SANS

Analyst Program

Survey

Threat Hunting: Focusing on the Hunters and How Best to Support Them

Written by **Mathias Fuchs** and **Josh Lemon**

April 2023

ANOMALI

Executive Summary

This is SANS's eighth year of conducting our Threat Hunting Survey, where we go out to organizations around the globe to understand how they have conducted threat hunting over the last year and try to gain some insight into what they may do in the coming year. Much of the work we put into this report involves taking raw statistics from our respondents and translating them into patterns and trends forming in the industry over the last year.

In addition to many of the common questions we asked threat hunters this year, we have added several new questions to dig deeper into how organizations perform threat hunting. We also have included more detailed questions about the daily activities of threat hunters within their organizations, along with probing the support that threat hunters get from leadership. We also take a small dive into understanding how ransomware and extortion threat actors influence our threat hunters' hunt missions.

With these new groups of questions, we try to understand further details regarding what a threat hunter's typical day looks like, whether they are required to do other tasks at the same time as hunting, and how much time they may be able to allocate to perform hunt missions within their organization.

From our own experiences, we have found that the level of engagement from leadership can significantly influence how successful threat hunting can be for an organization. With the additional questions we asked this year, we discovered that leadership teams, and even the C-suite, are becoming more involved with methodology and more aware of hunt missions. We have also collected information on areas where threat hunters need support from their leadership teams.

This year, we discovered that a third of respondents believe they have a mature or greater threat hunting capability within their organization. We also tried to use free-form answers to uncover further why organizations believe they are mature when it comes to threat hunting. This process uncovered some interesting trends relating to the reliance on tools for threat hunting.

We again shine a significant spotlight on tooling used by our fellow threat hunters and how that tooling influences methodology, training, and strategy. We discovered a trend in which tooling is starting to influence an organization's approach to threat hunting, instead of a threat hunting strategy influencing tool selection.

We have also spent a significant amount of time understanding how organizations utilize resources to conduct threat hunting, and have found an increasing trend of organizations performing threat hunting with their internal staff. Although a quarter of respondents are still using external organizations, we uncovered their level of satisfaction with this process. We're also starting to see an increasing trend of threat hunters crying out for more training, education, and support from management.

Lastly, we've collected information on the effectiveness of threat hunting to understand where organizations see improvements as a direct result of threat hunting. The results show that threat hunting is essential for an organization to defend itself against threat actors. We look at this in further detail throughout the report—meanwhile, here are some of the other findings:

- 24% of respondents claimed that threat hunting is their full-time job.
- 43% of threat hunting missions last for one to two days.
- 69% of organizations experienced ransomware attacks that influence their methodology.
- The use of AI and machine learning for hunting has decreased by 5%.
- 49% of organizations adapt their hunt missions based on the tools they already have.
- 73% of organizations define a methodology, but only 38% follow it.
- 63% of organizations use internal staff for hunt missions.
- 34% of organizations are formally measuring threat hunting efforts.
- 81% of organizations measuring their threat hunting saw an increase in their overall security posture.
- 73% of organizations need additional training or more skilled staff.
- 78% of senior leaders are either aware of or engaged in threat hunting.

Figure 1 provides a snapshot of the demographics for the respondents to the 2023 survey.

