hump in the first place.

Moving left of the hump, we see that a large number of SecOps functions seem to never have gotten out of the Initial or Repeatable states. For many, this is the natural fallout of being in continual fire-fighting mode. Some simply keep backsliding into bad habits. Others lack the necessary skills or resources to push the program onward and upward.

To the right of the hump, we see that respondents assigning high maturity ratings to a surprisingly high number of functions. We can't help but **hear Inigo Montoya saying** "You keep using that word 'Efficient;' I do not think it means what you think it means." Indeed, we suspect the high bar inherent to these upper echelons of maturity wasn't conveyed well by our definitions. That said, only 16% claim to have reached the highest maturity level. The reality is that progressive movements along this maturity scale are more exponential than linear. Having 'Defined' processes is an important stepping stone, but it's a lot more than two steps away from a truly 'Efficient' SecOps program.

To study the relative maturity of SecOps programs by sector and size, we categorized all organizations in our sample as "less mature" and "more mature" based on the functional maturity ratings supplied by respondents. We have some sample size challenges for many combinations, but Figure 18 shows this comparison for the top sectors.

FIGURE 18 SECOPS MATURITY RATING BY SECTOR

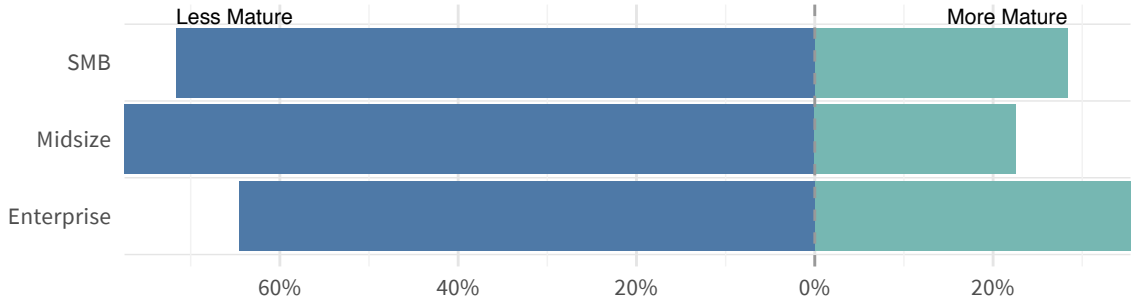


MSSPs occupy the top maturity slot, but they really have no excuse not to be No.1. They specialize in handling SecOps functions on behalf of their customers—it's what they do. We were rather shocked to see the public sector in second place for overall maturity. These respondents didn't divulge many details, so we're left to assume that this group represents various three-letter agencies that know a thing or two about operational maturity rather than local municipalities.

In an interesting twist, the bottom of the chart features the traditionally regulated verticals of finance and healthcare. It's absolutely plausible that a bank's definition of 'mature' doesn't match an advertising firm's and that some verticals have to work much harder for the same baseline. That said, we're curious if the increased burden of compliance detracts from the pursuit of maturity.

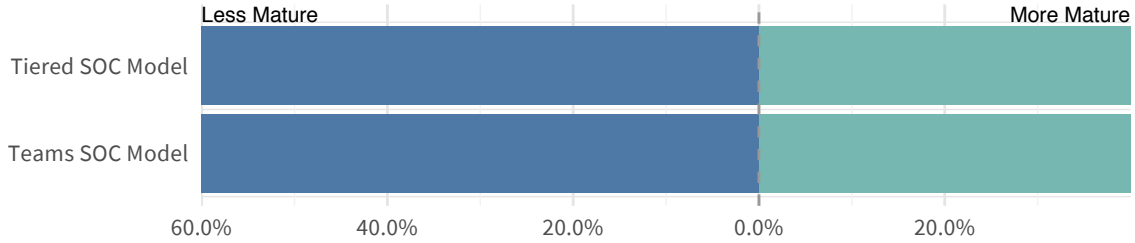
When it comes to maturity differences by organization size, clear conclusions are difficult to draw. Per Figure 19, larger organizations do indeed rate as somewhat more mature. But size does not appear to perfectly correlate with maturity, because midsize firms exhibit less maturity than SMBs. This may again stem from the usage of MSSPs among SMBs.

