SANS

Analyst Program

Survey

A SANS 2021 Survey: Threat Hunting in Uncertain Times

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

September 2021

DOMAINTOOLS®

Executive Summary

For six years, SANS has conducted a Threat Hunting Survey to examine how cybersecurity professionals hunt inside their organizations to more rapidly detect and identify threats. This year's survey seeks to better understand the current landscape of threat hunting for organizations and the benefits that threat hunting can bring to an organization's security posture. Based on the responses to the 2021 survey, this paper summarizes changes that we have seen over the past two years of authoring the threat hunting survey for SANS, as well as observations about those changes. We also look at how organizations have improved their threat hunting efforts over time.

Unlike in previous years, the 2021 survey included questions about the impact of COVID-19 on threat hunting efforts. Organizations experienced varying impacts from the pandemic: Some organizations experienced a negative impact on their security postures, while others saw a more targeted focus on cybersecurity and threat hunting in their organization. A significant number of respondents report uncertainty as to what type of impact the pandemic has had on their threat hunting teams. Significant uncertainty about the pandemic lingers, and many respondents report they anticipate significantly increasing their threat hunting activities in the coming 24 months.

Most of this year's respondents consider their threat hunting methodology and techniques under development and acknowledge that they need to make further progress regarding this function within their security program. Respondents report that when it comes to maturing their threat hunting program, the tooling they have for threat hunting and their ability to systematically measure improvement represent their top challenges.

When it comes to visibility into their environments, nearly all respondents report that automated alerting tools based on usual endpoint detection, SIEM, and traditional network detection tools remain the technologies of choice for hunting. We discovered that a strong preference remains for threat hunters to build their own internal tooling to gain better visibility into their environments, which highlights the challenges that still exist for getting full visibility with security telemetry tooling.

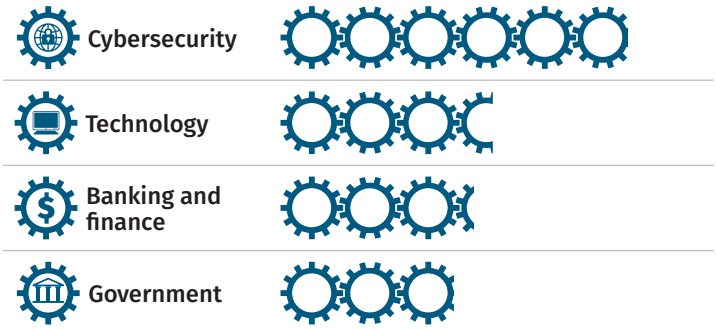
Key Findings

- **11%** of organizations observed some impact on their threat hunting team or methodology in the past year.
- **12%** fewer organizations perform threat hunting in 2021 as compared with 2020.
- **75%** of respondents prefer endpoint, SIEM, and traditional network detection tools for threat hunting.
- Organizations see a **10% to 25%** improvement in their overall security posture from threat hunting.
- **51%** of organizations manually track their threat hunting activities.
- **51%** identify lack of skilled staff and training as the primary barrier to success as a threat hunting team.

As a result of threat hunting, organizations' overall security posture continues to improve, further reminding us of the benefits that threat hunting can bring to an organization. The results also show that significant benefit accrues to security teams as well; because of their continuous security monitoring, they see better detection and fewer false positives.

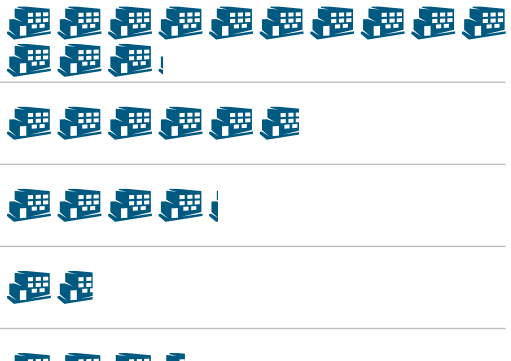
Figure 1 provides a snapshot of the demographics for the respondents to the 2021 survey.

Top 4 Industries Represented



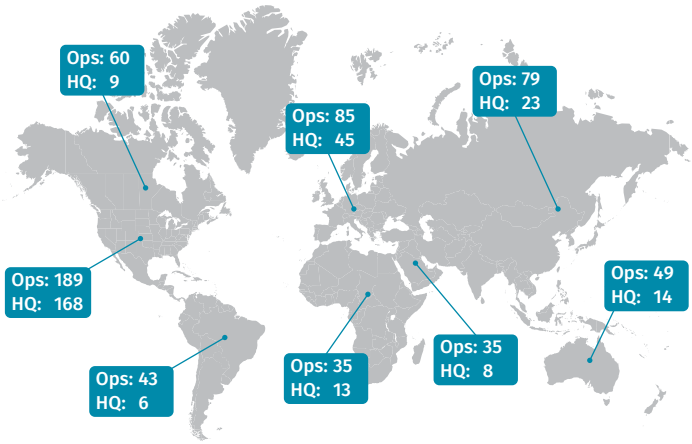
Each gear represents 10 respondents.

Organizational Size

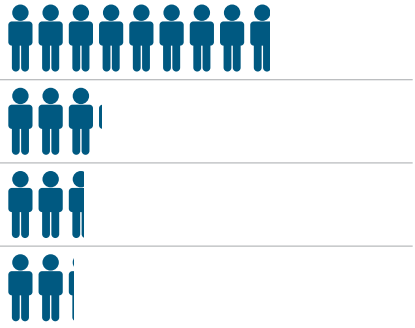


Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 10 respondents.

