SANS

Analyst Program

Survey

SANS 2022 Threat Hunting Survey: Hunting for a Standard Methodology for Threat Hunting Teams

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

July 2022

ANOMALI®

Executive Summary

This is SANS' seventh year of conducting our Threat Hunting Survey, in which we examine how cybersecurity professionals conduct hunts in their organizations to detect and identify threats faster. In this paper, we include raw statistics from respondents, along with advice for threat hunters to consider in the next 12 months (and beyond) as they further build and improve on their threat hunting capabilities.

Our goal is to better understand how organizations develop their methodologies for threat hunting, how those methodologies influence the selection of tools and technology, and how organizations determine staffing for threat hunting teams. We spent a lot of time in the past few years learning about the methods organizations use to conduct threat hunting, and this year we wanted to know how organizations build their methodologies and maintain them over time.

We explored organizations' self-assessed maturity levels, and we asked for details about why respondents characterize their maturity as such. This year, we found that organizations overwhelmingly characterize themselves as still maturing when it comes to their threat hunting processes, with most attributing their nascent state to a lack of training and education.

When it comes to tools, we found an interesting change: Respondents use tools better suited to vulnerability management. Although this represents a particularly creative way of using vulnerability management tools, it reflects the changing landscape of how threat actors increasingly compromise organizations through known vulnerabilities.

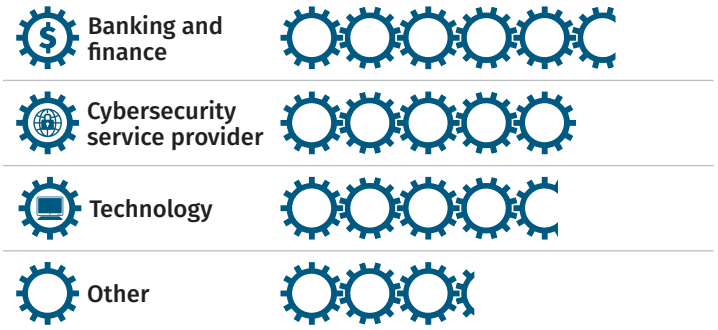
We found a correlation between organizations that are still maturing their threat hunting methodologies and those particularly unsatisfied with their current tools. Unfortunately, this is not surprising. From what we observe within the industry, organizations often procure tooling and technology prior to building processes or methodologies. For more mature organizations that use formalized methodologies to conduct threat hunting, we also drilled down to discern precisely what methodologies they leverage.

Another key finding this year is that training and education play a big part in the challenges that organizations face, which we address in further detail throughout the report. Meanwhile, other noteworthy findings include the following:

- 51% of our respondents consider their threat hunting as still maturing.
- 68% of organizations lack training or skilled staff for threat hunting.
- 62% of our respondents use internally developed tools.
- 48% are seeking to extend their threating hunting capabilities into the cloud.
- 25% of organizations outsource threat hunting tasks.
- 68% of organizations measuring their threat hunting saw an increase between 25% to 75% in the overall security posture of their organization.
- Nearly half (47%) of organizations that threat hunt have noticed improvement in the accuracy of threat detections and fewer false positives.

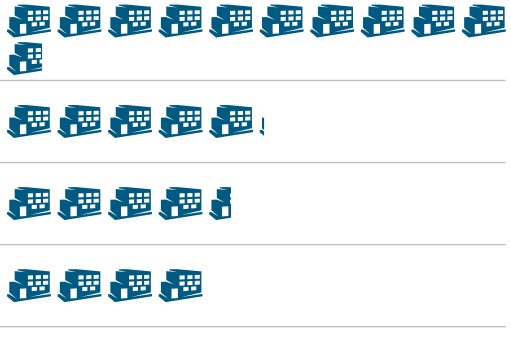
Figure 1 provides a snapshot of the demographics for the respondents to the 2022 survey.

Top 4 Industries Represented



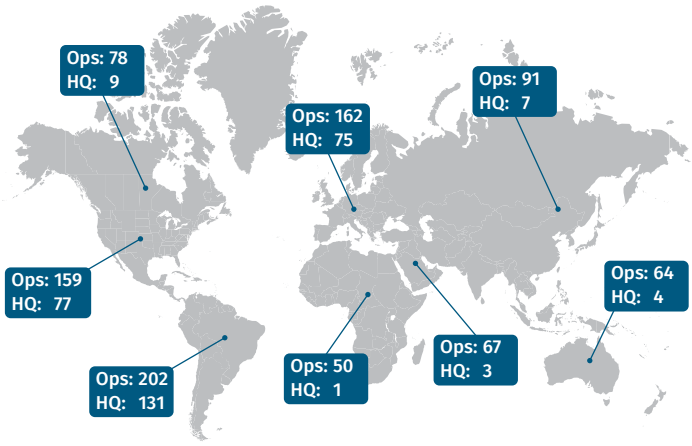
Each gear represents 10 respondents.

Organizational Size



Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented

Each person represents 10 respondents.

Figure 1. Demographics of Survey Respondents

Threat Hunting Maturity

To kick off our threat hunting survey this year, we asked respondents how mature they considered threat hunting to be within their organization. For this initial question, slightly more than half (51%) of respondents indicated that they are still in the "maturing" stage and developing threat hunting inside their organization. This number shows an increase over what we saw in the 2021 survey, in which 40% of respondents indicated that they were in a maturing state.[1] See Figure 2.