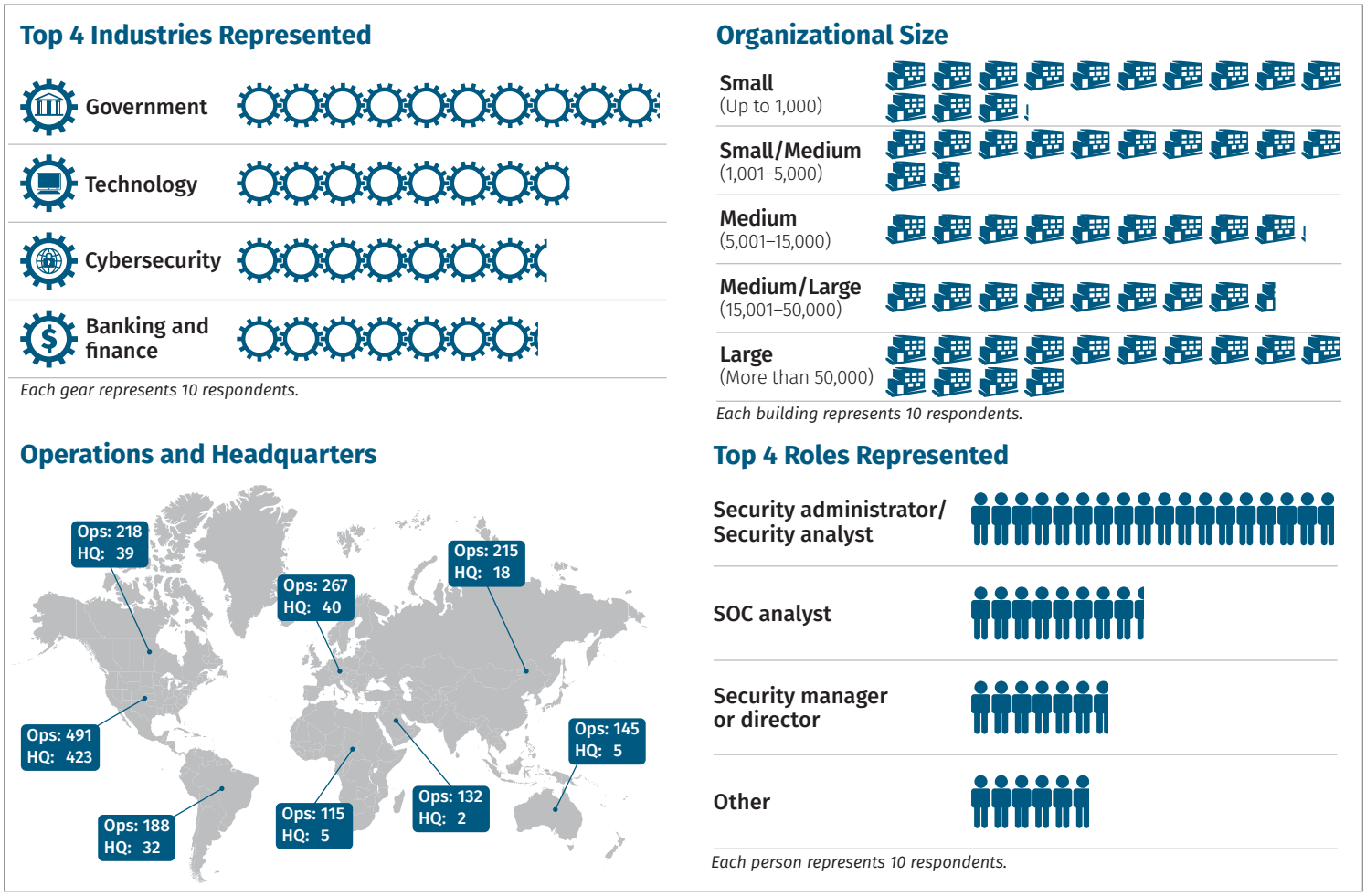

Figure 1. Demographics of Survey Respondents

Participants

We were particularly interested in how respondents characterize their organization's level of threat hunting maturity. Almost a third felt that their organizations are mature or very mature, whereas 40% are still in the process of maturing. We included an open-ended query that allowed respondents to provide details about their perceived maturity. From these responses, five clusters emerged.

Cluster 1: We have so many great tools.

One argument for a high-maturity level that we got quite a few times was that an organization is mature because it has so many great tools in place. A decent tool stack helps hunting, yet it is only a part in the whole picture that successful and mature threat hunting presents. As in most past surveys, we again want to stress the point that a fool with a tool is still a fool.

Threat hunting is very much about using the knowledge of your defenders inside an organization to catch threat actors that are not detectable through automated means.

Cluster 2: We ingest specific threat intel and work with it.

We got that answer quite a lot, and it is incredibly positive to see it. This is how high-maturity threat hunting is supposed to work. The threat hunter defines risk levels for various attack risks in an organization, acquires intelligence that describes the risks in a technical form, and produces a hunting hypothesis.

Cluster 3: We measure threat hunting.

Improvement always entails measurements. How would you know if you got from A to B if you have no ability to identify either A or B? Several respondents said that they are mature because they kept measuring threat hunting and it improved. That sounds like an exceptionally good approach and is also suitable for procuring budgets for threat hunting.

Cluster 4: We are developing but lacking resources.

Another frequent response was that organizations are still building up their threat hunting practice but lack resources to do so quickly. Some of the respondents whose answers fell into this cluster also stated that their newly forming teams are augmented by external entities like managed security service providers (MSSPs).

Cluster 5: We have a manual or ad-hoc approach.

Another cluster was made up of respondents who claimed that their hunting approach is very manual and ad-hoc. That is also reflected in later questions where we can see that there are barely any full-time threat hunters. Although this approach might render particularly satisfactory results depending on the team conducting manual hunts, there is no guarantee for success, nor is there a guarantee for repeatability.

Threat Hunting Maturity

Threat hunting maturity is heavily influenced by how well you select what you are hunting for. In low-maturity states, threat hunters throw many indicators of compromise (IOCs) from various sources at the network. This is like a shotgun approach. Although you might find traces of an attack, it is hard to see them among the vast number of false positives you will also receive. The logical solution is to better select which IOCs you want to hunt for in your network. The next maturity level of threat hunting entails taking a closer look at the IOCs at hand and picking the ones that are most likely to hit gold while at the same time not using the ones that produce many false-positive results. The highest stage is hypothesis-based hunting. In this approach you start without having any IOCs lined up for the hunt. The threat hunters build a hypothesis about who could attack their network. Based on that hypothesis, they find or create the appropriate IOCs based on the tactics, techniques, and procedures (TTPs) the attack group usually uses. All IOCs should be checked for their likelihood of producing false-positive results. Besides the ability to find attackers in the network, this approach also invariably leads to the development of long-term detection rules for the security operations center (SOC).

Although threat hunting is slowly being commoditized, as the clusters listed above show, there is still a great deal of inhomogeneity among the organizations who conduct threat hunting. In comparison, SOC operations are much more streamlined than threat hunting is. It is likely that over the next few years we will see more consolidation of the different approaches. This will also be driven by the product vendors who strongly invest in threat hunting capabilities.

Participants' Routines

Let us investigate the daily routine of today's threat hunters. Only 24% claimed that threat hunting is their full-time job; the remaining 76% have other obligations in addition to threat hunting.

Only 22% responded that they hardly ever get assigned additional tasks when on a threat hunt. In comparison, 28% claim that they mostly or always get additional assignments when conducting threat hunts. Although in general it might be beneficial for threat hunters to have a broader view of the organization's security, concurrent tasking might distract from a swift and streamlined threat hunt execution. See Figure 2.

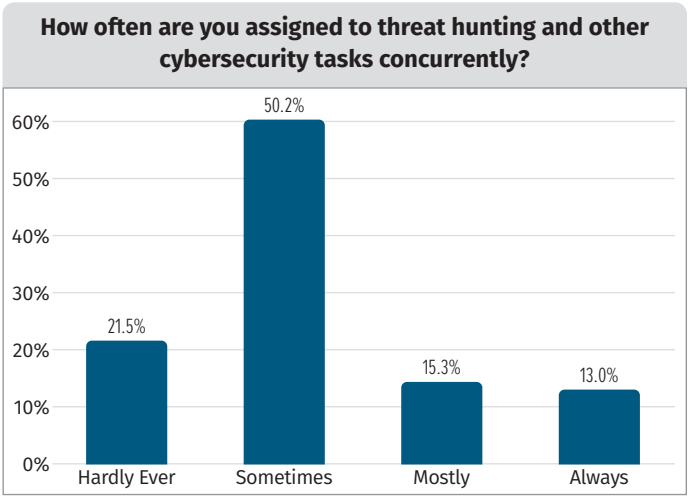

Figure 2. Threat Hunting Involvement

Continuing on the topic of distraction, we wanted to know how much time our respondents spend on a typical threat hunting mission. This is also an indicator of how they conduct threat hunting. If, for instance, a hunting mission lasts for 12 months on the same data, it will hardly be hypothesis-based hunting. The hypothesis might need to be reviewed a few times and new hunting methodologies set up.