Figure 1. Demographics of Survey Respondents

The Impact of COVID-19

A significant majority of respondents (73%) report that they currently perform threat hunting, with another 27% indicating that they don't currently perform threat hunting but would like to within the next 12 months. With 286 respondents contributing to this survey, we find it encouraging that so many currently perform threat hunting in the face of pandemic-related disruptions.

However, looking back at the 2020 survey results, we see a decrease in this year's survey in the number of organizations that currently perform threat hunting. The 2020 survey showed that 85% of respondents actively performed threat hunting (and so a 12% decrease in 2021). Going back to 2019, we found that 79% of respondents then performed threat hunting.

Why do we see such a significant decrease in the past two years? The decrease might result from a slight rewording of the associated question in 2021. This year, we specifically asked respondents to indicate if they currently perform any type of threat hunting within their organization, whereas in the two years prior we had asked respondents to indicate whether they performed threat hunting and, more specifically, who performed it (internal staff or third-party contractors). In previous years, the number of organizations that outsourced threat hunting was in the single digits, so the overall drop of 12% for this year may result from a combination of organizations reducing their external spend with third parties and potentially refocusing on their internal staff so as to reduce their overall internal staff in response to the COVID-19 pandemic.

Given the impact the pandemic has had on organizations, we also wanted to understand what, if any, effect this may have had on an organization's threat hunting capabilities. We found that 11% of organizations did experience some impact on their threat hunting team or methodology in the past year, with a further 17% of organizations unsure whether the pandemic impacted them at all. With regard to impacted organizations, we see a fairly even split between organizations that reduced threat hunting versus those that focused more on cybersecurity and threat hunting as a result of the pandemic. A few respondents even report threat hunting moving from external third parties to in-house resources.

Reasons why organizations reduced their focus on threat hunting in the past year remain merely speculative. With 11% of organizations affected by the COVID-19 pandemic not exhibiting an entirely negative impact, the reduction concerns us, given the role threat hunting plays in helping organizations catch threat actors that they would normally not find through other automated means.

Threat Hunting Teams and Maturity Levels

This year we also sought to understand how organizations staff their threat hunting teams. In previous years, we did not ask this question directly. However, this year we wanted to understand whether an organization uses dedicated threat hunting staff (staff within the organization who have other roles) or simply outsources to third parties. We also allowed respondents to select multiple choices; after all, some organizations may have few staff dedicated to threat hunting but also draw on the resources of other departments as needed for larger or more long-term threat hunting. We found that 93% of respondents have in-house staff dedicated to threat hunting for their organization. Given the length of time and planning required to perform continuous threat hunting, we welcome this statistic. We found that 59% of organizations draw on resources from elsewhere in their organization and that 37% outsource to third parties. See Figure 2.

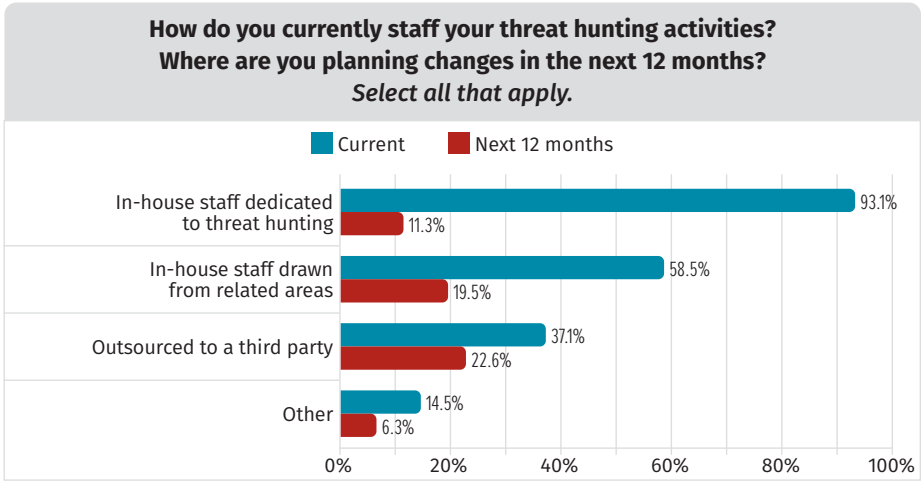


Figure 2. Threat Hunting Staff

Given that more than 90% of respondents indicate that their organizations have dedicated internal resources for threat hunting, along with just under 60% reporting that they use additional in-house staff to augment threat hunting, it seems that most organizations have at least one or more individuals managing threat hunting, with a large proportion of organizations using internal cross-functional staff to supplement their threat hunting missions. This seems a reasonable model, as it gives some consistency to the overall hunting strategy for the organization and enables them to surge resources when needed.

We sought to understand what mature organizations think of their threat hunting capabilities, based on a four-point scale ranging from Immature (very limited threat hunting capability and extremely manual processes) to Very Mature (hypothesis-based threat hunting). Most of our respondents (40%) sat within the Maturing category, closely followed by the Mature (25%) and Immature (21%) categories. Only 14% reported that they were Very Mature (i.e., using hypothesis-based threat hunting). See Figure 3.