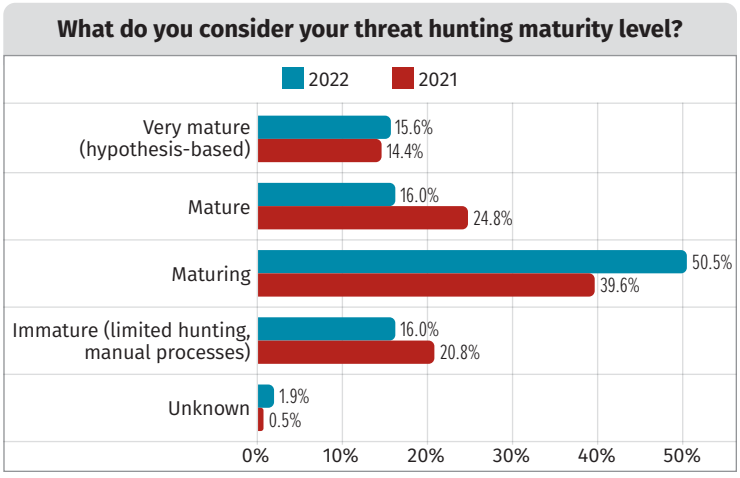


Figure 2. Threat Hunting Maturity

[1] "A SANS 2021 Survey: Threat Hunting in Uncertain Times," September 2021, www.sans.org/white-papers/sans-2021-survey-threat-hunting-uncertain-times/, p. 3. [Registration required]

The increase in this number from last year's survey comes from organizations that no longer consider themselves to be in the mature state with regard to their threat hunting. Perhaps organizations are taking a more realistic approach, or maybe organizations now understand threat hunting is an ever-evolving task in an organization (and thus ensure its continuous setup as appropriate for their organization).

Asking respondents how they assess the maturity of their organization's threat hunting generated numerous comments, many reflecting an approach to maturity and further growing their capabilities. Common themes include: "It's a growing area," "Log sources are maturing," and "The company is maturing, as it realizes that information security is not just a business support area, but a strategic area." In addition, some respondents still struggle with consistency as to how they share data or standardize their threat intelligence, as indicated by comments such as "Lack of standardization and sharing of threat data."

By far, lack of skilled staff or training represents the primary barrier to successful implementation of threat hunting, with 68% of respondents indicating this obstacle. The next three barriers almost tied for second place: a lack of defined processes or methodology (49%), budget constraints within an organization (48%), and limitations of tools or technologies already existent within an organization (47%). See Figure 3.

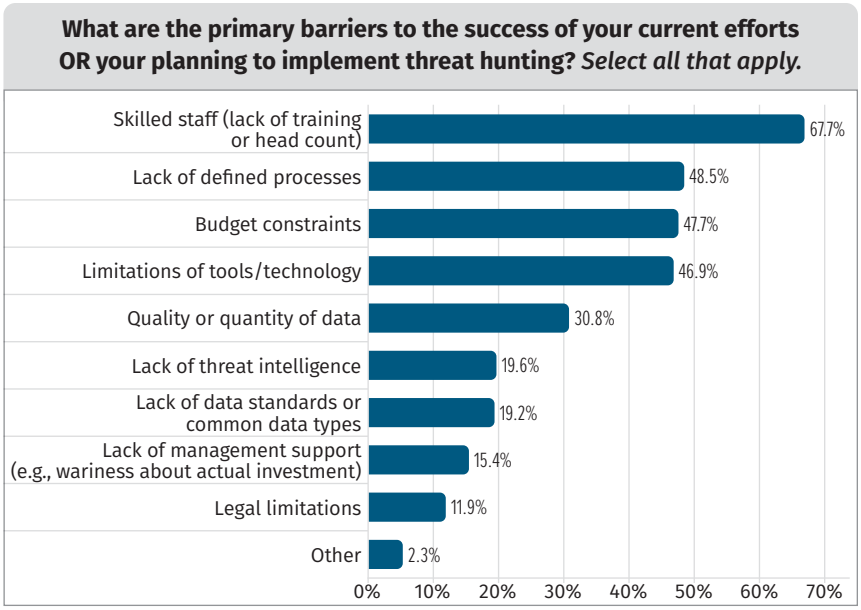


Figure 3. Barriers to Threat Hunting Success

The findings for the barriers that organizations face isn't surprising: Skilled staff (lack of training or head count) is the first barrier that organizations must overcome. If organizations had better-skilled or -trained threat hunters, they might more ably resolve issues related to a lack of defined processes or to the ability to find cost-saving benefits.

For the fourth-highest-ranked challenge, respondents see a significant issue in the limitations of their tools and technologies. It's important that organizations understand that processes really must be built before acquiring tools or technology to facilitate those processes. Purchasing tools and then trying to wrap a process or methodology around them is a backward approach, not only for threat hunting but also for performing any type of cybersecurity operations role.

Respondents this year also indicated for the first time that they want to build better capabilities for threat hunting within the cloud. And we continue to see respondents looking for better enrichment of data and contextualization of data, which are common requests by threat hunters to increase their efficiency and speed in understanding what they are looking at. Confusion still seems to exist, however, between exactly what threat hunting is and what regular security operations within an organization should be. We found that this confusion is slowly decreasing over time, but in the threat hunting surveys we have offered, it still shows as an issue facing some of our respondents.

Tooling for Threat Hunting, or Hunting for Tooling

As in the past couple of years, we wanted to look into the hunters' tool chests. Although threat hunting is not a pure tooling game, selecting appropriate tools factors significantly into the quality of threat hunting. Good threat hunting usually means bringing together skilled staff, internal knowledge, and tools that establish visibility.

When most employees worked from home due to COVID-19 restrictions, the demand for alternative or additional threat hunting approaches likely increased. For that reason, this time we asked not only about which tooling and technologies their organizations currently use, but also what they implemented in the past 24 months.

Threat hunting has some fundamental aspects. Hunters need visibility into a high percentage of the available endpoints in an organization. That way, every covered endpoint acts as a sensor. As a result, the room for an attacker to move freely reduces. Once threat hunters have almost total visibility into the enterprise, they need to know what to look for. That's where good, actionable threat intelligence comes into place. So, the trinity of requirements for threat hunting comprises qualified hunters who use tools to establish visibility and who then bring knowledge and threat intelligence into action.

Unsurprisingly, classical security tools like SIEMs and EDRs again led the list this year, with 83% of respondents using them for threat hunting. We find these tools in most midsize and large organizations today and sometimes even in small companies. SIEMs and EDRs are expensive and usually offer functionality that supports all forms of threat hunting.