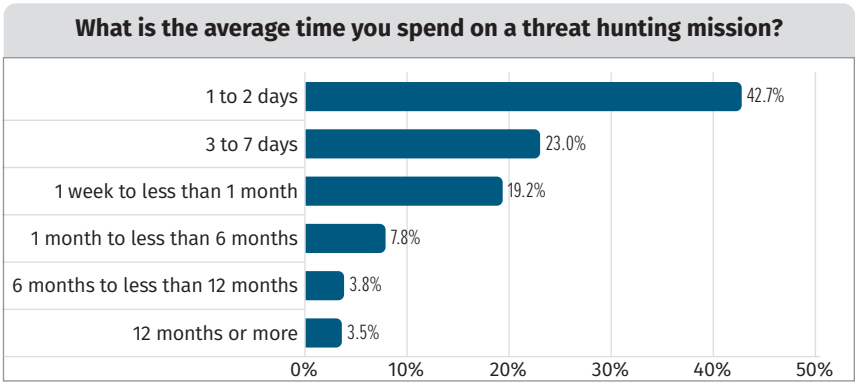

Figure 3. Average Time Spent on Threat Hunting

For many of our respondents (43%), a typical hunting mission lasts for one to two days. Only 15% of the respondents said a hunting mission takes longer than a month. For future surveys, it might be interesting to take a closer look into the relationship between hunting techniques and hunting mission duration as well as potential outcomes. See Figure 3.

Another interesting point is how much extortion-based cybersecurity incidents influence what organizations are hunting for. Most respondents (69%) claim that ransomware attacks have influenced their hunting decisions. We believe that to be quite logical because ransomware is a risk to most organizations—particularly higher than most other risks. This clearly means it must be considered in threat hunting.

Hunting with Tools, or Tooling to Hunt

High-quality threat hunting is usually a combination of good tools (software tools and intelligence), skilled people, and sound processes that govern the hunt. In a nutshell, we can leverage the PPT framework (people, processes, and technology) to look at various aspects of threat hunting.

As in past years, we wanted to investigate all three angles. We already discussed parts of the people angle in the previous section. In this section, we will investigate hunters' tool chests. We are particularly interested in which class of tools our respondents use and how satisfied they are with them.

Over the last year, a large majority of hunters used tools like SIEMs, endpoint detection and response (EDR), and other automated alerting systems. Most of the solutions on the market support quite a few hunting functions. This year, the percentage of respondents who are using tools in that category increased again from 83% to 89%.

To us, it is also interesting to understand how often custom-made and homegrown tools are used in threat hunting. Our assumption is that the more vendors cover in their commercial tools, the less need there is for tailored solutions within a hunting organization. The use of "configurable, customizable, internally developed search tools" went from 62% last year to 67% this year. So, the growth is remarkably similar to the increased use of SIEM and EDR solutions. Although homegrown tools can be greatly beneficial and powerful, they are not free. Very often, these tools are maintained by a small group of people or even a single developer. This reduces development costs, but increases the resources needed to manage the application. That includes, but is not limited to, developing strategies for how to keep the tool, even when the lead developers leave the organization. See Figures 4 and 5.

What tools/technologies do you currently use? Which of these tools/ technologies did you implement in the past 24 months?
Select all that apply.

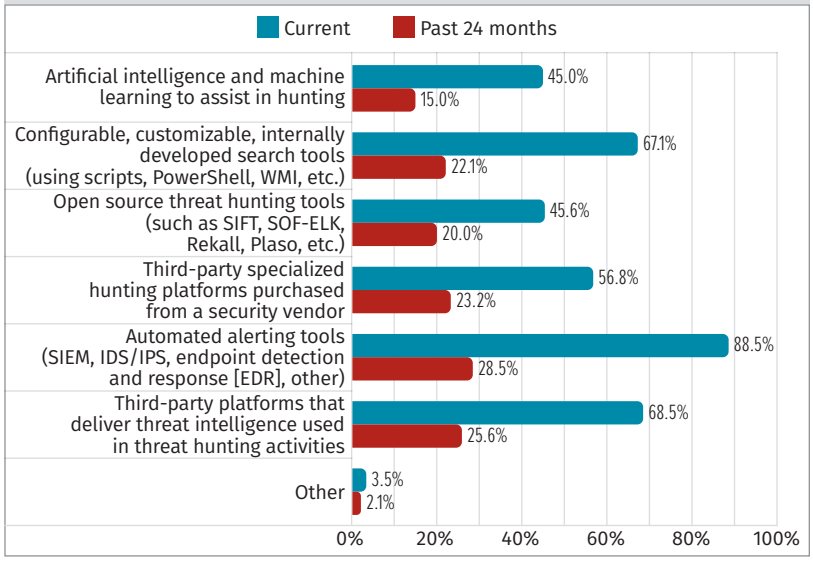

Figure 4. Tools/Technologies in Use (Current)

What tools/technologies do you currently use? Which of these tools/ technologies did you implement in the past 24 months?
Select all that apply.