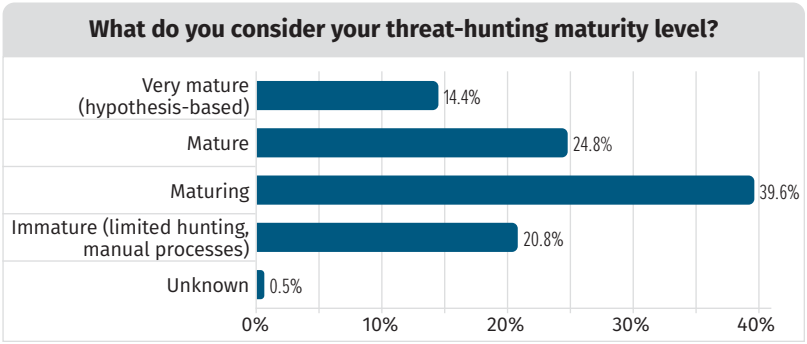


Figure 3. Threat Hunting Maturity Levels

We asked respondents to provide open-ended responses as to why they self-describe at any particular level. Availability of tooling to perform threat hunting ("Just starting to utilize threat hunting tools and capabilities") as well as a lack of automation with the tools they did have available ("We need better tooling, more automation") emerged as dominant challenges.

Given the evolving nature of threat hunting—a necessity because hunters must keep up with the changing tactics and techniques of threat actors—the majority of respondents categorize themselves in the Maturing category. Additionally, many respondents judge themselves harshly, assuming that prebuilt tooling may exist to cover all the tasks that they want to accomplish. In reality, organizations cannot fully automate threat hunting, and currently available tooling might not cover the types of hunting activities for which organizations need to perform data analysis. If tools were available for these activities, organizations would be wise to use them as part of a detection strategy (to catch threats as opposed to threat hunting). So, for all you threat hunters out there, remember this: Automated tooling won't catch that threat actor who has managed to evade detection.

What's in a Modern Threat Hunter's Toolbox?

The potential output of threat hunting depends on three important factors: visibility, skills, and threat intelligence. Visibility comes first. After all, without visibility, you can't bring intelligence or skills into action (no matter how good they might be). What's the point of knowing what an attack looks like when you can't check your whole environment for traces of an attack? To establish broad visibility, threat hunters need the right tools. For that reason, we looked into the toolboxes of today's threat hunters.

Unsurprisingly, 75% of respondents report that their leading tool sets include endpoint detection and response (EDR), SIEMs, and IDS/IPS. See Figure 4.

Interestingly, "Configurable, customizable, internally developed search tools (using scripts, PowerShell, WMI, etc.)" comes in second, at almost 66%. This second-place finish indicates that tool vendors can still improve with regard to threat hunting.

Third-party threat hunting platforms that deliver threat intelligence comprise the third category, at 61%. These tools support the third factor of threat hunting: threat intelligence. However, without visibility generated by other means, it remains dead knowledge.

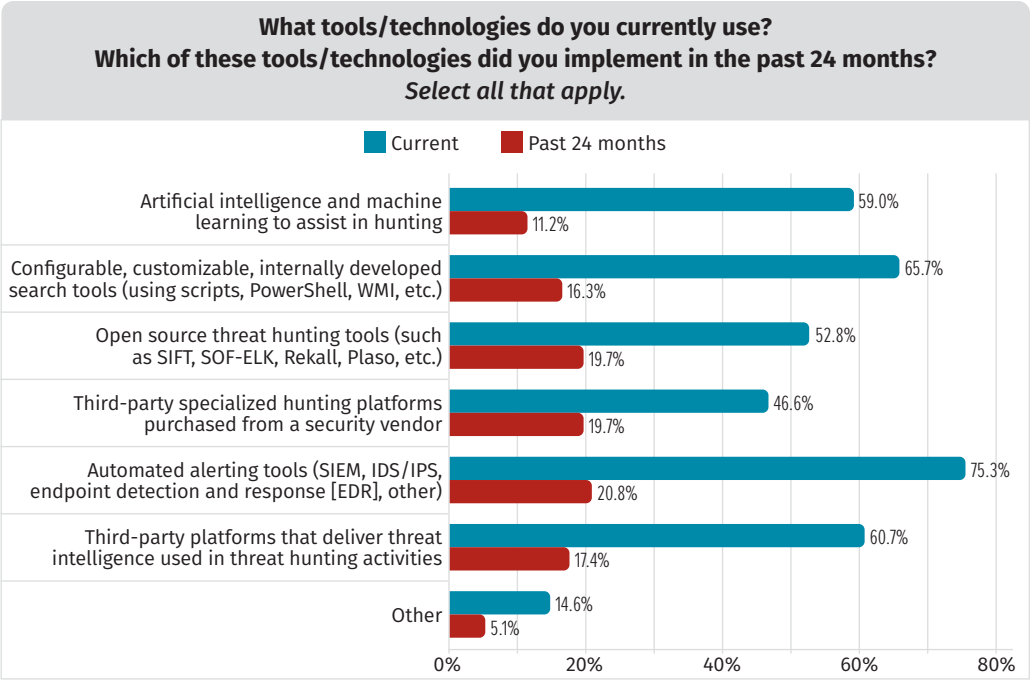


Figure 4. Tools/Technologies in Use and Planned

Approximately 60% of respondents use artificial intelligence (AI) and machine learning (ML) to assist in hunting. This trend appears to be new, compared to last year's survey.

With regard to the various tool categories, hunters give AI their highest single rate of satisfaction. Roughly a third of our respondents identified as Very Satisfied with this technology. Second place in the Very Satisfied category split between automated alerting tools such as SIEM/EDR/IPS/IDS and custom-made tools, each at 29%. See Table 1.

ADVICE

Although generally not a bad idea to use internally crafted tools for specialized hunting needs, these in-house tools still have costs associated with them. For instance, you need to ensure that the tools still work when key personnel who developed them leave the organization. As well, you must factor in the development of detailed documentation for homegrown solutions. Commercial tools might reduce the need for documentation to a degree.