"Third-party platforms that deliver threat intelligence" came in second, at 66% of our respondents. An observation from the last few surveys—and from real-world scenarios—is that coverage gaps still seem to exist with regard to off-the-shelf tools. In fact, 62% of our respondents use internally developed tools, beating out open source tools, which come in at 40%. So, commercial tool vendors have quite an opportunity to listen to their clients, evolve, and close the various feature gaps. See Figure 4.

The developments over the past 24 months provide interesting insight. We asked respondents to identify which of these technologies/tools (the ones they had previously identified) they added to their tool chest in the previous two years. See Figure 4.

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

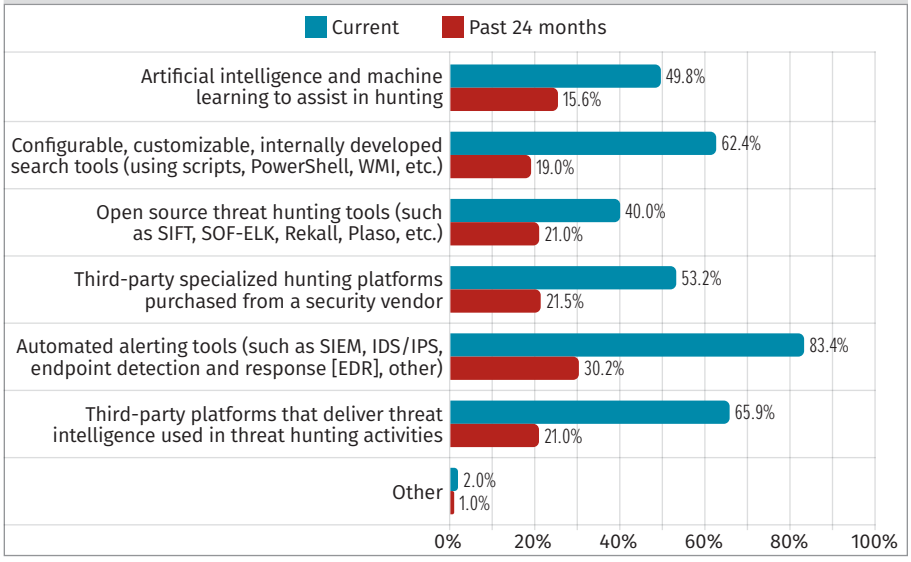


Figure 4. Threat Hunting Tools/Technologies

Unsurprisingly, classical tools such as SIEMs and EDRs come in first again, at 30%. So, almost a third of respondents changed their security posture by investing in SIEMs, EDRs, and IDS/IPS solutions. Interestingly, nearly half of respondents count on artificial intelligence (AI) and machine learning (ML) tools; only 16% invested in these tools over the past two years. That is the lowest growth percentage of all categories covered.

Many organizations report that during the COVID-19 pandemic they struggled to pick the right solution within the different categories. If you are interested in how well specific solutions work to detect various attacker groups, MITRE offers an independent assessment on its website.[2] (It's always a good place to understand how tools work in real-world scenarios). Also, MITRE offers a highly beneficial blog post[3] that explains how the scoring works, from which you can glean a lot of information about how to evaluate security tools and avoid pitfalls in the evaluation process in general.

Also noteworthy, several respondents reported that they started using vulnerability management solutions for threat hunting (an interesting development). In the past two years, the number of easily exploitable vulnerabilities that affect external-facing infrastructure (Exchange Servers, Log4j, Confluence) shifted the playing field. Whereas classical threat hunting looked for traces of an attack from the inside, the proactive, vulnerability-focused approach operates from a different hypothesis. When an organization exposes a vulnerable application to the internet, it usually can be considered breached. Instead of relying on traces of the breach, security teams can save time by starting their hunt with a vulnerability assessment to find the most likely entry points.

We also wanted to know how satisfied threat hunters are with the various tools they use for threat hunting. This year again, our respondents are very satisfied with automated alerting tools such as SIEMs, EDRs, and IDS/IPS solutions: 35% of respondents are "very satisfied" with their solution and 45% are "satisfied." Generally, the satisfaction shows as evenly distributed across the different tool sets. The overall dissatisfaction vote comes in at below 7% across the board. These numbers might indicate that tool vendors getting ever closer to meeting threat hunters' needs. See Figure 5.

What is your level of satisfaction with the tools/technologies that you are currently using in support of your threat hunting activities?

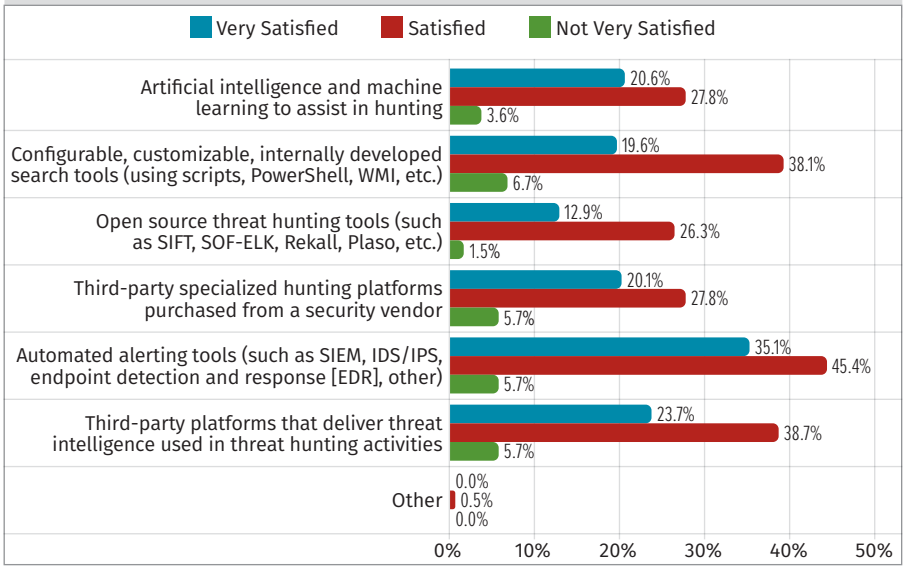


Figure 5. Level of Satisfaction with Tools/Technologies

[2] "Open and fair evaluations based on ATT&CK," https://attackevals.mitre-engenuity.org

[3] "Making Sense of Attack Evaluations Data: Who Really Won and How to Avoid Common Pitfalls," MITRE-Engenuity, https://medium.com/mitre-engenuity/making-sense-of-att-ck-evaluations-data-42ca844940b9

Another interesting point is the way in which tools impact how organizations run today's threat hunting operations. Specifically, that 44% of respondents report that they have to shape their threat hunting methodology to match the capabilities of a preexisting tool, a factor that may severely limit the effectiveness of threat hunting. As previously indicated, visibility is one of the main requirements for threat hunting. We differentiate between horizontal and vertical visibility. *Horizontal visibility* means how much of the endpoint population a tool covers. *Vertical visibility* describes which artifacts a solution can see per endpoint. Whereas horizontal visibility is usually not limited by a tool but by lousy asset management, vertical visibility can be strongly reduced when using the wrong tool. Rarely is anything as frustrating in threat hunting as when you acquire sound intelligence in the form of indicators of compromise (IoCs) and cannot bring them into action because the tools in place can check only half of the features described in the IoCs.

A lack of vertical visibility is more likely to occur when tools dictate the approach rather than when the approach influences tool choices. In light of that, it's good to see that 41% of our respondents pick their tools to support a predefined methodology.

Hunting for the Right Methodology

Over the past few years, during which both the authors have had the opportunity to conduct the threat hunting survey, one thing has interested both of us: how coordinated an organization is when it comes to conducting threat hunting. This year we spent some time refining our survey questions to better understand how organizations coordinate or build a methodology to enable them to threat hunt inside their organization. We directly asked a number of questions designed to better understand not only whether an organization has a threat hunting methodology, but also which types of tools and resources they use(d) to develop that methodology.

As part of our findings, we discovered that 75% of respondents believe that they have one or more clearly defined methodologies for threat hunting within their organization. Of these respondents, 40% indicated that they have a formally defined methodology, while 36% state that their methodology is ad hoc (this last percentage perhaps due to them still discovering what type of methodology best suits their organization or their capabilities within the organization). See Figure 6.

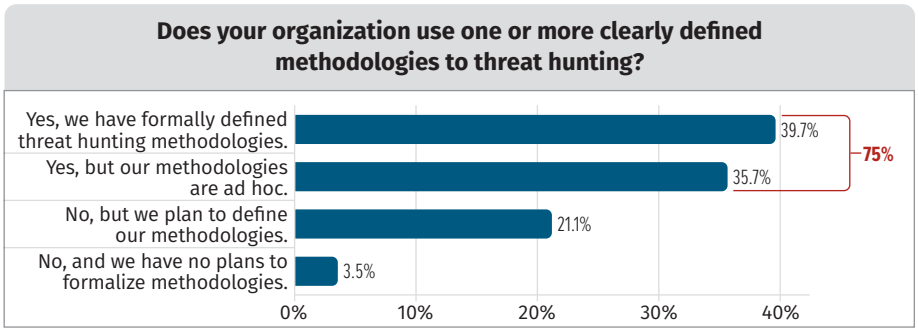


Figure 6. Threat Hunting Methodologies

Of the respondents who reported that they have no formal methodology, 21% indicated that they plan to develop a methodology in the near future, with only 4% reporting that they have no formal methodology and no plans to formalize any type of threat hunting methodology. Building a formal threat hunting methodology is important for a number of reasons. Arguably most important, a formal process ensures that when you conduct threat hunting you have a defined scope and specific procedure to ensure that you do not repeat activities conducted in the past and that you get the best coverage possible for your organization. Otherwise, without a methodology, an organization may derive little benefit from conducting any type of threat hunting.

Reviewing a threat hunt methodology either quarterly or twice a year is probably enough for most organizations. Remember, a methodology exists to guide an organization on how you define scoping for a hunt, how you go about conducting a threat hunt, what tooling and technology you need, and how you might review the benefits and outputs of a threat hunt. Reviewing threat hunting methodology too often could lead to fatigue or confusion among those who are conducting the threat hunting activities, along with the possibility for any output or measurements from a threat hunt to not be easily compared with previous threat hunts.

According to this survey, 75% of respondents use some type of methodology. So, what type of methodology do these organizations use? Well, unfortunately this is not a simple question to ask in survey form because organizations use a variety of methods. To get some type of sensible answer, we left the answer for this question as a free-form text field, which means we spent a lot of time trying to categorize all the various answers. We broadly narrowed down responses into the following most common categories:

- Indicator of compromise (IoC) or tactic tool and technique-based
- Known threat actor technique-based
- Hypothesis-based
- Threat intelligence-led

The "indicator of compromise (IoC) or tactic tool and technique-based" technique was the most commonly mentioned type of technique used for developing a methodology for threat hunting. Such placement is unsurprising, given that extracting indicators from external reporting, or threat intelligence feeds, is a relatively simple task to perform and probably the easiest when performing repeatable searching. The only big downside we see to this form of methodology development is that security teams should include indicators inside of an alerting system or a SIEM for more automated detection and triage.

Respondents who reported developing hunt methodology based on the "known threat actor technique" predominantly identified specific frameworks, such as the MITRE ATT&CK framework,[4] the Cyber Kill Chain,[5] or frameworks provided by U.S. federal government authorities. Using these to develop a threat hunting methodology represents an improvement over using indicators because organizations are at least using frameworks that better represent what threat actors do regardless of the type of attack for which they might be hunting. The challenge with this technique, however, is that it is extremely broad and might not suit specific threats targeting the organization you're trying to protect (which could leave you threat hunting based on hypotheses that may never apply to your organization).

The third most common category based on respondent reporting was "hypothesis-based" threat hunting. This is really good to see because it means that an organization is developing a hypothesis based on what a threat actor may target related to their organization and also how that threat actor may act once inside the organization. The significant benefit with this type of threat hunting is that it really narrows the focus of which threats you hunt and which activities those threats might perform inside an organization. Think of this as a narrowed approach compared to the "known threat actor technique" discussed previously.