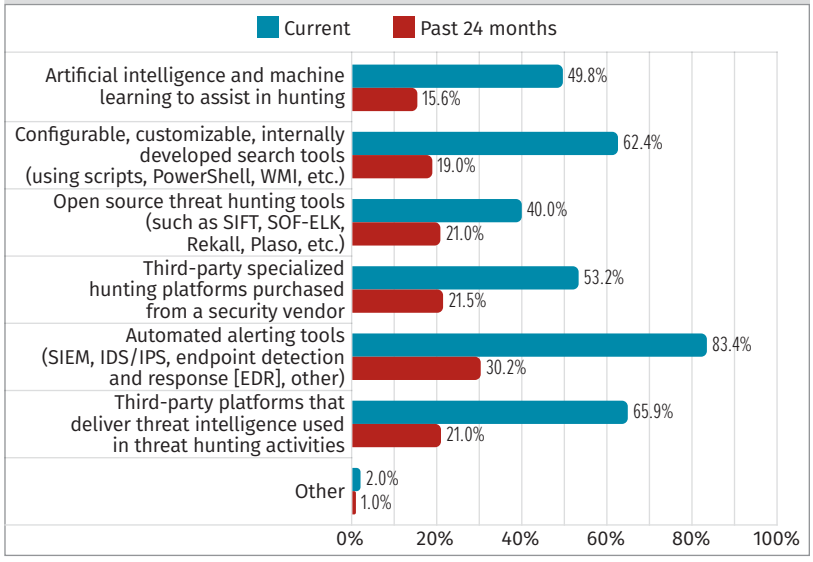

Figure 5. Tools/Technologies in Use (Last Year)

Hunting consists of multiple stages. The stage where you use tools like SIEMs or EDRs is usually preceded by intelligence work that results in a hunting hypothesis. Over 68% of our respondents use tools to deliver and manage intelligence. That is a slight increase of 2% compared to last year.

The only category that went down was "artificial intelligence and machine learning to assist hunting." Last year, that category of tools was used by 50% of respondents, but this year it lost some traction and came in with 45%.

If we look into satisfaction levels with the existing solutions to identify a "winning team" of tool categories, similar to the past few years, the combination to use would be tools in the SIEM/EDR category together with "third-party platforms that deliver threat intelligence." The SIEM/EDR category showed 82% of the respondents being satisfied or very satisfied, and third-party platforms made 62% of our respondents happy. As in previous years, satisfaction with third-party tools is matched by homegrown tools, which also leave 62% of our respondents satisfied.

Obviously, these numbers always must be taken with a grain of salt. Although the frequently used tool categories get a lot of responses, the less-used tool categories do not receive so many ratings. That might slightly skew the results.

Visibility Implications

This year, we want to investigate the influence tools have on hunting strategies. In an ideal world, the definition of what a hunter wants to hunt for comes first, and the tools are selected based on the needs dictated by the strategy. In the real world, however, companies already had tool stacks in place long before they started investing in threat hunting. These tools are often expensive and will not be replaced easily.

Additionally, less experienced hunters might benefit from being guided on what to hunt for by a tool. One big downside of this tool-centric approach is that it leaves predictable visibility gaps, either horizontal or vertical. Horizontal visibility gaps mean that one is not always covering all the networks or endpoints. Vertical visibility gaps indicate the known blind spots of tools. Since the Conti Ransomware chats surfaced in 2022, we know that attack groups try to purchase security tools to test them for gaps. These visibility gaps can and will be exploited by the attacker. We also see this in the wild.

Whereas only a few years ago most ransomware actors would not be able to get around even a halfway decently configured EDR, they now are starting to adopt and seem to be sharing strategies to evade automatic detection by EDR solutions. These evasion strategies might impact your hunting success. So, even if you use off-the-shelf platforms like commercial EDRs, make sure to not only focus on the contents provided by the vendor, but also leverage customization features to implement your own approach. That will significantly reduce the hiding space for an attacker.

Let's look into the numbers of how threat hunting strategies and tool choices influence each other. Unsurprisingly, 49% of our respondents claimed that they adapt their hunting approach to the already acquired tools. See Figure 6. Thirty-two percent define their strategy first and select the tools based on requirements dictated by the strategy. The rest of our respondents do not have visibility into how their tools and strategy play together.

Real-world experience, however, shows that prior tool choices dictate how hunts happen. That includes all limits that the tool choice might bring with it.

We asked further how satisfied the hunters are with the hunting approach derived from the tools that are already in place. Although only 11% were extremely satisfied, the large majority (47%) was "somewhat satisfied." That can be interpreted as a testament to vendors getting better in satisfying hunters' needs with their tools.

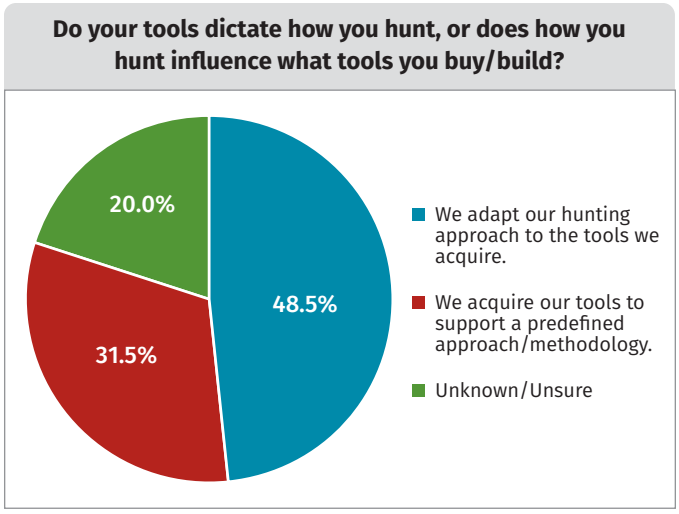

Figure 6. Influence of Current Tools on Future Tool Needs

Methodology vs. Policy

In last year's survey we were interested in whether clear policies for threat hunting existed in organizations. The result was that policies had arrived in many organizations, but others were still maturing. This year, we wanted to better understand what drives the creation of policies and threat hunting methodologies.

Our first step was getting an idea of how prevalent documented threat hunting methodologies are in respondents' organizations. Although 73% claimed that they have methodologies in place, only 35% formally define them, leaving 38% following ad hoc methodologies. That makes evaluating and improving methodologies harder than when using a formalized approach. At the same time, it might also speed up hunting by reducing the overhead introduced by formalities.