Conversely, threat hunters don't appear too convinced of third-party platforms that deliver threat intelligence, with 13% of the respondents Not Very Satisfied with these tools.

This leads us to the threat intelligence provided by the sources or feeds that hunters use to augment their drills. Sixty-eight percent use threat feeds from a general security vendor, likely because vendor threat intelligence often comes for free with other security products

Table 1. Level of Satisfaction with Tools/Technologies

Tools/Technologies	Very Satisfied	Satisfied	Not Very Satisfied
Artificial intelligence and machine learning to assist in hunting	32.6%	22.7%	4.1%
Configurable, customizable, internally developed search tools (using scripts, PowerShell, WMI, etc.)	28.5%	31.4%	5.8%
Open source threat hunting tools (such as SIFT, SOF-ELK, Rekall, Plaso, etc.)	21.5%	29.7%	2.3%
Third-party specialized hunting platforms purchased from a security vendor	21.5%	20.9%	2.9%
Automated alerting tools (SIEM, IDS/IPS, endpoint detection and response [EDR], other)	28.5%	38.4%	9.9%
Third-party platforms that deliver threat intelligence used in threat hunting activities	22.1%	26.7%	12.8%
Other	8.7%	4.7%	0.0%

such as SIEMs and EDRs. However, almost 60% of our respondents claim that they use threat intelligence sourced from a dedicated threat intelligence vendor. See Figure 5.

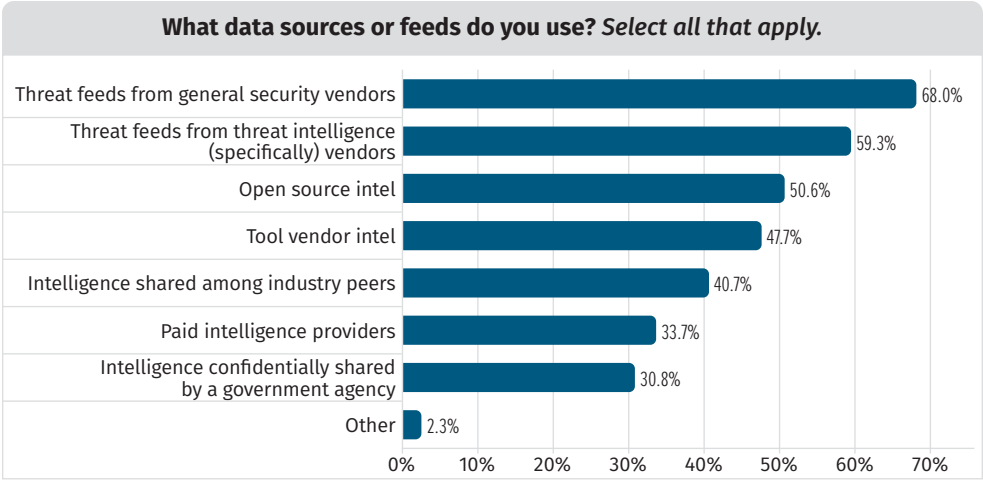


Figure 5. Threat Data Sources or Feeds

However, when looking at the satisfaction levels in Table 2, specialized threat intelligence vendors fare only slightly better than the general security vendors in the Very Satisfied category, with the general security vendors winning the race in the Satisfied category. Interestingly, intelligence shared by government agencies does not seem to satisfy threat hunters. Although 31% of our respondents use that kind of intelligence, only 12% describe themselves as Very Satisfied with the data.

To summarize, we see two notable trends:

- The most notable change this year is the rise of AI and ML in threat hunting. Because of this trend's relative newness, we cannot get good data about how well this approach works for now, but in next year's survey we will ask how it worked out and keep you posted.
- The high rate of custom-built tools shows that vendors can still improve their tools to better suit hunters' needs. It also means that organizations need to ensure that they retain the knowledge about custom-made tools and their application even after key employees leave the organization.

Table 2. Satisfaction with Data Source/Feeds

Data Source/Feeds	Very Satisfied	Satisfied	Not Very Satisfied
Threat feeds from general security vendors	22.8%	39.5%	6.0%
Threat feeds from threat intelligence (specifically) vendors	23.4%	31.7%	4.2%
Tool vendor intel	12.6%	28.7%	6.0%
Open source intel	13.2%	31.1%	4.8%
Paid intelligence providers	12.6%	17.4%	2.4%
Intelligence confidentially shared by a government agency	9.6%	15.6%	6.0%
Intelligence shared among industry peers	12.0%	24.6%	3.6%
Other	0.6%	0.0%	0.0%

How Beneficial Is Threating Hunting—and How Can It Be Improved?

Organizations need to understand the effectiveness or usefulness of threat hunting to their overall security, especially as an indicator of improvement or maturity for an organization. This year respondents report that the overall improvement in their organizations' security postures ranged somewhere between 10% and 25%, roughly where it has sat for the past two years.

Looking at the yearly trends since 2019, it appears that organizations improve their security posture by approximately 25% as a result of performing threat hunting. Overall, this brilliant result highlights the positive impact that threat hunting can have on organizations. Even considering some of the challenges that organizations have with threat hunting, as shown in statistics earlier in this report, the overall increase and benefits remain undeniable.

More than 60% of respondents formally measure the impact that threat hunting has on their overall security posture, along with a quarter not performing any type of measurement, and 14.9% report as unsure whether their organization performs any type of overall benefit analysis. Slightly more than half perform some type of measuring, but you want to remember that measuring the benefit of threat hunting entails significant effort.

For organizations that formally assess the benefit to their security program from threat hunting, 51% unfortunately still manually track their threat hunting activities and outcomes, whereas 45% of respondents perform more automated, or structured, tracking of their threat hunting activities and outcomes. See Figure 6.

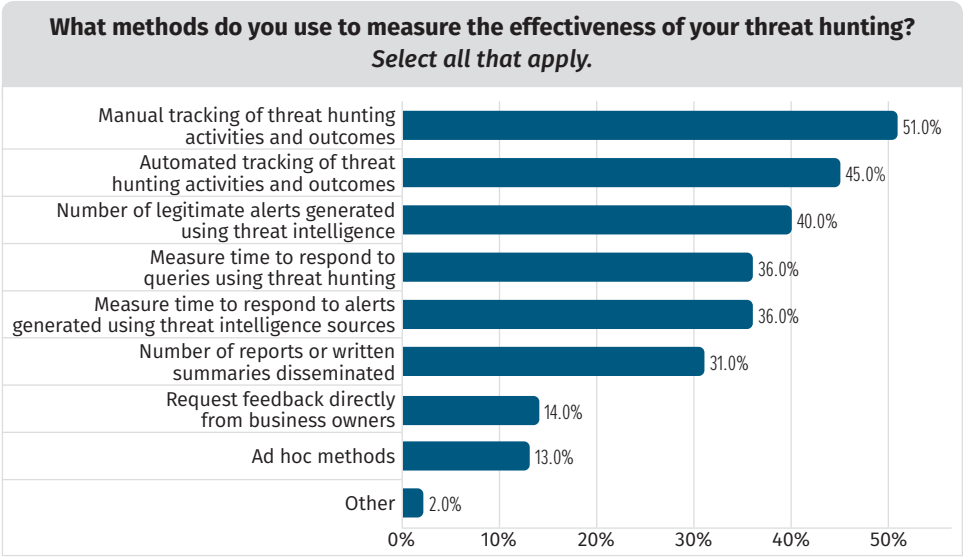


Figure 6. Methods to Measure Effectiveness

Most still use manual tracking, but even that wins against organizations that do not track outcomes at all. Based on 2021 results, a gap clearly exists in how organizations show benefit to their overall security posture.

It is also worth noting that the 28% of organizations observed either no impact (none) or a negative impact on their overall security posture as a result of threat hunting. It should also be noted that 27% of respondents also report that they haven't performed any threat hunting but look to do so in the next 12 months. We would err by excluding these results from the overall report, even though we likely see them because organizations had yet to start threat hunting at the time they responded to this survey.

For organizations that did see some type of improvement due to threat hunting, where did that improvement lie? Significant improvement in the creation of more accurate detections and fewer false positives, at 43%, stands out. See Figure 7.

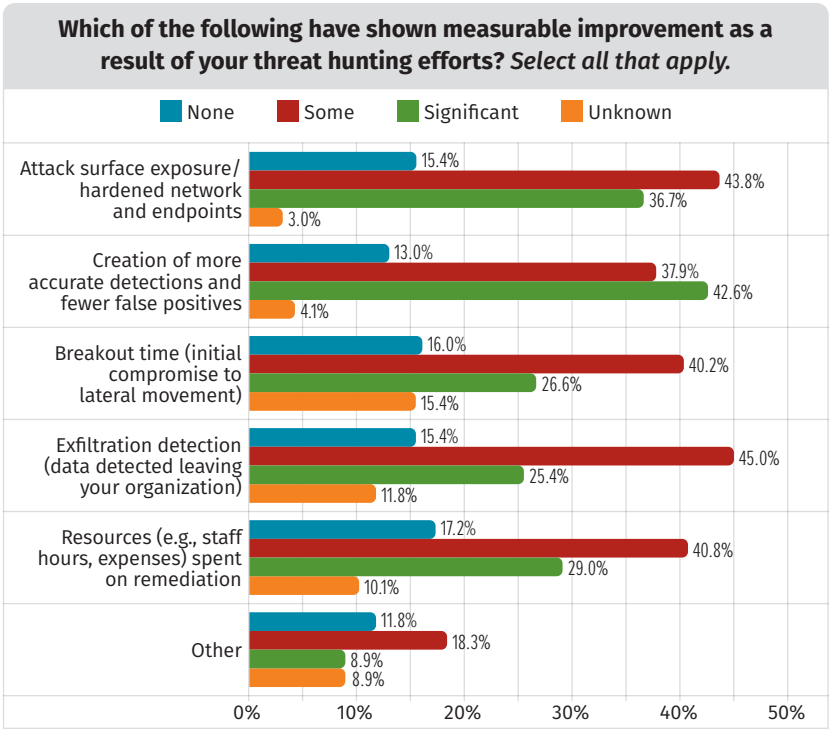


Figure 7. Areas of Improvement

This makes sense, because threat hunters should hunt areas of their environment where they have no detections and, when possible post-hunt, turn what they uncover into ongoing detections for the rest of the organization. This trend also continues from the 2020 survey results, where 28% of respondents observed significant improvement in the same area, along with 36% of respondents who noted the same trend in 2019.

We see this interesting trend in the same strongest category over the past three years. Therefore, perhaps attaining more accurate detections and fewer false positives really does require employing a strong threat hunting team within an organization.

Note two other interesting results here, related to organizations observing measurable improvement: a reduction of exposure to their organization's attack surface, with 37% observing a significant improvement, and a reduction in the hours spent on remediation, with 29% of respondents seeing a significant gain in this area.