Lastly, respondents reported that they are using "threat intelligence-led" threat hunting. Based on the responses received, it appears this is a combination of extracting indicators from threat intelligence along with searching for techniques used by threat actors from public intelligence. This appears to be primarily used by organizations that are somewhere in between "indicator of compromise (IoC) or tactic tool and technique-based" and "hypothesis-based" threat hunting. We hope, though, this actually shows organizations are slowly but surely transitioning to a more hypothesis-based threat hunting methodology.

A significant finding from other responses indicates that some organizations predominantly use their alerting system and investigate those alerts and consider this task threat hunting. If you review security alerts or detections and triage those, however, you are performing a fairly normal security operations center role, which unfortunately is not threat hunting. Organizations that fell into this category really need to remember that threat hunting is the task of manually looking for threats inside an organization where they do not have automated detections or alerting coverage for suspicious behavior.

Regardless of the exact technique used to develop a threat hunting methodology, it is imperative for your organization to think about how it can hunt in a more repeatable process, how it can show measured improvement over time, and how the hunt contributes to the overall security posture to reduce dwell time and lessen the number of threat actors achieving their actions on objectives. Remember, as a threat hunter, you are not really in the position to prevent a threat from ever entering an organization. However, you are very much in a position to prevent threat actors from performing their actions and achieving objectives, which you really should consider the best measure of threat hunting success.

---

[4] "MITRE ATT&CK," https://attack.mitre.org

[5] "The Cyber Kill Chain," www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

One of the largest influences we found, for organizations developing a threat hunting methodology, was staff resourcing. In this survey, 90% of respondents indicated that they consider staffing resources for their organization a significant factor with regard to threat hunting methodology development. Breaking that down further, we found a close split between organizations that said that their methodology directly impacts acquiring additional staff (23%) and organizations that said they develop their methodology based on resources currently available within the organization (23%). Although it makes complete sense that it would be silly to build a methodology that could never be staffed, it is also important to understand that when it comes to a methodology for threat hunting you should ensure its scalability to better cope with fluctuations in staffing levels.

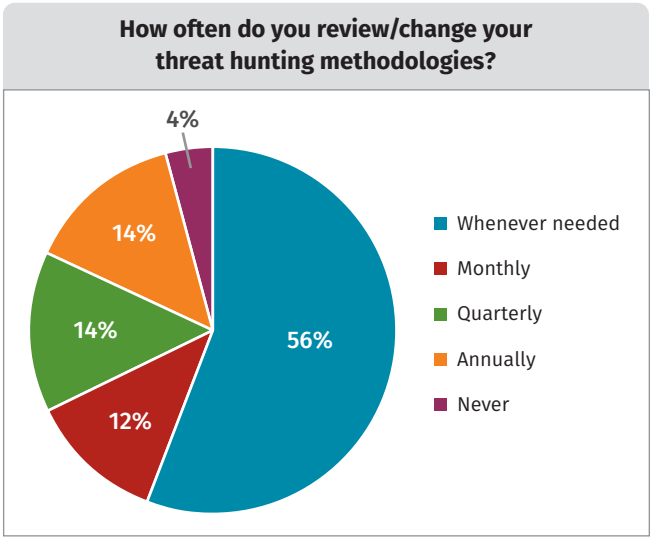


Figure 7. Frequency of Changes to Threat Hunting Methodologies (Excluding Unknowns)

As we delved into these results further, we also tried to understand how often organizations conduct any type of review or assessment and methodology to ensure that it is still works as intended and continues to provide the benefit the organization anticipated. We asked respondents how often they review their threat hunting methodologies. The majority knew details about when this occurred. However, 16% were unsure. To make these numbers useful, we excluded the 16% from the data, leaving us with 56% who indicated that they reassess their methodology only when the organization needs to. This number may indicate that threat hunting within organizations is more ad hoc than formalized. On the plus side, organizations at least seem to be thinking about making changes or reviewing their threat hunting methodology, with only 4% indicating that they never review their methodology. It is comforting to see that 40% conduct regularly scheduled reviews of their methodology (12% conduct monthly reviews, 14% conduct quarterly reviews, and 14% perform annual reviews). See Figure 7.

When it comes to looking into the future, we also wanted to know which changes organizations plan to make (or would like to make) to their threat hunting capabilities. Often, a close correlation exists between an organization's threat hunt methodology (and intentions) and the practicalities of executing that methodology based on other factors (people, tools, capabilities). This year, more organizations than not (53%) reported that they need more internal staff with investigation-based skills to perform threat hunting. In most cases, this often points to two essential needs inside an organization: actually acquiring staff for the threat hunting team and training and education skills for that staff. See Figure 8 on the next page.

Other improvements that organizations significantly seek include the ability to acquire tools and capabilities to extend their threat hunting into the cloud (48%), better incorporating AI and ML into threat hunting tools (45%), and better contextual awareness provided by an organization's internal data sources or the tools used within the organization (43%). This is the first time we've seen from respondents that they want to extend threat hunting capabilities into the cloud, which seems like a natural fit given how many organizations are moving their IT workloads into the cloud. The other two most-wanted improvements are better capabilities and better visibility built into their threat hunting tools. The desire to have better functionality within threat hunting tools has been a common theme we've heard from respondents whenever we ask for details about tools they use for threat hunting. Obviously, threat hunting tools have a long way to go to meet the needs of threat hunters today.