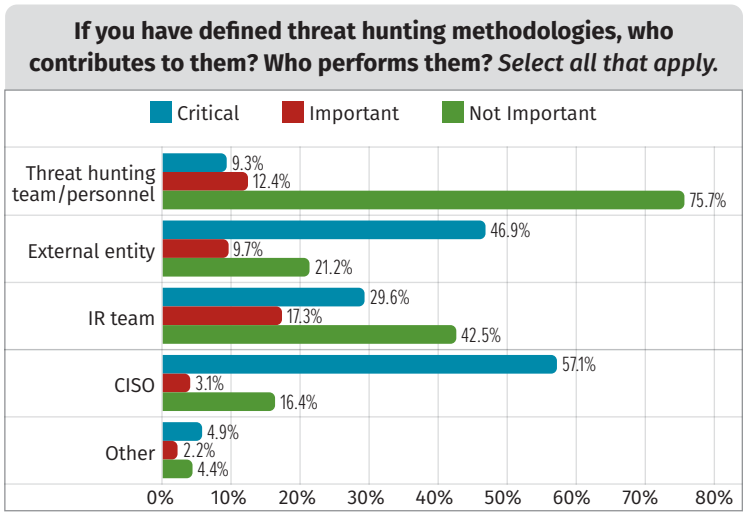

Figure 7. Methodology Contributors/Performers

For those who have defined methodologies, it's interesting to understand who drives them. We asked which distinct roles contribute to the definition, as opposed to which roles perform threat hunting methodologies. See Figure 7. It's not a surprise that the threat hunting teams are heavily involved in not only executing, but also defining the methodology. Also, the incident response (IR) teams have a leading impact on both creation and execution. This does not come as a surprise because many IR teams also execute threat hunts in organizations.

What is interesting, though, is that the chief information security officers in our respondents' organizations seem to have a significant impact on the definition of threat hunting methodologies. We interpreted this as another sign that threat hunting has arrived at C-level.

We already discussed how tooling influences methodology. What we left out is how people influence hunting strategies and how hunting strategies affect staffing. The question is quite like the one in the tools section: Do you as an organization prefer to live with the resources you have and make the best out of it, or do you prefer to define what you need first and then accumulate the resources to drive your strategy? See Figure 8.

Do your selected methodologies affect staffing strategy or does staffing influence your methodologies?
Select the best response.

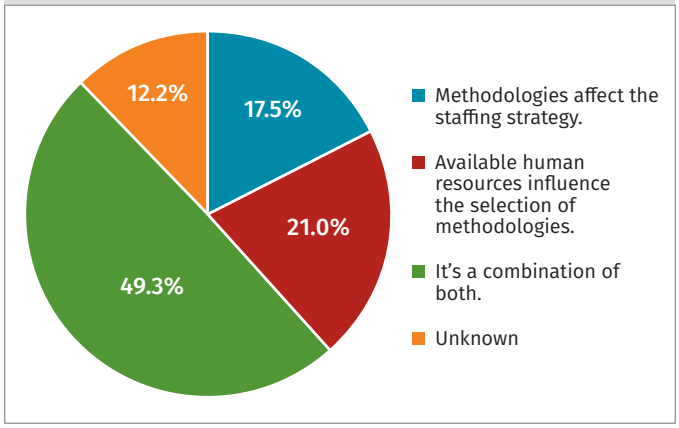

Figure 8. Staffing Drivers: Methodology vs. Staffing

For nearly half of our respondents, it's a blend of whether staffing influences the methodologies used or the methodology strategy affects further staffing, probably the most realistic approach for most organizations. Yet, for 21% of our respondents, the methodology is driven based on the staff's ability.

Although it's logical to start with what you already have, organizations need to eventually come to a point where they define how they want to hunt based on requirements rather than on capabilities. In the next step, they need to develop threat hunting teams to a point where they can fulfill the requirements.

Finally, this time we wanted to dive deeper and better understand what kinds of methodologies are floating around. The results are quite interesting. Most responses indicated quite sophisticated threat hunting strategies and methodologies. Although there were a few outliers, most respondents start with some form of mapping the field and defining their goals. This is then followed by defining the data needed to accept or reject the hypothesis. In the next step, the hunt is executed, and then the results are evaluated. A lessons learned session feeds back into the future methodology every now and then.

A good example of a threat hunting methodology would be the following response we received:

"A threat hunt is requested/suggested by management or pulled from a schedule or predetermined high-fidelity threats, then research is done to determine TTPs used and the scope of the hunt. This data is used to generate a hypothesis and hunt plan including tools and data required. Hunters have the ability to evolve … the scope and hunt plan as needed during the hunt. Any dramatic changes are discussed with the larger hunt team for validation of theories."

Internal Staff—or Outsourcing?

Conducting threat hunting is often a unique task traditionally performed by incident response staff with intimate knowledge of an organization's network, its intended functions, and the history behind how that network was initially built. In the past, we regularly saw organizations use internal staff members to conduct threat hunting due to their knowledge of the organization and its IT systems.

This year, we again asked respondents if their organization conducted threat hunting with internal or outsourced resources. We found that 63% of respondents indicated that they do not outsource their threat hunting missions, whereas 22% outsource them or seek assistance from external organizations. We also had 15% of respondents indicate either that they were unaware if third parties were assisting their organization or that outsourcing was not applicable in their specific circumstances. See Figure 9.