FIGURE 19 SECOPS MATURITY RATING BY ORGANIZATION SIZE



Earlier in this report, we examined the structure of SecOps programs according to "tiers" and "teams." We hoped to determine which one of these models led to greater maturity, but the data had other plans. We see no differences or advantages for one or the other models. Choosing teams of mixed levels and roles or constructing a tiered system seems to be largely based on various organizational characteristics and circumstances.

FIGURE 20 SECOPS MATURITY RATING BY SOC STRUCTURE



We asked respondents in a SecOps director role if there was someone dedicated to driving the maturity of the program. The majority said yes (part of their own role, presumably). The question on our minds was whether having someone with that responsibility actually helped. Our findings suggest programs classified as "more mature" were 3X more likely to have someone responsible for getting them there. Even if this result reflects some confirmation bias, explicitly tasking someone with driving maturity is a cheap experiment that won't hurt your chances of success.

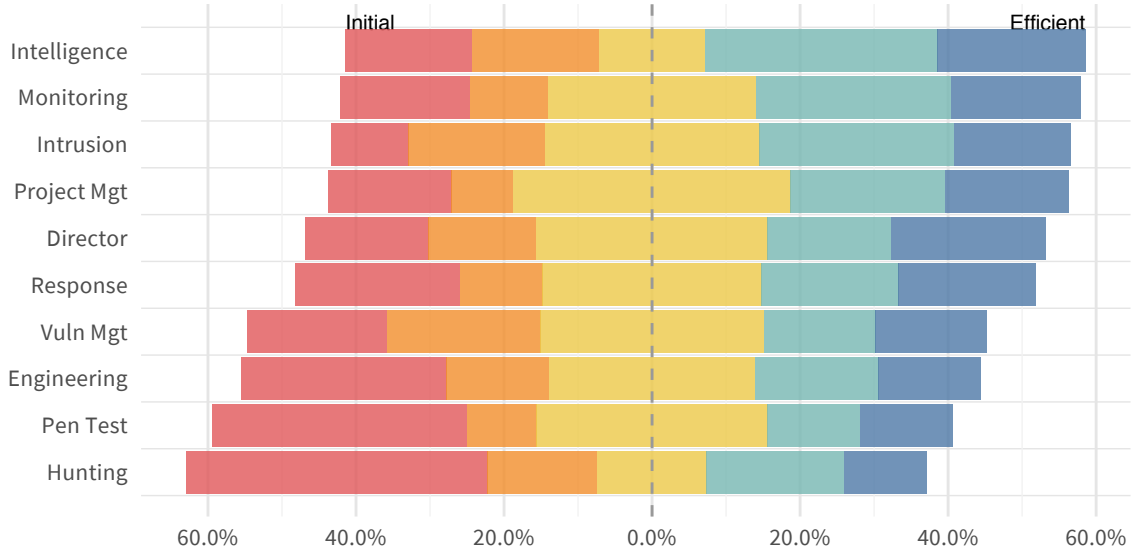
FUNCTION-LEVEL MATURITY

Having established a view of maturity across the program, we now compare maturity ratings among the 12 SecOps functions in this study. Figure 21 shows responses for all five levels of maturity across each function. The scale ranges from Initial (red) to Efficient (blue).

Overall, we find the variation in maturity among the functions less than expected. The least mature function (threat hunting) shows only a ~20% difference from the most mature function (threat intel). And speaking of threat intel—since when did that become the poster child for maturity? We can't help but wonder if respondents interpreted the rating of "Managed" as "a tool automatically integrates and manages intel for us." As evidence in favor of this, multiple respondents mentioned automation and third-party products in comments regarding threat intelligence.

Of the more core functions, event monitoring and intrusion analysis land toward the top with distributions leaning toward the mature end of the scale. Malware analysis is rather interesting with a disproportionate amount of ratings at each extreme. A possible explanation is the nature of malware analysis products—if you implement one, you almost immediately warp a maturity level or two.