What improvements do you need to make/would you plan to make with respect to your threat hunting capabilities? ***Select all that apply.***

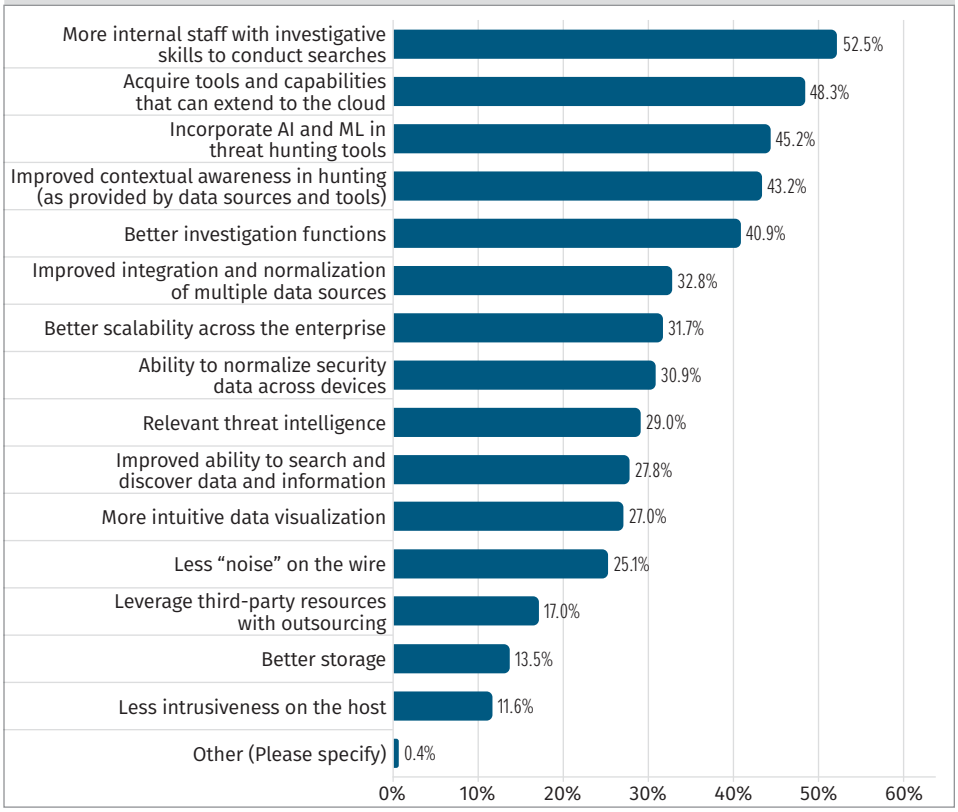


Figure 8. Threat Hunting Improvements Needed

People Are at the Center of Threat Hunting

Like last year, we wanted to know who usually hunts in organizations and how well different staffing approaches work. This year's survey showed a surprisingly high number of respondents who use external threat hunters (25%). So, every fourth company outsources threat hunting. At the same time, 59% run all threat hunting operations in-house. Both approaches come with upsides and downsides.

On the one hand, external threat hunters might have an advantage because they will usually hunt in multiple organizations, which means they can quickly transfer experiences from one client to another. On the other hand, external hunters are typically not as close to the organization as internal staff. They might not always have the same level of understanding about an organization's infrastructure. Both approaches work, but organizations can also always team up internal and external forces to get the most out of hunting exercises.

To some extent, that appears to be what's happening most often. Among organizations that outsource threat hunting, 60% indicated that they define the hunting grounds and outcome with the external party, which suggests a joint approach. A quarter (26%) of respondents who outsource threat hunting determine the hunting grounds/scope and outcomes internally. The external entity ends up just executing the threat hunt. In these settings, it might make more sense to insource the actual hands-on activity as well.

With regard to personnel sourcing strategies, COVID-19 did have a negative impact. We wanted to better understand what the virus affected the most. The good news is that only 14% of respondents stated that COVID-19 negatively impacted their hunting. The regulations around COVID-19 significantly limited travel and personal contact. For that reason, it is not surprising that most adverse effects related to training and threat hunting occurred in other remote locations.

As to planned staffing for threat hunting, our data points to a significant increase in the number of hunters in most organizations. While just 7% think about reducing threat hunting capacity, 65% want to grow their teams between 10% and 100% (see Figure 9). Although this has the potential to strengthen these organizations' security posture, the current employment market might not prove conducive to filling their open positions any time soon.

Does your organization plan to change its investment in the tools or staffing for threat hunting in the next 24 months?
Estimate to the closest percent how much the change in investment might be.

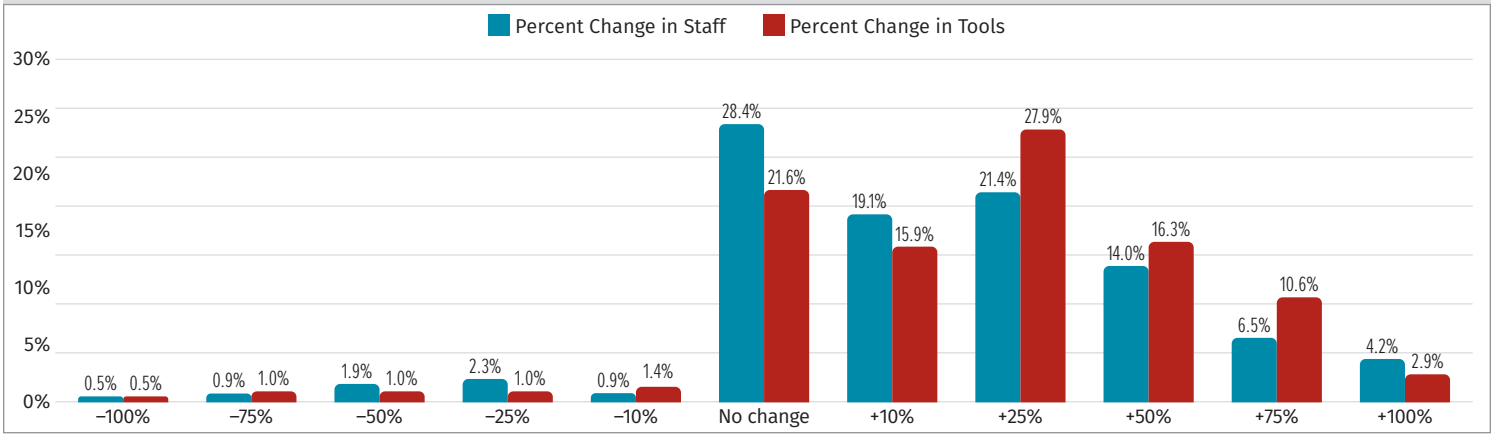


Figure 9. Threat Hunting Investment Plans

Measuring Success in the World of Threat Hunting

Measuring threat hunting success vitally informs organizations about the utility of their threat hunting and also ensures that the methodologies and techniques they're using evolve and continue to protect. Therefore, organizations must measure success in a consistent and repeatable manner. We asked how many organizations formally measure the impact of threat hunting; only 43% reported that they formally measure the effectiveness of their threat hunting. See Figure 10.

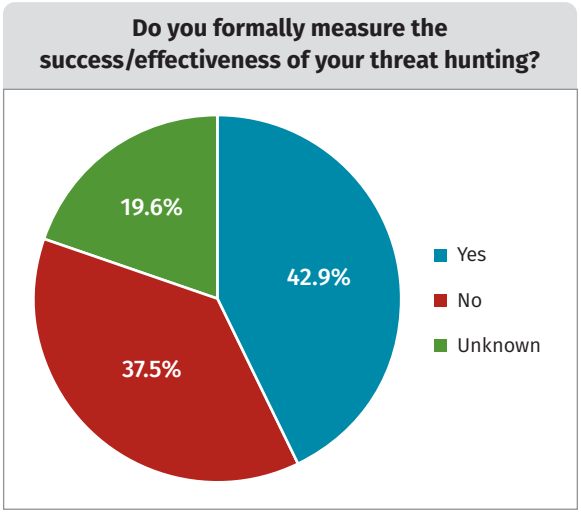


Figure 10. Measuring Threat Hunting Effectiveness

This is a significantly and sadly low number because this question was asked to respondents who are actively conducting threat hunting within their organization. In contrast, in the 2021 survey, we found that 60% of respondents measured the impact threat hunting has on their organization. This means that we've seen a significant shift backward in respondents being able to show the usefulness of threat hunting to their organization. Also note that some respondents (20%) indicated they are unsure whether their organization formally measured threat hunting. This percentage also slightly increased from the 2021 survey, where 15% of organizations reported as unsure with regard to any threat hunting measurement scheme that might have been in place.

Of the organizations that measure how useful threat hunting is to them, the majority of respondents (74%) track their success through automated means, whereas 68% manually track threat hunting success. In contrast to the 2021 survey, in which only 45% of respondents performed automated tracking, it is good that most respondents this year tracking threat hunting effectiveness use some type of automated means. With regard to how organizations measure the success of threat hunting, 60% look at the number of legitimate alerts generated based on threat intelligence sources that perform alerting for their organization—a relatively simplistic way of tracking the effectiveness of alerts to your security operations team (who have to triage them). A large percentage of respondents (47%) use ad hoc methods to measure effectiveness. Concerningly, though, ad hoc methods with regard to measurement do not enable you to show change over time for the organization, which is really what you want to do to ensure your threat hunting is meaningful to the business.

We also delved deeper by asking respondents how much of an improvement overall threat hunting has had to the security posture of an organization. In this survey, 85% report that they see some impact to the security posture of their organization. That represents a brilliant win for organizations conducting threat hunting, showing that threat hunting does have a meaningful impact on organizations. Note, however, that 10% of respondents indicated they see no change to their organization, and 5% of respondents reported they see a negative impact on their organization's security posture. In the 2021 survey results, 28% of respondents observed no impact or a negative impact on their overall security posture, so it is a positive that this number is slowly decreasing. It will prove interesting in future years what any of those negative change may have been. However, given the small number of respondents who reported such, we might not garner enough responses to produce meaningful information. Of the organizations that reported a positive impact to their security posture, most respondents (48%) saw a 25% to 50% increase in the security posture for their organization. An encouraging and exciting number to report is the 7% of respondents who reported a 100% security posture improvement. See Figure 11.

Has threat hunting provided improvement in the overall security of your organization?
If so, estimate the percent improvement during the past 12 months to the nearest percentage.

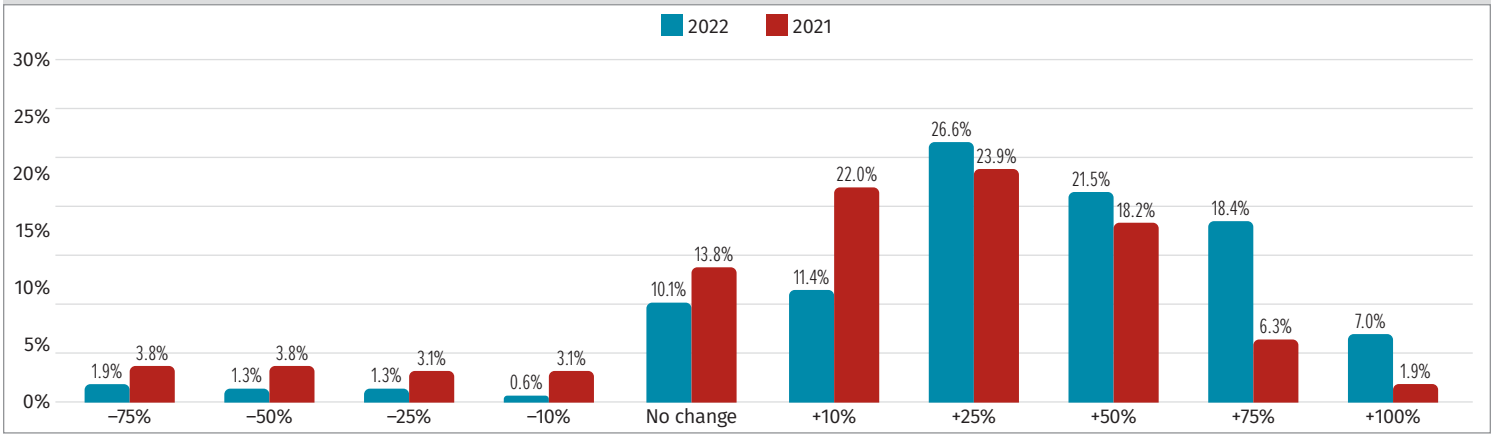


Figure 11. Threat Hunting Improvements to Security Posture

So, at which locations do organizations report this positive change within their security posture? The most significant place where organizations observe a measurable improvement is in reducing the overall attack surface and hardening of the network and endpoints within their IT environment, with 53% of respondents indicating that they see significant improvement in this area. In addition, 47% reported that they see a significant improvement in more accurate detections and fewer false positives for the security operations team, along with 40% of organizations seeing some improvement in the same area.