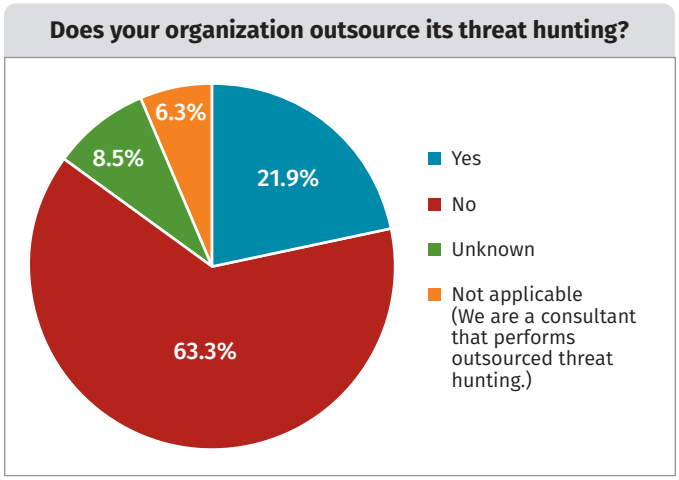

Figure 9. Outsourcing Threat Hunting

Looking back at our historical responses regarding staffing threat hunting missions, we have seen the number of organizations outsourcing their threat hunting activities move around slightly. Back in 2021, we found that 37% of respondents were outsourcing threat hunting activities, whereas last year (2022), the number decreased significantly to 25%. This year we are again seeing a decline in the number of organizations outsourcing their threat hunting missions. This trend of slowly moving away from completely outsourcing threat hunting is what we would expect organizations to do as they become more mature with their tooling and staff knowledge around threat hunting. Although this year we didn't dive into organizations that seek assistance from third parties, this is likely an area we would have to explore further in future years, given that we are starting to see the number of organizations entirely outsourcing threat hunting decrease. See Figure 10.

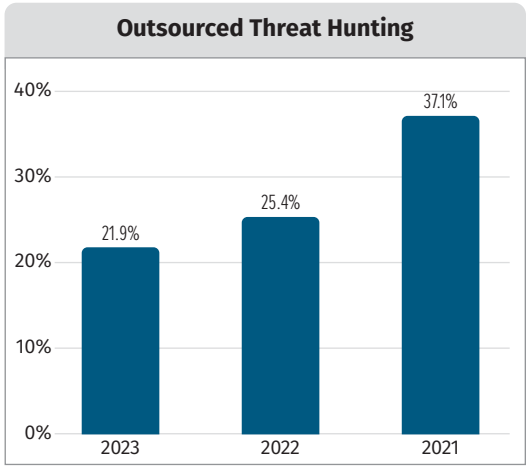

Figure 10. Outsourcing Year Over Year

So why have the number of organizations outsourcing threat hunting decreased over the last three years? It's worth keeping in mind that in 2020 we began to see the impact of COVID-19 on how organizations were staffing their security departments. We may now see the correction in the changes that occurred with internal security departments following their adjustments to the COVID-19 pandemic.

For organizations that use third parties for threat hunting activities, we see that just over half of those organizations (52%) are working together with the third party to determine the hunting ground and the mission that needs to be achieved for a threat hunt. Twenty-one percent of respondent organizations choose the hunting ground and the outcomes for the hunt mission themselves, and 24% of organizations leave those decisions entirely up to the third parties performing threat hunting on their behalf.

Organizations that are completely outsourcing their threat hunting, along with letting the outsource provider entirely determine the hunting ground and the goals of the threat hunt, are very few in terms of the number of respondents overall (3%). Of these respondents, 38% had 500 or fewer employees. This is not surprising given the time it can take to set up and perform threat hunting, which may be prohibitive for smaller organizations. It is reasonable for small organizations that do not have a large security department or substantial cybersecurity maturity to seek advice entirely from a third party.

We only began asking who was determining an organization's threat hunting goals in last year's survey (2022). This year, we see that organizations using a third party to assist them are starting to lean more toward letting the third party entirely determine the goals of a threat hunt. Last year, only 15% of respondents used a third party and allowed the third party to set the goals of the threat hunt. In contrast, this year we have seen that increase to 24%. There could be various reasons behind this change. One possible influence may be that the outsourced organization has tools for specific tasks that may limit or lend itself to what can be used as the hunting ground.

This year, we also sought to understand whether outsourcing threat hunting worked for organizations. We found that 15% of these organizations were somewhat or extremely dissatisfied with the results that the third party had achieved. Twenty-two percent of respondents indicated a neutral level of satisfaction, whereas 63% were either somewhat or extremely satisfied with outsourcing their threat hunting activities. See Figure 11.

Figure 11. Solution Satisfaction Levels

Overall, this is a relatively good finding. Ideally, we don't want to see many organizations that are outsourcing hunting dissatisfied. For the organizations in the neutral level of satisfaction and dissatisfied categories, it is likely time for their organizations to start investing further in internal tooling and knowledge for their threat hunting teams. It is common, as organizations grow and mature their cybersecurity posture, that they will likely see less benefit from outsourcing threat hunting entirely and better outcomes when they leverage the knowledge of their internal team members to perform threat hunting. Organizations need to remember that their internal staff members often know their environment the best, and this is really what you want when you're tracking down a threat actor that may be intentionally staying very quiet and producing very little alerting inside an environment.

Measuring Threat Hunting Efforts

To understand whether threat hunting impacts an organization, it is first essential to see whether organizations are formally measuring the impact of their activities on the organization. This year we saw a decrease in the number of organizations formally measuring the success of threat hunting—falling to 34% from the 43% that formally measured threat hunting in 2022. Looking back at the 2021 survey results, we see 60% of organizations were formally measuring their threat hunting. This progression of organizations decreasing any formal measurement of threat hunting activities is a concerning trend. Organizations must provide some level of confidence, or understanding, to the business of the value threat hunting offers them. Often, these types of measurements are most valuable when it comes to showing value against budget investment for training and tooling for threat hunting operations. See Figure 12.