FIGURE 21 FUNCTION-LEVEL MATURITY RATINGS



The SecOps director function is right in the middle of the stack and balanced maturity-wise. As the closest indicator of overall program maturity, this is as it should be.

Given the importance of incident response to a SecOps program, it's worrying to see it fall below the fold. When looking for clues, we saw free-form responses that helped lend some perspective. One respondent said: "We need to document plans and test them. It's mostly based on memory and staff discretion right now." Another remarked: "We need better processes, procedures and trained personnel."

Vulnerability management represents table stakes for a security program, yet it ranks fairly low on the maturity stack here. Vulnerability scanners return more data than ever these days and therein may lie the problem. It's not unusual for a midsized organization to see tens of thousands of vulnerabilities vying for their attention and action. Vulnerability fatigue is probably as common as alert fatigue among SOC analysts, but we don't talk about it as much anymore.

At the bottom of the stack, we see penetration testing and threat hunting. Generally, we'd expect only the largest and most mature organizations to have an internal penetration testing or red team function, so this result wasn't surprising. The reason for threat hunting bottoming out the graph is more nuanced, however.

As a relatively new SecOps function, threat hunting is still working its way up the maturity stack as a discipline, with purpose-built tools and products in active development. Furthermore, by its very nature, threat hunting depends on data from many of the other functions. Even if threat intelligence and event monitoring are "mature" within silos, they're of little help to threat hunting if not correlated. One respondent put it this way: "It takes way too long to figure out certain things… Speed and agility are hard without quality, enriched logs." That sentiment was not unique. For threat hunting to improve and mature, other functions must correlate their data with some degree of automation.

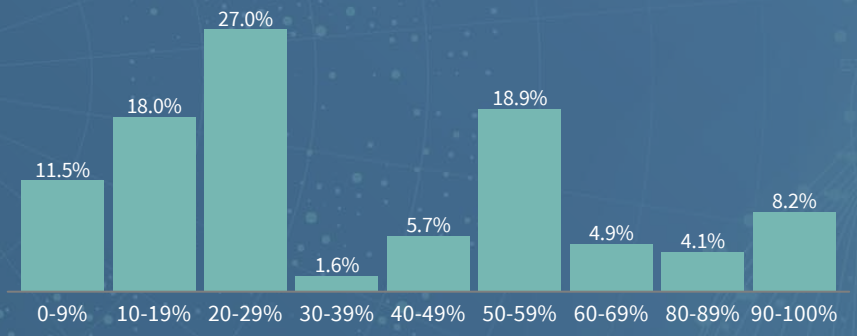
Coding to Maturity?

If you've been in tech for a while, you may have seen a sticker or T-shirt that reads "Go away or I will replace you with a very small shell script." Even though it's meant to be grumpy nerd humor, there's an element of truth behind the words. It's unlikely that code will replace you anytime soon, but it could replace a lot of your repetitive tasks that sap so much time and energy.

In SecOps, the ability to code or script can mean the difference between being overwhelmed and comfortably making progress. No budget for the tool you need? Just code up a basic facsimile yourself. Even getting readily available open-source software working correctly or integrated into existing tools may require at least basic scripting. Because of this, we thought it would be interesting to ask respondents what proportion of their colleagues can code or script.

On average, a little over one in three (36%) of SecOps staff can code. The median is 30%, and the distribution around those centralities is shown in Figure 22. The average remains fairly constant when comparing MSSPs vs. In-House programs and even across different levels of experience. The one demographic that seems to have a higher ratio of coders is SMBs. We can't help but wonder if this is a necessary adaptation in order to maximize value from constrained resources.

FIGURE 22 PROPORTION OF SECOPS STAFF WHO CAN CODE OR SCRIPT



In lower-maturity programs, 25% of staff possess coding or scripting skills. That statistic rises to 40% for higher-maturity programs.

That's all well and good, but what we really wanted to know was whether having more coders on staff drives SecOps program maturity. The data hints at a possible correlation here. In lower maturity programs, 25% of staff possess coding or scripting skills. That statistic rises to 40% for higher-maturity programs. Admittedly, there's a sort of "chicken or the egg" issue here. Which comes first—the coders or the maturity? Perhaps it doesn't matter.