Surprisingly, 46% of respondents indicated that they see some improvement in their overall resources to spend time on remediation following a security incident. Logically this makes sense because the goal of threat hunting is to find an adversary faster, in the hope that you catch them before they complete their actions or objectives. So, that organizations see some improvement in reducing the time spent on the remediation makes complete sense for those successfully conducting threat hunting. See Figure 12.

Which of the following have shown measurable improvement as a result of your threat hunting efforts? *Select all that apply.*

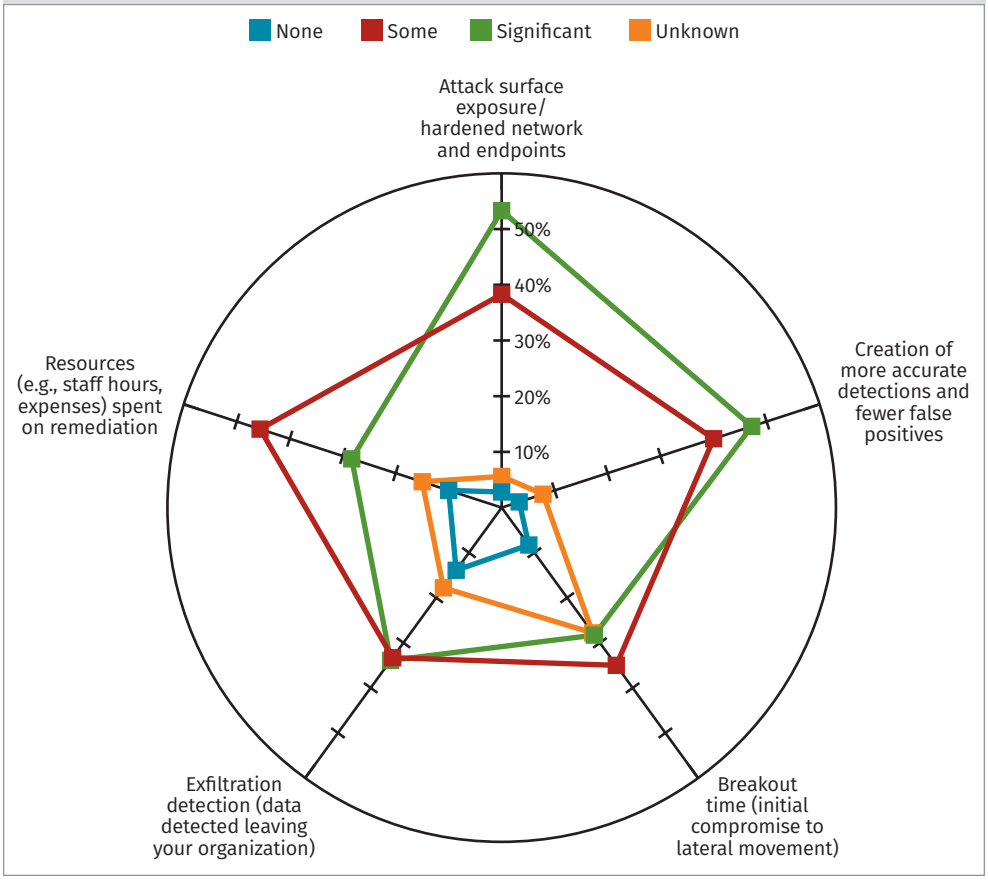


Figure 12. Threat Hunting Measurable Improvements

Although no clear outliers show as to areas where organizations do not see some improvement to the security posture, one area has the lowest percentage (that is, the highest number of respondents unsure of any measurable change): the measuring of breakout time (the time it takes an adversary to laterally move from an initial compromised system to a second compromised system). As for breakout time, 28% of respondents reported as unsure whether they had seen a measurable improvement. During threat hunting, organizations might find it difficult to determine whether they have caught an adversary on an initially compromised system or on a subsequent system afterward. This difficulty might partly explain the struggle of knowing, at least from statistics of just performing a threat hunt, whether an organization has decreased breakout time.

Conclusion

Based on this year's survey, decision makers in companies are finally recognizing the importance of threat hunting. Many respondents now want to improve threat hunting operations, with 51% reporting that they are still maturing. Over the next few years, we'll witness increasingly high demand for skilled staff and tools that act as force multipliers for threat hunters. The biggest thing that holds back organizations from becoming more proficient in threat hunting is their lack of skilled staff; 68% of our respondents identify that as the main reason for threat hunting failures.

Threat hunters report being more satisfied with their tool sets. Traditional security tools such as SIEMs and EDRs remain high on the list of satisfactory tools. Tools with AI to support threat hunting show up in only 50% of our respondents' organizations, but only 16% claim that they have invested in that tool category in the past 24 months.

At 44%, many threat hunters claim that they have to shape their threat hunting operations based on the capabilities of current tools. Often that approach proves unsuccessful. Organizations will always find it beneficial to let their teams' processes/procedures drive tool decisions in security instead of allowing tools to dictate processes.

When looking at the past year of the pandemic, only 14% of respondents reported a negative impact on actually conducting threat hunting operations. They observed more negative effects on training availability, which may add to the dramatic staffing-shortage situation. Unsurprisingly, most respondents want to grow their threat hunting operations significantly. Over the next few years, the challenge in the industry will be to educate people about threat hunting techniques and tactics. Tool vendors need to get even better at acting as force multipliers and at taking as many tasks from threat hunters as safely possible.

Our general impression is that the industry is getting closer, as compared to the past few years, to proficient and professional threat hunting across the board. Problems have been identified, and organizations are planning to mitigate them.

Sponsor

SANS would like to thank this survey's sponsor:

ANOMALI®