Barriers to Success

More than half (51%) of respondents report that lack of skilled staff and lack of training to raise the skill levels of staff remains the primary barrier to success of their current or planned efforts to implement threat hunting. Following closely, at 43% each, organizations report two other challenges: limitations to tools/technologies and a lack of defined processes. See Figure 8.

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

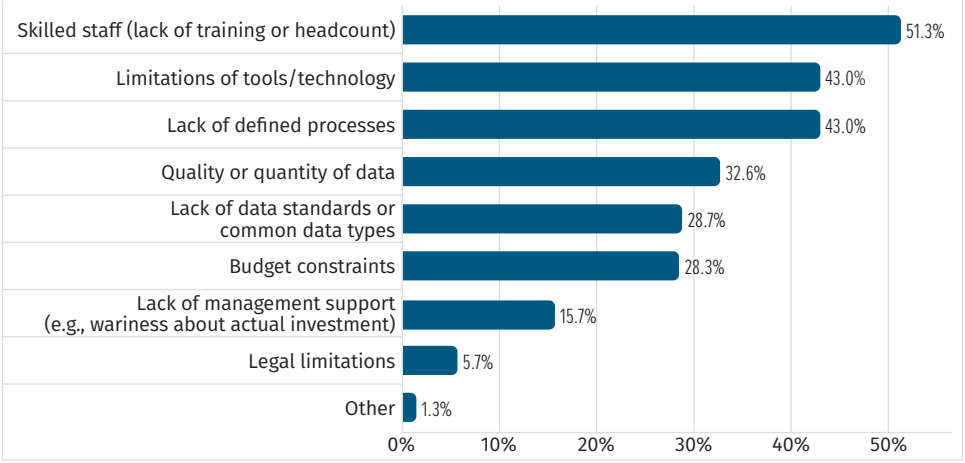


Figure 8. Barriers to Threat Hunting Success

With regard to challenges threat hunters face, the issue that appears most clearly prevalent, and that also underlies a number of the other issues identified, is the challenge of finding skilled staff and the ability to train current staff. Having skilled staff allows an organization to better select tools and technology, and to better define processes required to perform threat hunting (and even potentially influence how data is structured and collected). Without skilled and knowledgeable staff, threat hunters face significantly greater challenges when attempting to find overall efficiency or to improve their hunting efforts.

Understanding the barriers represents only part of the equation for improvement. Figure 9 shows the specific improvements organizations need to make with regard to their threat hunting capabilities.

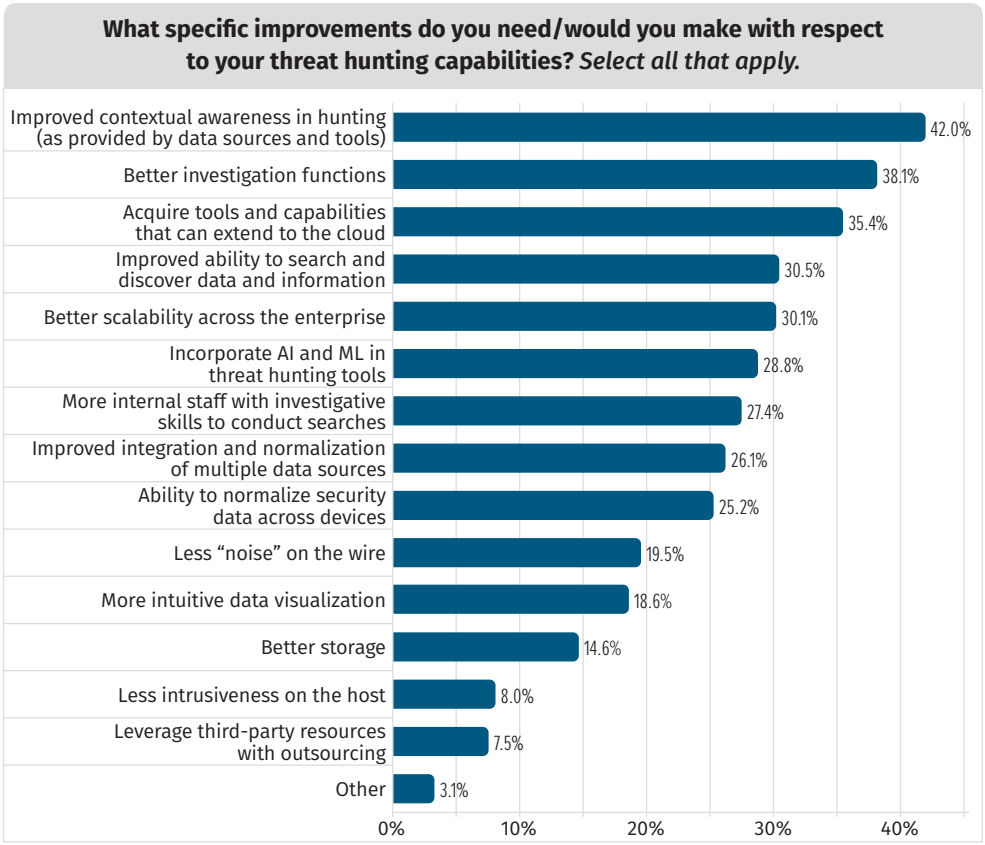


Figure 9. Specific Threat Hunting Improvements Needed

Three improvements stand out:

- **Improved contextual awareness related to data provided back by tools used for threat hunting.** Being able to contextualize data that we use for threat hunting proves extremely important. It can tell us the difference between legitimate activity within a network and suspicious activity that requires further hunting.
- **Ability to have better investigation functionality.** Both this and the first item essentially provide the visibility that enables threat hunters to successfully complete hunt missions. Unsurprisingly, therefore, these come out as the two most requested capabilities to improve the overall efficiency for our threat hunters.
- **Acquire tools and capabilities that can extend to the cloud, underscoring the need of organizations to extend visibility with the current tools into cloud-based services.** As more organizations move toward the cloud with their storage and compute workloads, it makes sense that threat hunters see this as a significant visibility gap when it comes to successfully and efficiently hunting for unknown threats. The challenges involved with performing investigations, and also hunting within cloud by services, featured in our top two improvement requests from 2020's survey as well. Clearly, we need to understand this as an ongoing challenge threat hunters face inside an organization.

What Do Today's Threat Hunting Teams Look Like?

We want to understand how threat hunting has worked historically within organizations, especially when compared to other IT security department initiatives. After all, the question of how to justify the expenses for an effective threat hunting team demands an answer.

To justify the costs, an organization must define the desired output and clearly identify a set of requirements, ultimately leading to a well-defined plan to introduce, maintain, and improve threat hunting.

Almost 40% of the respondents report that they document threat hunting requirements, and 34% at least record requirements ad hoc. So, in reality, only a quarter of the respondents fly blind when it comes to threat hunting requirements.

However, defining the requirements represents only half the game. Organizations constantly need to adapt to new threat landscapes. So, organizations take just their first step by defining requirements. Threat hunting adds the most value when organizations continuously monitor its effectiveness, with outcomes fed back into the requirements process—what almost 70% of our respondents do. This response tells us that, broadly speaking, threat hunting has become a standard business process for many organizations. See Figure 10.

Do you use these requirements to evaluate the effectiveness of your threat hunting operations over time and assess the need for additional resources?

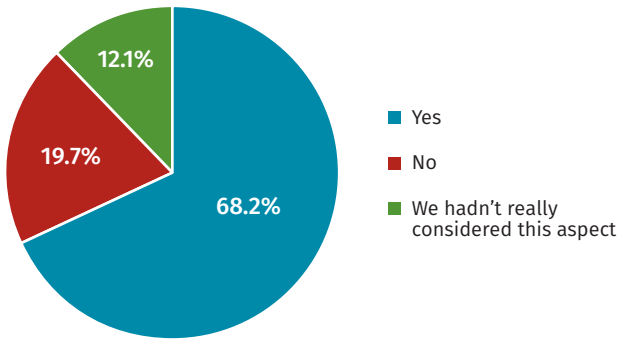


Figure 10. Requirements Feedback

To get a more in-depth view of threat hunting requirements in our respondents' organizations, we asked for some real-life examples.

The most common response defined uncovering visibility gaps (often a quick win in threat hunting) as one threat hunting goal. When conducting hypothesis-based threat hunting operations, we have three potential outcomes: accept the hypothesis (which entails a compromise), reject the hypothesis, or realize that we could not check the hypothesis due to visibility gaps. Usually, these visibility gaps also affect the organizations' detection capabilities. Identification of visibility gaps can significantly positively impact the security posture of an organization. Additionally, organizations can easily measure this objective.

Environmental and Economic Impacts in 2021

We live in difficult times. The number of criminally motivated attacks has increased in the past few years, but the breaches really spiked in 2020 and 2021. Ransomware has become an everyday subject for most CISOs. Few organizations have never experienced a breach. A breach's impact strongly depends on dwell time—the time between the first breach of the network and detection. At this point, ransomware attacks have hit most organizations already, but many of those organizations killed the attack at patient zero. Most organizations knew about and could prepare for the well-known ransomware trend, but other impact factors arrived less expected, yet with great power.

COVID-19 significantly and non-technically impacted IT security. The pandemic itself, and particularly the diverse global political reactions to it, affected many aspects of IT security. On the technical side, much of the workforce started working from home. Organizations had note laid out security plans for that new reality, leading to additional gaps in the protection of IT assets and an increase in the detection of breaches. During these times, financial constraints also impacted security in many organizations. Some organizations benefited quite substantially from the pandemic, whereas others struggled to survive; for these latter organizations, the pandemic impacted investments in security.

More than half (51%) of respondents said that the current situation did not impact their implementation of threat hunting, while 34% acknowledged a change, and 15% didn't know. Figure 11 shows how threat hunting changed for those who observed a change in their implementation.

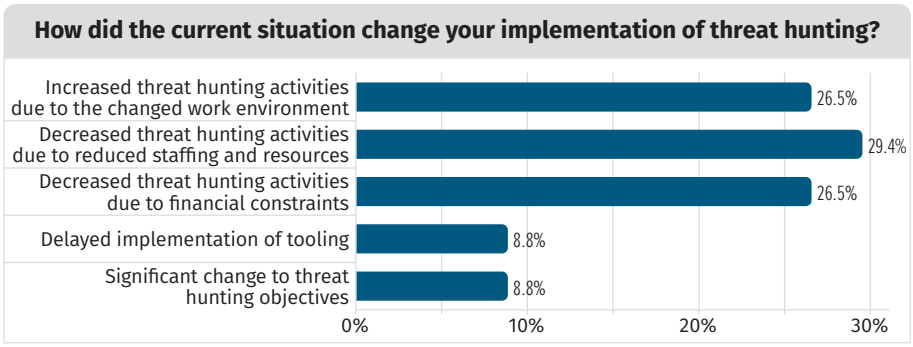


Figure 11. The Pandemic's Impact on Threat Hunting Implementations

We wanted to understand the impact on the implementation of threat hunting. On the one hand, financial constraints might reduce or stop threat hunting efforts. On the other hand, the increased risk might justify expanding threat hunting operations. These numbers indicate that more than half of our respondents cut back on threat hunting due to the current situation. So, while the risk increases, many organizations can't seem to afford to ramp up their threat hunting operations to compensate.

The general outlook for the next 24 months is more promising. Most of our respondents plan to increase spending on staffing and tools in the near future. See Figure 12.

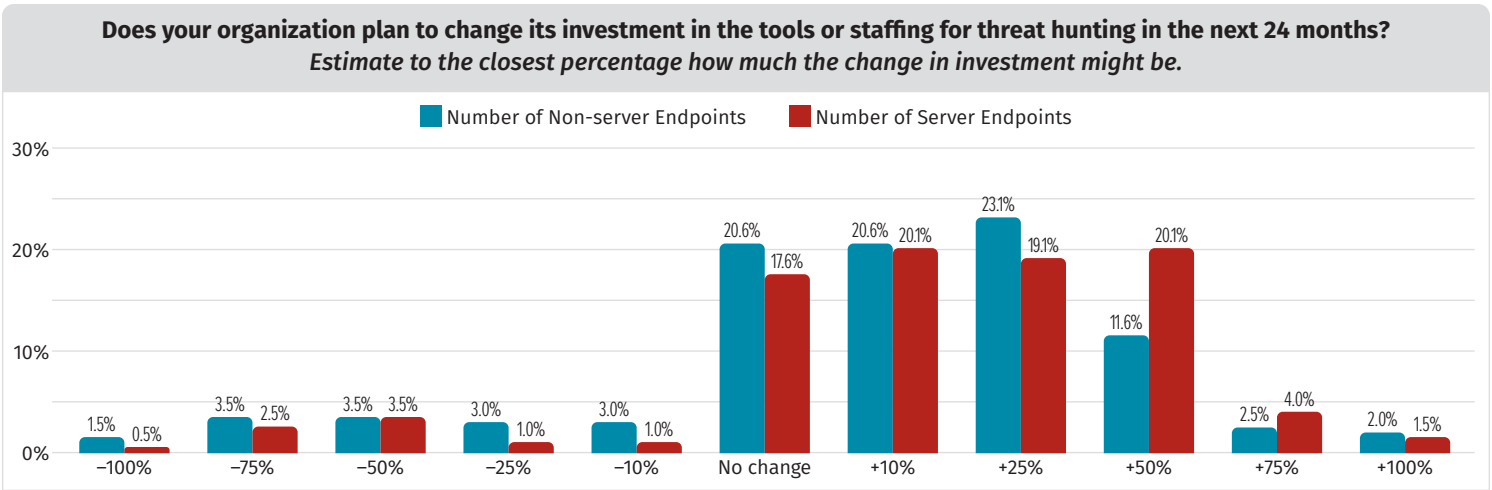


Figure 12. Spending Trends

Conclusion

Whether and how COVID-19 affected threat hunting in organizations was the most pressing question we sought to answer this year. Knowing from past surveys that threat hunting had not yet arrived in all organizations, we particularly wanted to learn whether the pandemic reversed the trend toward increased adoption of threat hunting.

Surprisingly, our data showed that many of our respondents observed an increase in threat hunting adoption despite the pandemic. Others experienced a decrease due to financial constraints. The overall outlook is good, though, as the general trend to more threat hunting appears to continue; most of our respondents have plans to increase spending on staffing and tools for threat hunting in the next 24 months.

Like in the previous years, organizations have primarily invested their tooling budgets into tools such as EDRs, SIEMS, and custom-made tools for threat hunting. Based on the data, how well organizations ensure the maintainability of their custom-made hunting tools remains unclear. However, we expect that we will not see a massive decrease in custom tools for threat hunting. So, organizations need to start thinking of taking real ownership of these tools, including documentation, education, and maintenance.

The fact that three-quarters of our respondents not only define threat hunting requirements but also measure its effectiveness supports this positive trend. This percentage means that many of our respondents have in place all the bits and pieces for a structured improvement process.

The organizations that measured the effectiveness of threat hunting over the past year saw a 10% to 25% improvement in their overall security posture compared to the previous 12 months. That represents a valuable counterweight to the increased risks COVID-related changes brought to peoples' workplaces.

All in all, we saw some standstill in the data (as expected). The outlook for threat hunting remains positive, however, and we already wonder what numbers we will see next year.

About the Authors

Mathias Fuchs, a certified instructor for SANS FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting, is head of Investigation and Intelligence at InfoGuard AG, where he is actively engaged in building the incident response (IR) practice. In that role, he uses his knowledge to shape his team; develop the necessary forensic, IR, and threat hunting capabilities; and proactively mediate security vulnerabilities that would be more difficult to manage later. Prior to joining InfoGuard, Mathias was a principal consultant at Mandiant, where he led large-scale cybersecurity investigations. He also was the lead security architect at T-Systems and a security consultant for international clients in a variety of industries.

Josh Lemon is a co-author for the SANS FOR509: Enterprise Cloud Forensics and Incident Response course and a certified instructor for SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and SANS FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is a managing director at Ankura, leading their APAC Digital Forensics and Incident Response practice in APAC, where he assists government and commercial clients with combatting sophisticated compromises, maturing their cyber defense and response programs, and threat hunting for malicious adversaries. Previously, he worked as a director at Salesforce.com in their international Salesforce Security Response Centre (SSRC), where he headed up the team responsible for looking at new cutting-edge ways to approach incident response at scale.

Sponsor

SANS would like to thank this paper's sponsor:

DOMAINTOOLS®