While having coders on staff isn't absolutely necessary, experience tells us they're definitely nice to have. A SecOps team who can build in addition to buy has more options on the table and more control of their destiny. And that's never a bad thing.

The Road to Maturity

So far, you may have noticed a consistent undertone throughout this report. Our primary focus is to understand where SecOps programs are on the path to maturity, as well as the challenges and successes along that journey. What separates those who get lost along the way from those who reach their goals? Is it having top-notch people? Well-defined policies and procedures? Acquiring the best technologies? Is it a mix of all these things?

The final portion of the survey asked a series of four open-ended questions designed to discover insights related to the journey toward maturity. We chose this format because structured or multi-choice questions run the risk of swaying and/or limiting responses. We wanted to know what was on their mind in their own words.

SECOPS CHALLENGES

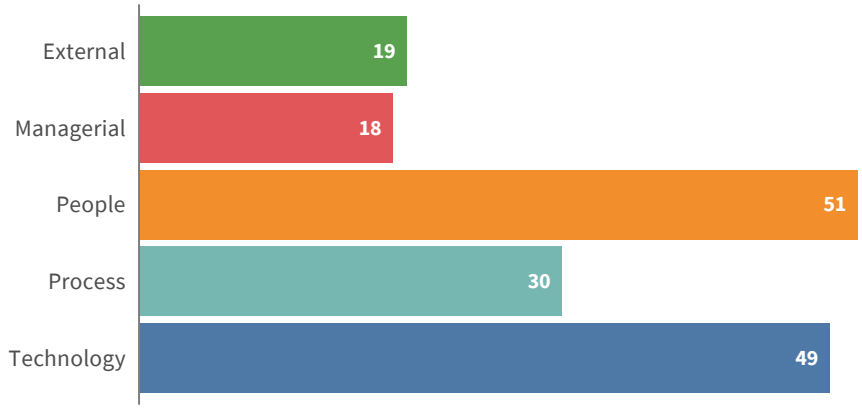
The first question we posed to respondents in this section regarded the most pressing current challenges to their SecOps program. As you may imagine, they had a lot to say. In going through comments, we quickly hit some challenges of our own in trying to count, compare and communicate what we learned from these responses in a meaningful way. Thankfully, a small number of common categories began to take shape as we reviewed input. Table 3 describes these categories.

TABLE 3 DESCRIPTION OF CATEGORIES APPLIED TO RESPONDENT COMMENTS

CATEGORY	DESCRIPTION
External	Anything outside the organization and its influence. Threats and regulations were two common examples of things mentioned in this category.
Managerial	Covers a range of organizational issues spanning governance, culture, policy, strategy, executive support, etc.
People	Pertains to human resources and their knowledge, skills and abilities.
Process	Pertains to processes, procedures, playbooks, etc.
Technology	Pertains to various types of hardware, software and data.

The fact that these common categories emerged from the comments shouldn't be too surprising. Even though each respondent faces unique challenges and circumstances, the basic factors that must be overcome are the same. Figure 23 shows that those challenges fall strongly along the lines of people and technology.

FIGURE 23 CATEGORIZED COMMENTS DESCRIBING PRIMARY CHALLENGES



The unstructured comments in this section make it hard to present results consistently. We came up with these categories to help. Refer to Table 3 for descriptions.

When people were the problem, the most prevalent complaint was a lack of SecOps staff. Close behind that was insufficient training for existing staff. Poor alignment of priorities was also a common complaint, especially concerning other IT or security teams and sometimes the business as a whole. Staff retention was mentioned, but more common was the challenge of getting good personnel in the first place.

Comments related to technology indicated a consensus on six basic and relatively balanced issues that are categorized in Figure 24. These span from acquiring the needed tools to implementing and configuring them properly to integrating everything to work together. Once all of that is done (it never is), respondents hit roadblocks in effectively correlating all the information coming at them from these technologies. Unsurprisingly, many of these comments tied back to SIEMs. These challenges seem to recall Drucker's words that opened this report: friction, confusion, and underperformance.

FIGURE 24 CATEGORIZED COMMENTS DESCRIBING **TECHNOLOGY** CHALLENGES

Figures 24 and 26 split comments in the Technology category into sub-categories to give a sense for what tech challenges and initiatives are about.

Given these challenges, it's not surprising that a lack of security orchestration and automation among people, processes, and technologies was a common refrain. When these things don't work together, inefficient manual tasks become the duct tape of the SecOps program. If you're an IT or security professional, you've lived this nightmare before. IP addresses are copied and pasted into emails. Security data is exported to CSV and massaged in spreadsheets in a desperate effort to correlate data and extract meaning. Customer specifications are **walked downstairs to the software engineers** who don't have the people skills to do it themselves. There must be a better way. Let's see how respondents are overcoming these challenges.

WIN-LOSS RECORD

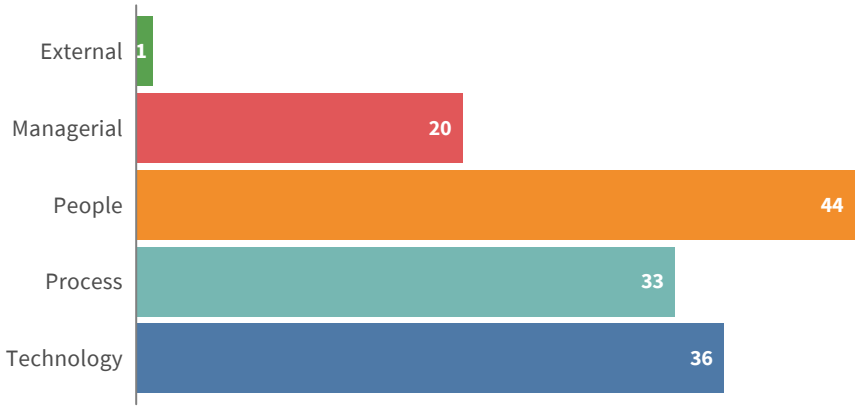
SecOps is a battle. You win some, you lose some and hope to learn something from both. When asked about the progress of their maturity journey, respondents seemed to accentuate the positive. Noticing this, we wanted to tally a quick win-loss record across programs in our sample. If respondents mentioned a positive accomplishment, we marked it as a win. Negative experiences and abject failures were put in the loss column.

Overall, we were glad to see three wins to every loss. We interpret that as a good sign. SecOps programs appear to be learning more than losing. Comments mentioning processes and technologies came away with the most wins and highest ratio of positive-to-negative sentiment. We examine the key initiatives driving these victories in the next section.

CURRENT INITIATIVES

Next, we asked respondents which initiatives were planned or already underway to meet these challenges. Responses here were interesting and ranged from lengthy, detailed roadmaps to the equivalent of a shrug. We again separated comments into the same categories used in the prior 'Challenges' section.

FIGURE 25 CATEGORIZED COMMENTS DESCRIBING CURRENT INITIATIVES

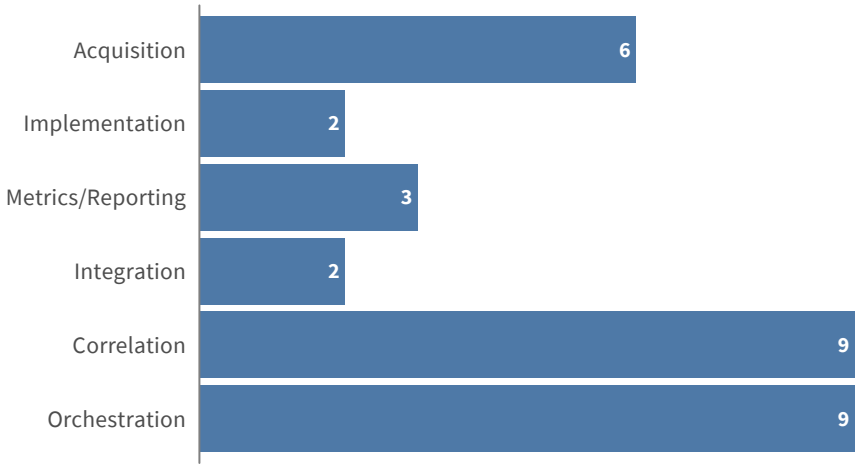


See Table 3 for descriptions of these categories.

The people, process, and technology categories took the lead again, but more balanced than we saw for challenges. There seems to be a stronger focus on process improvements, which form the building blocks of maturity programs. People and technology are again the leading categories, perhaps because there's a realization that technology challenges don't solve themselves. Good tools require good people to use them and good processes to guide them. Also bolstering the people category were numerous mentions of training and education initiatives.

The external category all but disappears among planned initiatives. Over a dozen respondents identified external challenges, but only one mentioned doing something to address them. This seems natural, as external factors are, by definition, outside of the organization's control.

FIGURE 26 CATEGORIZED COMMENTS DESCRIBING **TECHNOLOGY** INITIATIVES



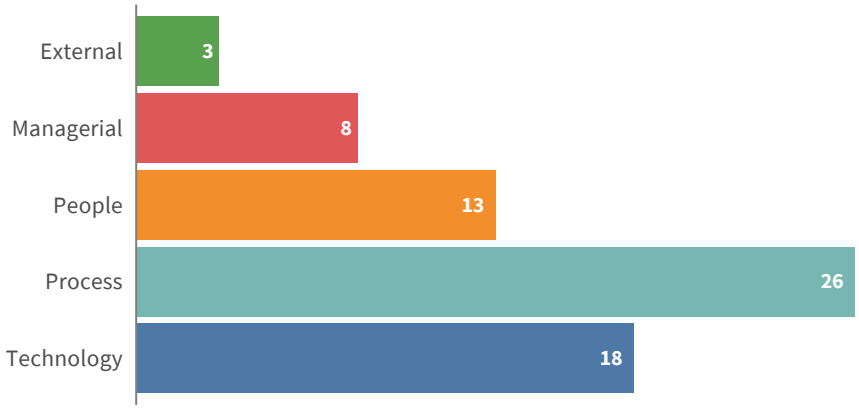
Beyond these broad categories, the most common themes among the initiatives described by respondents concerned correlation and orchestration. On the correlation side, respondents mentioned efforts to expand data sources, tune SIEM rules and enrich dashboards with contextual information. Comments pertaining to orchestration included the deployment of security orchestration, automation and response (SOAR) products, along with homegrown solutions to automate tasks and workflows.

MEASURES OF SUCCESS

Our final open-ended question asked participants to describe what maturity means for their organization and how they'll know when they achieve it. For the first time, the process category jumps out in front of the others in Figure 27.

Many responses simply pointed to the goal of streamlining existing functions. Quite a few others mentioned speed and responsiveness as key success metrics for their operations. It's clear that respondents want to see tangible results, and those results often come down to doing things demonstrably better and faster.

FIGURE 27 CATEGORIZED COMMENTS DESCRIBING 'WHAT SUCCESS LOOKS LIKE'



Overall, our analysis of these responses yielded one clear message: SecOps maturity is about robust, documented, repeatable processes that tie technology, teams and their respective functions together to drive success.

> **"OVERALL, OUR ANALYSIS OF THESE RESPONSES YIELDED ONE CLEAR MESSAGE: SECOPS MATURITY IS ABOUT ROBUST, DOCUMENTED, REPEATABLE PROCESSES THAT TIE TECHNOLOGY, TEAMS AND THEIR RESPECTIVE FUNCTIONS TOGETHER TO DRIVE SUCCESS.**

Conclusion & Recommendations

Thanks for traveling with us on this journey toward SecOps maturity. We hope the findings in this report provided helpful insight into the many challenges faced along that journey and spawned some ideas on how to navigate around them. To that end, we'd like to leave you with some practical recommendations based on our analysis of input from respondents.

Speaking of respondents, we would also like to express our sincere appreciation to all those who participated in this study. Time is a precious commodity in SecOps and in life, so thank you for investing it with us. Having read this report, we hope you view that as time well spent to benefit the community.