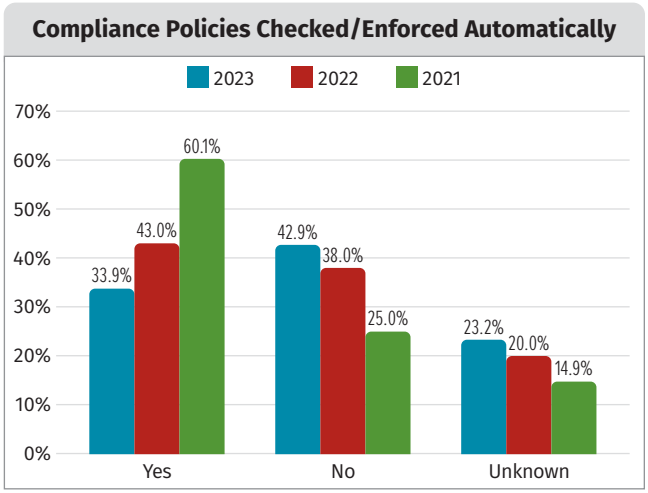

Figure 12. Measuring Efforts, Year Over Year

When asked if threat hunting improves an organization's cybersecurity overall, respondents provided similar responses to last year. This year, 81% of respondents had seen some improvement over the past 12 months because of threat hunting within their organization. Last year, 85% of respondents indicated that they saw some improvement in the previous 12 months. Even in the 2021 results, 71% of respondents saw a direct correlation between threat hunting and improving their cybersecurity posture over the past 12 months. By the numbers, this is a pleasing result, demonstrating how helpful threat hunting is to an organization. Although the numbers have moved slightly over the last three years, we still see an overwhelming majority across all three years saying that threat hunting has increased an organization's security posture when looking back at the last 12 months. If we break the numbers for this year down a little bit further, we can see that 67% of respondents say that they have seen a 25% or greater increase in the improvement of cybersecurity for their organization.

Although it is great to show how useful threat hunting can be to an organization's cybersecurity posture, we must also provide a complete picture of organizations that have yet to see any change or those that saw a negative change due to threat hunting. This year's respondents indicated that 15% of organizations saw no change to their security posture, and another 4% saw an adverse change in their security posture. For the organizations that saw no change, only 21% of them were formally measuring their threat hunting, so the remaining 79% may struggle to determine if there had been any change over the past 12 months.

Determining the usefulness of threat hunting is only as good as the method you're using to track the outcomes of your hunting. This year we saw manual tracking for threat hunting activities become the most popular method for performing any type of effectiveness tracking. We observed that 70% of organizations that formally measure the success/effectiveness of their threat hunting use manual tracking. Last year, manual tracking was also quite popular, with 68% of respondents using it. This trend of manually tracking threat hunting activities shows that there is a significant gap in the market when it comes to recording, sharing, or collating findings for a threat hunt. Although there are many options for recording case notes for digital forensics or incident response, we just aren't seeing the same when it comes to threat hunt missions.

So, what are some of the areas in which organizations are seeing a measurable increase in cybersecurity posture? Two areas stand out equally as having the most significant improvement to organizations' security posture. First, overall, 82% saw an improvement in attack surface exposure or hardening of the network and endpoints as a result of threat hunting. Additionally, another 44% saw a significant improvement from creating more accurate detections and reducing the level of false positives that organizations are seeing. These two were the same areas observed last year as having the most significant impact due to threat hunting within an organization.

It is unsurprising to see these two areas be the strongest due to threat hunting. Threat hunting, by its nature, is intended to go looking for unknown threats within an organization, and that is often where threat hunters find network and endpoint devices that are soft targets for threat actors. It is natural for these areas to see such a significant improvement for organizations performing threat hunting, because it would be typical for a hunter to find and improve an organization's attack surface.

It would also be natural for hunters to help decrease the number of false-positive alerts that an organization's SOC handles. Threat hunters should not only find undetected threats, but also turn their techniques from a hunt mission into detections for an organization, where possible. This is intended to increase the number of true positives that a security operations team handles for an organization, which, in turn, would decrease the number of false positives over time.

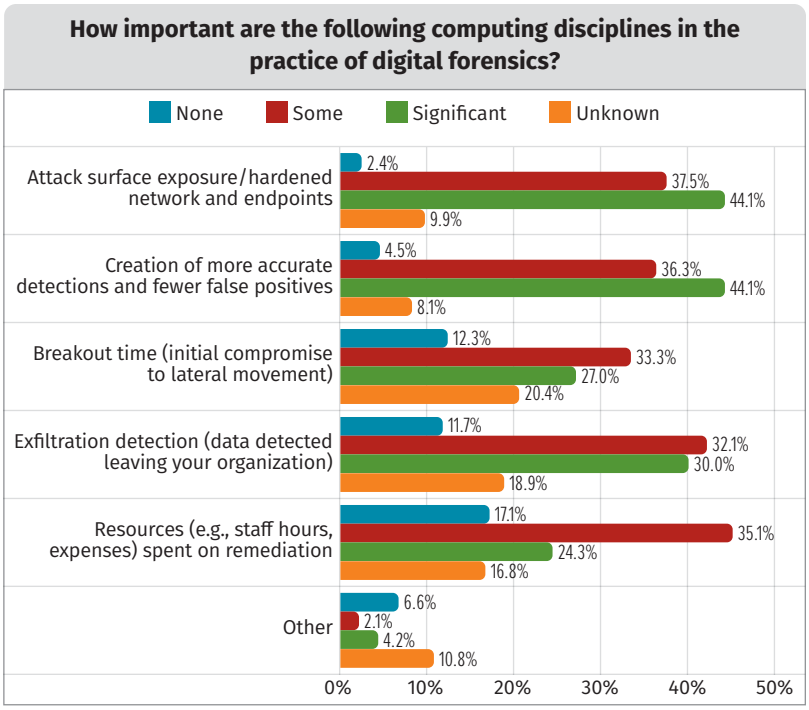

Figure 13. Overall Improvements Due to Threat Hunting

It is reassuring to see that the organizations measuring improvement from threat hunting activities are starting to see an even spread of "some improvement" among the five areas of measurement we asked about. This is still a positive outcome, because organizations should grow and see increased efficiency in all five of these areas when they conduct threat hunting correctly. See Figure 13.

When it comes to which areas organizations find challenging for planning or implementing threat hunting, we again see the need for more skilled or trained staff (73%) far outpacing any other area of challenge. Threat hunting is very much about using the knowledge of your defenders inside an organization to catch threat actors that are not detectable through automated means. This means you need defenders to be able to think creatively and know the areas that do not have automated detection, so they can use those within a hunt mission to catch threat actors. This cannot be achieved by just buying a new shiny tool that has been marketed this year. It comes down to knowledge and skill performed by humans. The use of tooling for threat hunting is important; however, we need humans to be able to use those tools creatively. See Figure 14.