1. **SecOps resources are scarce.** Allocating them optimally requires fully understanding the goals and risks involved in each area of the business. Starting there will enable you to better identify and prioritize SecOps use case requirements.

2. **Every journey needs good maps.** For SecOps programs, an accurate and current inventory of key people, processes, tools and assets provides this map. You'll surely get lost along the road without them.

3. **Balance structure and strategy.** We learned that the structure of SecOps programs differs among organizations, and this factor alone doesn't dictate capability maturity. Choose a structure that fits your strategy and tailor it to suit.

4. **Collaboration is king.** Yes, we know 'context is king' too, but the universal stress respondents placed on the interwoven challenges of people, process and technology demands more emphasis on ongoing collaboration at all levels of the organization.

5. **Empower your people.** Everyone has trouble finding and retaining SecOps staff, but the skills gap involves more than just headcount. Use orchestration and automation to free up analyst time and energy for higher-order functions that actually move the needle.

6. **Play by the book.** Use playbooks, organized by relevant use cases, to guide and streamline monitoring and response processes. Test them to work out the kinks so you're ready when it's time to play for real.

7. **Expect to fail.** Your SIEM technology won't identify every threat and SecOps programs must account for this. Avoid the "alert or it didn't happen" fallacy by investing in proactive functions for detecting and analyzing threats.

8. **SOAR to new heights.** Consider whether a SOAR solution should be part of your journey to SecOps maturity. These solutions take alerts from SIEM or similar technologies via APIs and enrich them with a variety of data sources. Predefined playbooks then take automated or semi-automated actions to respond to alerts and prep them for analyst investigation. SOAR solutions are not intended to replace analysts or existing detection technologies. Instead, they act as a virtual analyst with the intent to improve capabilities and overall efficiency.

Appendix A

Survey Methodology

Based on the goals specified in the introduction, we sought to collect a reasonably representative sample of respondents from a variety of security operations management, staff and supporting roles. We say "reasonably" because obtaining a random and perfectly representative sample from our target population is simply not realistic without extraordinary effort and cost. Not only are we seeking input from a rather niche domain (cybersecurity), but SecOps programs are particularly sensitive entities. Several would-be respondents expressed interest in the study but said organizational policy restricted them from participating.

1. To improve representativeness, we employed several independent sampling methods and sources:
2. We partnered with Cybrary to invite users from its member base who had the relevant qualifications. Cybrary also contributed an incentive for participation in this study: All respondents were eligible to win a **Cybrary Insider Pro** membership free for one month (three winners were randomly chosen later).
3. We created paid LinkedIn ads that invited users whose current roles and posted skills were relevant to SecOps.
4. We invited those who participated in our previous studies who said they were willing to be contacted for future studies.
5. The sponsoring organization for this study, Siemplify, shared the invitation with its list of customers, prospects and interested parties.
6. We posted a few open calls for participation on LinkedIn and Twitter.

All of these sources had a unique link, allowing us to compare the number of respondents across sources. Cybrary and LinkedIn generated the majority of the 309 total responses for this study. We disqualified 42 of those for various reasons. This left us with a sample of 267 usable responses that form the basis of our analysis and findings.

ACKNOWLEDGEMENTS

The Cyentia Institute would like to recognize and thank Adrian Sanabria for working with us on this project. Your industry insight was invaluable in helping us shape this study and interpret findings.

Several others provided guidance and feedback during the course of this project. You know who you are and we hope you know we appreciate your contributions.

Finally, we'd like to once again offer our gratitude to all those who participated in this study. We literally couldn't have done it without you.

Siemplify, the leading independent security orchestration, automation and response (SOAR) provider, is redefining security operations for enterprises and MSSPs worldwide. The Siemplify platform is an intuitive workbench that enables security teams to manage their operations from end to end, respond to cyberthreats with speed and precision, and get smarter with every analyst interaction.

www.siemplify.co

The Cyentia Institute produces rigorous, accessible research content that provides value to our partners' core audiences and the security community at large.

www.cyentia.com