Budget constraints, at 54%, is the second most challenging area cybersecurity staff face when it comes to threat hunting, followed by limitations on tools and technology for 51% of organizations. The challenge with the budget and funding for threat hunting likely contributes to both upskilling or training staff and having the capacity to purchase additional tools or technology. It is again essential that organizations focus on training and education for their threat hunting staff, because a skilled threat hunter not only can hunt for threat actors, but also ensure that funding is spent wisely on tooling and technology to further an organization's hunting capabilities.

What are the primary barriers to the success of your current efforts OR your planning to implement threat hunting? ***Select all that apply.***

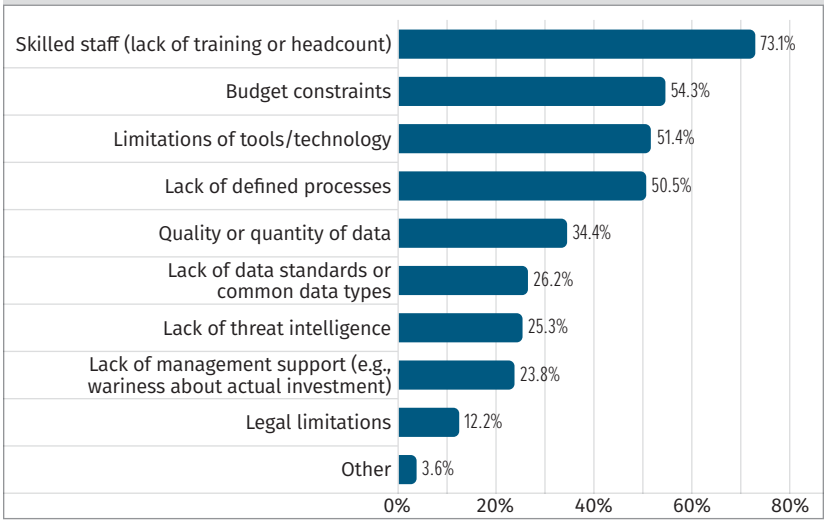

Figure 14. Barriers to Success

Unfortunately, the challenge of finding or educating threat hunting staff has become a concerning trend over the past three years. This area has become significantly more challenging for organizations since 2021, when only 51% of organizations saw skilled staff as a challenge. In contrast, in 2022, this grew to 68%, and this year we now see it in 73% of organizations. Several factors could be affecting this, ranging from a challenge with finding already skilled staff to finding funding for training or even finding skilled staff with outsourced providers. Whatever the reason, this is undoubtedly an area that organizations must focus on within the next year; otherwise, they will likely see unskilled threat hunters become a significant challenge that could have a detrimental impact on their threat hunting overall. Organizations should keep in mind that the benefits seen by threat hunting are very clear, based on the trend information we are seeing year over year from this survey. Investing in threat hunters could become a sound risk mitigation strategy for organizations.

The Need for Senior Leadership Insight and Involvement

A new addition to this year's threat hunting survey is understanding whether an organization's senior leadership is actively involved in threat hunting. It was interesting to see that 22% of organizations believe their senior leaders have no involvement in threat hunting or the activities that are performed during a hunt mission, leaving 78% to indicate that the organization's senior leadership is either aware of or has some involvement in threat hunting. This is likely due to increased interest in cybersecurity in the boardroom, so senior leaders need to understand what cybersecurity teams are doing to defend their organization. Pleasingly, 36% of organizations' senior leaders show a moderate, a lot, or a great deal of interest in what their threat hunting teams are doing.

This year, we also sought to understand in which areas threat hunters believe they need more leadership support. Naturally, we thought that this would closely correlate to threat hunters' challenges. However, we discovered that planning and process development (73%) stands out as the area where organizations need the most support from their leadership. This is, however, closely followed by staff training and skill development, at 72%, along with hiring at 64%. So, although staff development and further training are still areas that threat hunters see as needing more leadership support, we also see that threat hunters are looking to their leadership to provide planning and process to enable them to be more successful.

Conclusion

This year's survey indicated that threat hunting overall is becoming more professional. Many organizations have begun using hypothesis-based hunting, and overall methodologies have become more mature.

For many organizations, many factors of threat hunting are predetermined by the tool stack and the personnel they use. That does not come as a surprise, as tool vendors get better at understanding the needs of threat hunters and seek to deliver a better "out of the box" experience. This is supported by the ever-rising satisfaction levels with the tools. The only tool category that showed decreasing numbers in deployment are "artificial intelligence and machine learning solutions."

Although tooling has a significant impact on threat hunting, another influential factor can be external entities who run or at least support threat hunting operations. At least a quarter of our respondents outsource or out-task threat hunting. Those who do seem to be satisfied with the outcome of that setup. They also claim that in these setups, it is mostly the external entity that decides the methodology and goal of a hunt.

Threat hunting seems to be an ever-growing staffing nightmare. In this year's survey, 73% of respondents claimed that one of the biggest challenges of hunting organizations is to find skilled staff. Last year the same question came back at 68%, and in 2021 only 51% of our respondents saw staffing as a major issue.

If you ask yourself where all those threat hunters have gone, they are probably employed, and we can see the result of their work. In this year's survey, 81% of our respondents see a clear relationship between threat hunting and increased security levels.

It still is hard to measure the output of threat hunting in a formal and comparable way, so most organizations measure threat hunting output manually. Also, the number of organizations who measure at all has decreased again from 43% in 2022 to 34% this year. Back in 2020, 60% of our respondents claimed that they measured threat hunting.

There seems to be a trend to describe the output of threat hunting by indirect factors. The main measurable output of hunting operations is that it might deliver better detections with fewer false positives to the SOC. So, threat hunting acts as a testbed for SOC development. That is an effective way to increase security, get a shot at identifying attacks, and still be able to regularly provide output to the SOC.

Based on the answers we got this year, threat hunting has been professionalized. We are looking forward to seeing how it further develops over the next 12 months.

Sponsor

SANS would like to thank this paper's sponsor: