

Survey

SANS 2024 Threat Hunting Survey: Hunting for Normal Within Chaos

Written by [Mathias Fuchs](#) and [Josh Lemon](#)

March 2024

Executive Summary/Introduction

This is SANS's ninth year of conducting our annual 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 challenges they may face and how they may adapt in the year to come. As authors who also work in the field of threat hunting and incident response, we try to take the raw data from respondents and interpret it as best as possible while providing a little color and guidance for others in the field still trying to mature their threat hunting methodologies.

This year, we kept some of our longer-running key questions so we could better see trend information across multiple years, while also adding a few new questions about how threat hunters source information to shape what they go hunting for. As we analyzed the state of threat hunting within organizations in 2024, it became clear that these skills have become central to an organization's cybersecurity strategy. The survey revealed that half of the organizations now have formally defined threat hunting methodologies, which is a notable increase from the 35% reported in the previous year. This indicates a maturity in the industry and a push toward standardized processes for better threat detection and incident response. However, this progress is not without its challenges; the lack of skilled staff, although reduced from 73% in 2023 to 50% in 2024, remains the top barrier, followed by data quality issues and tool limitations.

The survey also highlighted a shift in how organizations stay updated with the newest attacker techniques. Vendor blogs and papers (59%) and independent blogs (59%) are the primary sources, with commercial intelligence providers also playing a significant role (55%). Interestingly, 50% of respondents stated that their organization conducted its "own research," underscoring the importance that threat hunters currently put on performing independent threat intelligence for their specific organizational needs. This emphasis on diverse intelligence sources demonstrates a comprehensive approach to maintaining a current threat landscape perspective.

Despite the strides in methodology adoption, a concerning trend is the increase in organizations outsourcing their threat hunting—37% in 2024. Outsourcing can introduce challenges, such as a potential disconnect between the organization's unique systems and the nuanced threat landscape, along with risks in data governance and continuity in a cybersecurity strategy. Organizations that outsource increasingly allow third-party providers to determine the hunting ground and outcomes (34% in 2024), raising concerns about the efficacy and alignment of outsourced threat hunting with the organization's goals.

On a positive note, there is an increase in organizations measuring the success and effectiveness of their threat hunting efforts, up from 34% in 2023 to 64% in 2024. This indicates a recognition of the value of metrics in guiding and improving threat hunting practices, along with showing value back to the broader organization. However, the effectiveness varies, with 62% reporting measurable improvements in their security posture and 23% reporting a negative impact, highlighting the need for effective implementation strategies.

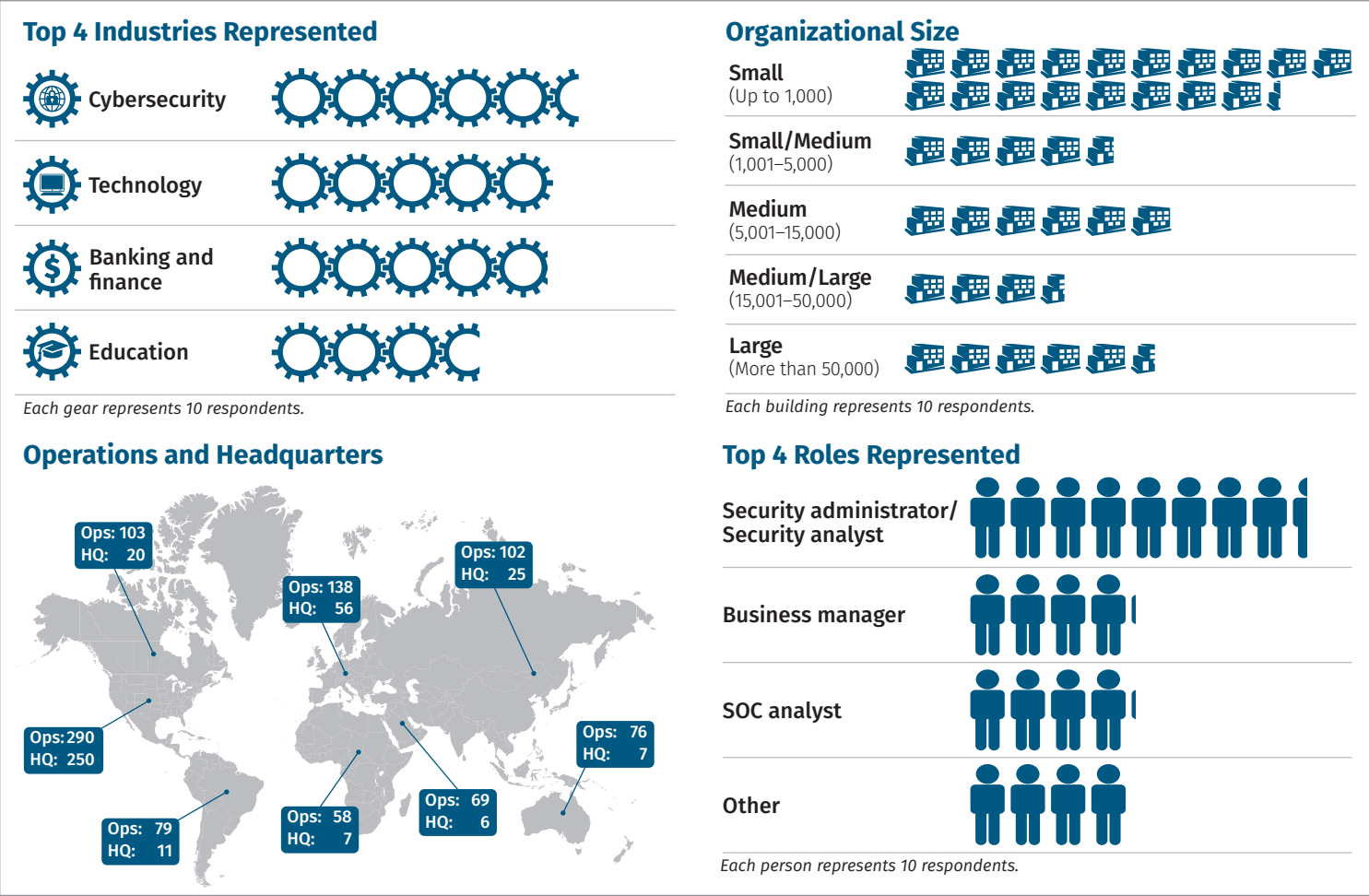
The 2024 survey presents a cybersecurity landscape that increasingly recognizes the importance of threat hunting, both in-house and outsourced, and is actively working toward overcoming the barriers to its success. The commitment to regularly reviewing and updating threat hunting methodologies reflects a dedication to keeping pace with the dynamic nature of cyber threats. As organizations continue to evolve their threat hunting capabilities, they are likely to see further alignment of their cybersecurity efforts and strategic objectives, while also defending against or uncovering new threat actors.

Lastly, we have gathered data on the impact of threat hunting to gauge its success in bolstering organizational defenses. The findings underscore the critical role of threat hunting in equipping organizations to combat threat actors. Detailed analysis of these outcomes is presented in the report; for now, let us highlight a few additional insights from the SANS 2024 Threat Hunting Survey:

- Business email compromise (BEC) threat actors are currently the most common threat actors caught by threat hunting (discovered by 68% of those surveyed).
- Organizations now review/change their threat hunting methodologies as follows:
 - Whenever needed (35%)
 - Monthly (26%)
 - Quarterly (20%)
 - Annually (11%)
- Outsourced threat hunting is utilized by 37% of organizations.
- More than half of the organizations (51%) have adopted clearly defined methodologies for threat hunting in 2024, signifying a significant evolution in organizational practices compared to previous years.
- About 64% of organizations formally measure the success or effectiveness of their threat hunting efforts.
 - There is a marked decrease in organizations with no plans to formalize methodologies, from 7% down to 2% in 2024.
- Available human resources have begun to influence the selection of threat hunting methodologies more heavily, with 47% of organizations acknowledging this trend in 2024.
- The chief information security officer (CISO) is a primary contributor to threat hunting methodology development, with significant involvement at 40%.

- Significant improvements as a result of threat hunting efforts were observed in:
 - Attack surface exposure/hardened network and endpoints (49%)
 - Creation of more accurate detections and fewer false positives (49%)
 - Resources spent on remediation (39%)
- About 30% of respondents use vendor information as a fallback for their threat intelligence, while 14% rely entirely on vendor threat intelligence.
- Incident response teams increased their contributions to developing threat hunting methodologies to 33% in 2024, up from 30% in 2023, suggesting a greater integration of threat hunting within broader security functions.
- Concerns about the quality or quantity of data have risen from 34% to 44%, and issues regarding the lack of data standards or common data types have increased from 26% to 33%, highlighting the challenges of managing and leveraging a growing flood of cybersecurity data.

Figure 1 provides a snapshot of the demographics for the respondents to the 2024 survey.



Participants/Demographics

This year we were again looking at a broad spread of industries (Figure 2). Cybersecurity leads at 15%. It's good to see that 9% of our respondents are working in manufacturing organizations. They are one of the areas that have been hit very hard by ransomware attacks in the past few years.

From a size perspective (Figure 3), the survey covers organizations from less than 100 employees (24%) up to more than 100,000 employees (9%)

Threat hunting is a multidisciplinary operation. We clearly need people who know how to hunt, people who can plan the hunts, and intelligence analysts that feed sound intel into the operation. On the other hand, we have the more business-focused side that needs to understand and support threat hunting. This is reflected in the roles our respondents have.

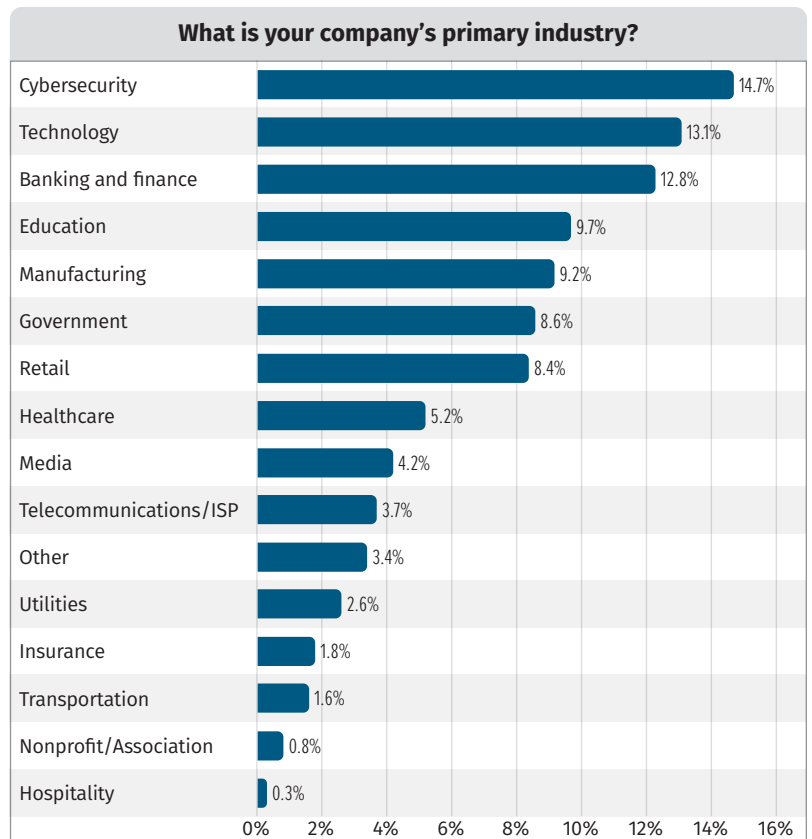


Figure 2. Respondents' Primary Industry

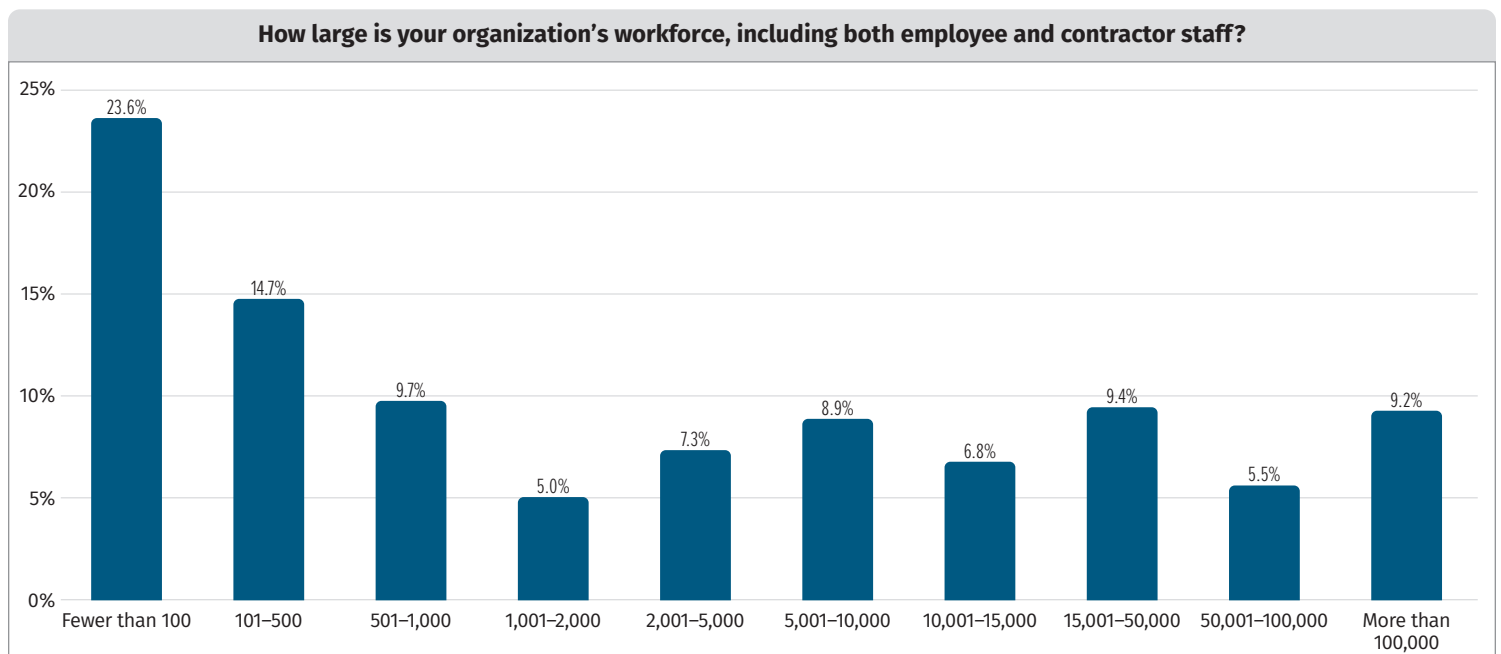


Figure 3. Respondents' Organization Size

Twenty-two percent of our respondents are security administrators or analysts. However, at number two we see 11% who represent the role of business managers. This mix allows us to address not only technical but also financial and personnel topics in our survey.

One fact that does skew the results a bit is the geographical profile of our respondents (Figure 4). Sixty-five percent of our respondents work for organizations headquartered in the United States. Although that might impact staffing and organizational topics, we don't believe that this impacts how threat hunting is done technically.

How We Hunt and What We Find

The variety of cyber threats is large and seems to get larger every year. As a result, in this year's survey we wanted to know what threat hunting teams hunt for and what they find. As the maturity level of threat hunters keeps increasing, most threat hunting operations today are a form of intelligence-based hunting—it may be simply looking for curated indicators of compromise (IOCs) or full-blown hypothesis-based hunts.

Keep in mind that the way threat hunters hunt will impact what they find. So, the numbers we see in our survey results will never be a perfect representation of the current threat landscape. That is also true because ransomware actors or criminals that conduct business email compromise are usually easier to detect than highly funded nation-state attackers.

We asked what attackers our respondents are facing in their threat hunting operations. Surprisingly, ransomware attacks were not number one this year. At almost 68%, business email compromise (BEC) is the number-one attack type that threat hunters detect these days, followed by ransomware at 64% (Figure 5).

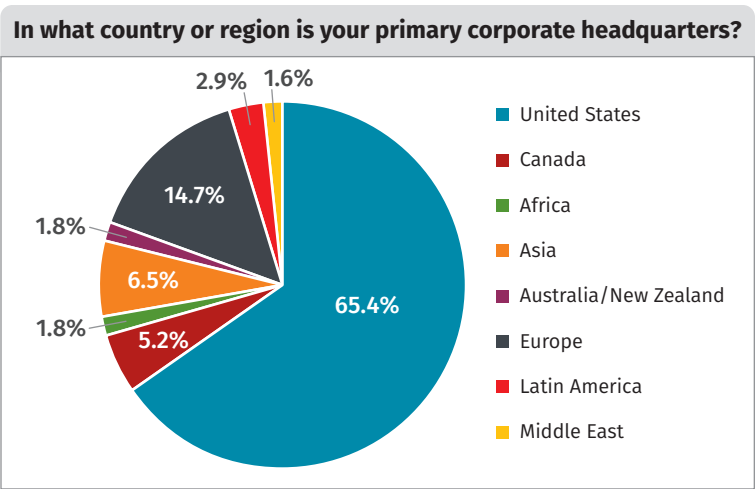


Figure 4. Respondents' Corporate Headquarters

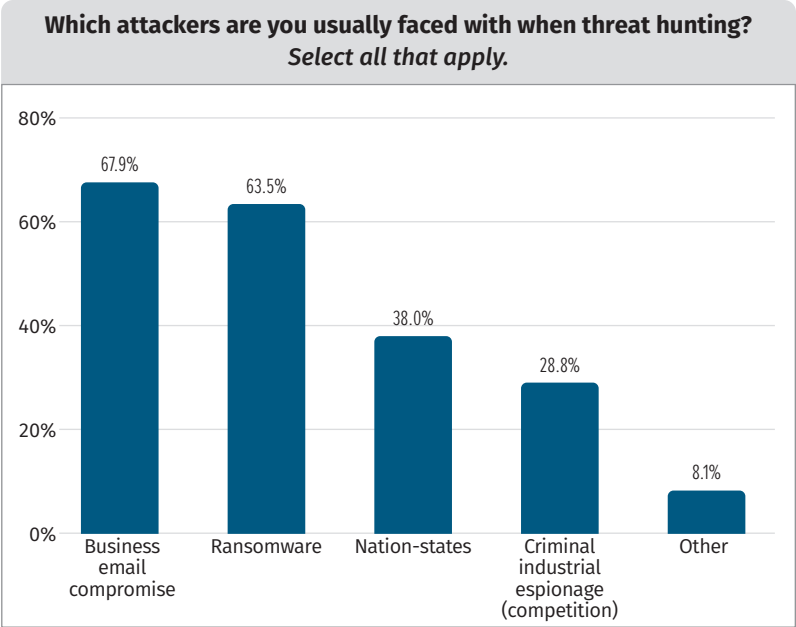


Figure 5. Most Common Types of Attackers

Although ransomware attacks are similar across the board, BEC comes in various forms and has been on the rise in the past few years. Attackers take over email accounts of legitimate employees within target companies and use a variety of social engineering tactics to get victims to transfer money to the attackers' accounts. One common tactic is to mimic an executive of the target company and pressure an employee with access to company bank accounts to transfer money for a super-secret and urgent project. Another quite common approach is for the attacker to intercept emails between the target company and its business customers. The attackers convince the target's customers to transfer money owed to the attacker's account rather than to the target's account. Usually, they give reasons like an ongoing audit in one country that would prevent them from receiving the amount due to that country's bank account.

To facilitate these tactics, attackers need to have access to one or more mailboxes within the target company. That usually happens by phishing or credential theft. Even though this type of attack is not limited to cloud-based email services, we see it happening most often in these setups. That might be because more companies have moved their communication and collaboration solutions into the cloud. The advantage of this for the threat hunters is that hunting for BEC in most relevant cloud infrastructures is very well documented and very clearly scoped. Although hunting for attackers in an enterprise infrastructure with thousands of computers and hundreds of services with tons of log sources and other evidence is something that you can never cover 100%, hunters might be able to apply the BEC detection tactics and leverage all the available logs that the cloud provider offers.

Let us add one side note when comparing ransomware and BEC concerning the money flow in these two cybercrime categories: Fairly often it is claimed that ransomware schemes only work because cryptocurrencies exist and make the money transfer to criminals possible. If that were true, BEC would not exist because it uses real-world bank accounts for the transfers. So, in this attack field, the responsibility does not fully lie in the laps of cybersecurity specialists; it also is the responsibility of the banks that facilitate these wrongful payments to the attackers' bank accounts.

Tactics, Techniques, and Procedures (TTPs) for the Attack Schema

In the survey, we looked deeper into the TTPs for some of the most hunted attack schemas. We didn't ask for BEC in particular, because the responses for this category would not show much variation. BEC does not usually require large-scale access to the victim's infrastructure, which significantly reduces the interaction with the victim's infrastructure. Locard's exchange principle tells us that a perpetrator will always bring something into a crime scene and leave with something from the crime scene. However, the less time someone spends at the crime scene and the less parts of the crime scene someone touches, the less exchange of evidence will occur.

Ransomware attacks, on the other hand, are very intrusive, and attackers usually leave a noticeably clear trail of evidence when they pivot through the network. The number-one TTP reported by our respondents for this hunted attack scenario is “custom malware” (see Figure 6). This is not a surprise because the ransomware executable is usually, with very few exceptions, a custom-made binary. Looking for that TTP is not especially useful for proactive threat hunting because the encryption binary will only be dropped in the final stages of a ransomware attack and swiftly executed.

Another common TTP for ransomware actors is targeted exfiltration, which is second for this attack scenario according to our respondents. It might not be as targeted as exfiltration in nation-state attacks because ransomware attackers usually operate on a tight schedule, but ransomware groups have clear preferences as to which kinds of data they try to locate and exfiltrate. Incident responders frequently find traces that indicate what ransomware attackers looked for in the network.

The number three TTP, according to 54% of our respondents, is off-the-shelf tools like Cobalt Strike or Brute Ratel. This also includes legitimate remote access solutions like Anydesk.

To 27%, “deleting traces” is nothing that most ransomware actors do very successfully. We do see them trying to purge their traces, however, which quite frequently results in their leaving even more traces or tipping off the SOC that an attack is ongoing.

What we found interesting is that 18% of respondents see “physical access” being used in ransomware attacks. Please contact us if you are aware of cases where the attackers physically intruded into the target company in ransomware cases.

Next, we investigated the TTPs our respondents saw in nation-state cases. Clearly, the leading TTP is “living off the land” at 76% (Figure 7). Whenever an attacker plants malware on a device or pivots to a device using malware, there is a very real chance of their being detected. Using legitimate tools that already exist in a company is a good way to remain undetected, but there are still several methods to detect an attack.

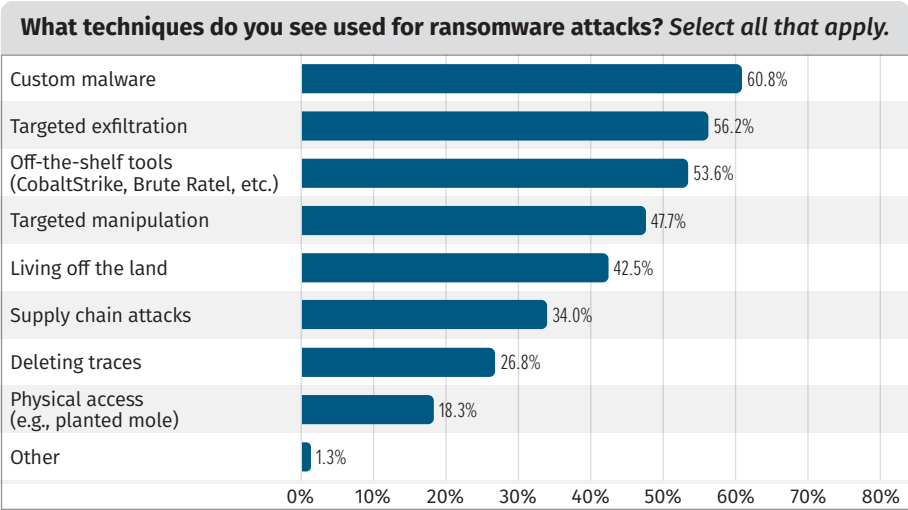


Figure 6. Ransomware Techniques

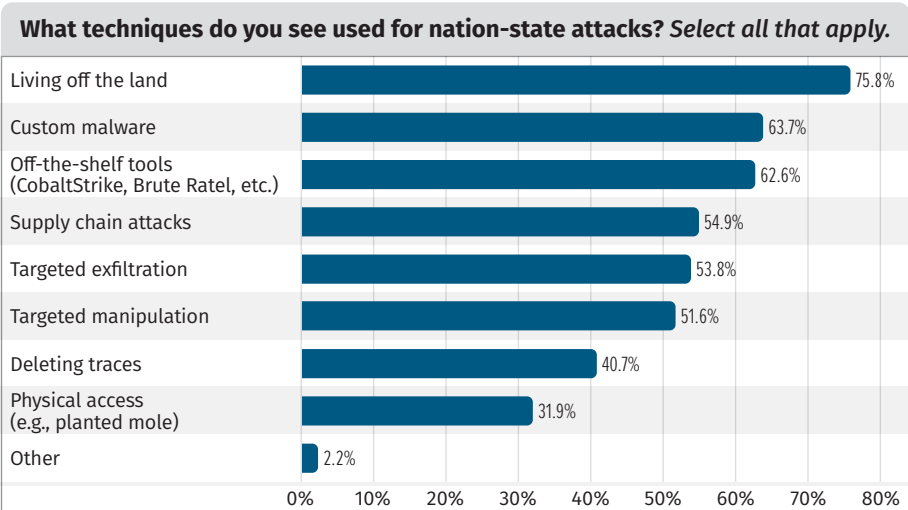


Figure 7. Nation-State Attacker Techniques

When nation-state attackers penetrate a network, they frequently use custom-made and often highly sophisticated malware. This is reflected in the survey results where 64% of our respondents have seen custom malware in nation-state attacks. Also, the number of physical access attempts, for instance in the form of a planted mole, is quite high at 32%. This does not come as a surprise because often the cheapest and easiest way to gather information from or gain access to a company is a human asset. Finally, we asked our respondents which TTPs they see in industrial espionage cases. These numbers might be a little skewed because nation-states are involved in industrial espionage as well. The distribution of TTPs is not entirely different than for the ransomware category; however, the category of physical access is higher at 30% versus the 18% in ransomware cases. This does not come as a surprise because industrial espionage cases have been human operations long before IT was introduced.

Charting the Shifting Sands of Cyber Threats

In the dynamic landscape of cyber threats, staying current with the latest attacker techniques is vital for effective threat hunting. This is the first year that we asked respondents how they stay up to date with the newest attacker techniques. Their responses suggest that the most favored sources for this information are vendor blogs and papers—slightly more than 59% of respondents rely on them (Figure 8). These platforms often provide timely insights and analysis from cybersecurity product and service providers, which can be instrumental in understanding new threats in the field.

Sources of Information

It’s unsurprising that vendor blogs and papers are the most used source of new attacker techniques, because they’re also often completely free to organizations. The challenge organizations may face from vendor blogs, however, is that the results may be painted with a brush stroke that can often make the vendor stand out better in the market or shed a better light on its “wares.” It is important for organizations to consume this material while fully understanding who wrote it and why. A great example of this is the report you’re currently reading: Although both authors were compensated for our time in analyzing the results and writing this report, the content is created independently of SANS or the sponsors. Hopefully, this continues to instill trust in this report and our analysis.

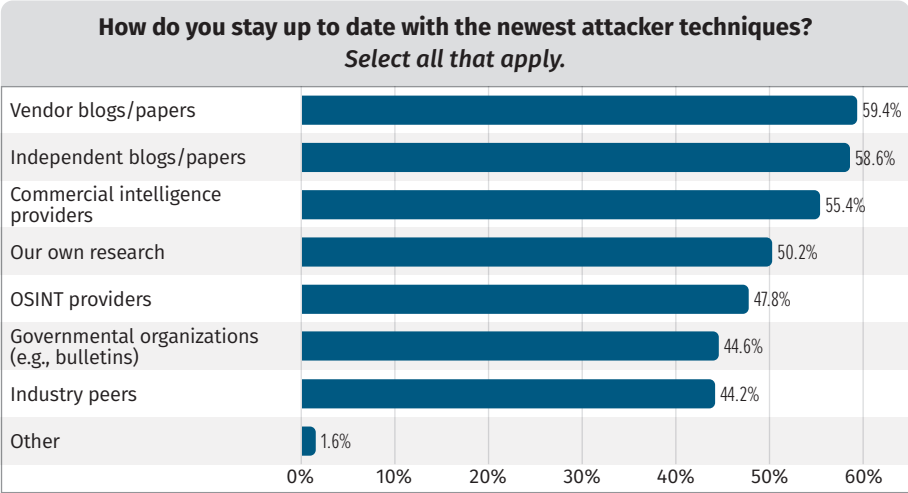


Figure 8. Sources for the Latest Attack Techniques

Closely following vendor blogs and papers are independent blogs and papers, preferred by slightly less than 59% of respondents. This preference indicates trust in the expertise of individuals and organizations outside of commercial entities, which can offer unaffiliated and possibly more diverse perspectives on emerging threats. These sources are often considered to be at the forefront of threat discussion, because they can move quickly to disseminate information without the constraints that might affect commercial providers.

Commercial intelligence providers are also a significant resource, with 55% of respondents utilizing them. These entities specialize in threat intelligence and often have the resources to provide extensive research and real-time data on threat actor techniques, making them valuable assets for organizations building their threat hunting capabilities.

Interestingly, “our own research” is cited by 50% of the respondents, highlighting that a significant number of organizations conduct in-house threat research but rely on it less than they rely on vendors and independent blogs. This self-reliance is crucial for contextualizing and understanding how generic threat information applies to their specific environments. It allows for tailored threat hunting that aligns with the organization’s unique risk profile and security posture. However, this is likely the costliest option because it requires staffing, time, skills/education, and resources to be successful.

Governmental organizations’ bulletins are utilized by 45% of respondents. This is a much more difficult statistic to analyze because we both know from personal experience in different countries that some government organizations can provide attacker information quite quickly, whereas others take much longer to declassify information and make it available to non-government organizations. Governments that can move quickly on this information can provide strategic insights and alerts about state-sponsored activities or high-impact cybercrime campaigns, which can be extremely beneficial to organizations for threat hunting.

Overall, the diverse range of sources reflects a multifaceted approach to threat intelligence gathering in cybersecurity. Given that the variance between how organizations find new attacker techniques in all the sources is only 15%, it shows that organizations are ensuring they use a multi-source approach for more robust and proactive threat hunting.

Structured Tracking of the Threat Landscape

Implementing a formal program to track changes in the threat landscape is essential to an organization's cybersecurity posture. When asked if organizations formally keep track of changes to the threat landscape, 61% of respondents affirm that their organizations have established such a program. This proactive stance enables continuous threat hunting and monitoring, which is crucial for the early detection of potential security threats and vulnerabilities.

On the other hand, the survey reflects a significant portion of respondents (29%) that do not have a formal program in place, along with another 10% that aren't sure. This gap exposes these organizations to hunting with outdated threat intelligence, potentially leading to delayed threat actor discovery and mitigation. The lack of a formal program might indicate resource constraints, a lack of awareness, or possibly an underestimation of the importance of continuous threat landscape monitoring.

Having a strategy for tracking changes to the threat landscape is only helpful if you have the ability and tooling to track those changes. We found that respondents indicated their dominant method for monitoring changes to the threat landscape is using open-source intelligence (OSINT) tools (70% of respondents). Most organizations likely favor OSINT tools due to their accessibility and the breadth of data they can scan, not to mention their low price tag. Additionally, OSINT tools are continuously improving, with the cybersecurity community continuing to publish or update new tools. Survey results suggest that the cybersecurity community places significant trust in the collective power of publicly available information to track changes to the threat landscape.

Commercial intelligence tools also play a pivotal role, with 61% of organizations utilizing them to track the threat landscape. These tools can offer more curated threat intelligence, with features tailored to organizational needs such as real-time alerts, in-depth analysis, and integration with existing SOAR or SIEM tools. They can provide a more targeted and refined set of data, making them an asset for organizations that require a more curated approach to threat intelligence.

Although internally built tools are used notably less often (33%), this may also reflect organizations that are further along with their maturity. Hopefully, organizations with their own internally built tools will have more automation to track threat landscape changes.

The Vendors' Threat Landscape

Reliance on endpoint detection and response (EDR) and extended detection and response (XDR) vendors is significant yet varied among organizations. We wanted to understand organizations' dependence on EDR/XDR vendors to track the threat landscape.

The majority of this year's respondents consume EDR and XDR vendors' threat intelligence. However, most use that information in combination with their own threat intelligence (47%), 14% depend on vendor-supplied intelligence completely, and another 30% use the information as a fallback to their own threat intelligence. The use of threat landscape information from an EDR vendor can be significantly useful given that EDR vendors often have a comprehensive view of the threat landscape through their customers that are using their products. It's vital for organizations to consider that although EDR vendors are likely to see a good cross-section of common threat actors, they may be less likely to see targeted threat actors for your organization. This is often where your own threat landscape intelligence becomes useful.

Are Hunters Using a Methodology or Being Given a Policy?

The statistics from 2023 and 2024 regarding the adoption of clearly defined methodologies for threat hunting demonstrate a significant evolution in organizational practices. In 2024, the data shows that more than half of the organizations (51%) report having formally defined threat hunting methodologies, marking a notable increase from 35% in the previous year (Figure 9). This growth reflects a maturing industry with an enhanced focus on establishing standardized processes to improve the effectiveness and efficiency of threat hunting activities. Formally defined methodologies can lead to better consistency in threat detection, faster incident response, and more effective allocation of resources, which are critical for maintaining robust cybersecurity defenses in an increasingly complex threat landscape.

Conversely, there is a slight decrease in organizations relying on ad hoc methodologies, from 38% in 2023 to 35% in 2024. This shift may indicate a trend toward more systematic threat hunting approaches as organizations recognize the benefits of structure and predictability over improvisation. Interestingly, the percentage of organizations planning to define their methodologies has decreased from 20% to 13%, possibly suggesting that many of those with intentions to formalize processes in 2023 have already done so. This premise is also supported by a marked decrease in organizations with no plans to formalize methodologies, from 7% in 2023 to 2% in 2024. This change could signal a broad acknowledgement of the necessity for formal methodologies in the continuous and increasingly complex battle against cyber threats. Overall, these trends underscore a proactive shift in the cybersecurity community toward institutionalizing threat hunting as a key defense strategy.

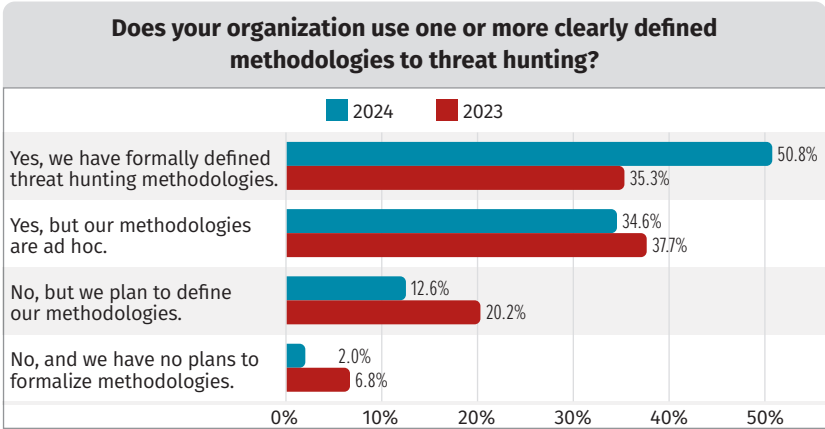


Figure 9. Use of Threat Hunting Methodologies

The responses from the last three years provide an insightful look into how organizations adapt their threat hunting methodologies over time. This year, the percentage of organizations that revise their threat hunting methodologies “whenever needed” has decreased to 35% from 45% in 2023 and 48% in 2022 (Figure 10). This positive trend might suggest that organizations are moving toward more regular and scheduled reviews of their

practices rather than ad hoc changes, which can help ensure a more disciplined and consistent approach to threat hunting. The increased frequency of reviews can be critical for keeping pace with the rapidly evolving nature of cyber threats, where new vulnerabilities and attack strategies emerge at a continually increasing pace.

A corresponding increase in monthly reviews seems to show where our “whenever needed” respondents have moved: This increase has more than quadrupled from 6% in 2023 to 26% in 2024. This leap indicates a shift toward more dynamic and responsive methodologies, potentially driven by the recognition that cyber threats are becoming more sophisticated and require frequent attention to ensure that threat hunting activities remain effective.

Quarterly reviews have also steadily increased over the years, aligning with the best practices of regular check-ins and updates to security processes. Interestingly, the number of respondents who are “unknown/unsure” about their review frequency has more than halved, dropping from 18% in 2023 to 7% in 2024, which may indicate better internal awareness and communication regarding threat hunting. Similarly, the percentage of organizations that never review or change their methodologies has decreased, suggesting a decline in complacency and an increased understanding that stagnation in threat hunting practices can lead to vulnerabilities within cybersecurity defenses.

Generally, a threat hunting methodology is designed to be flexible enough to be adapted to the ever-changing threat landscape. Although a threat hunting methodology should be used as a guide during hunting missions, it probably does not need to be updated monthly; monthly updates could be a sign that the methodology is not broad enough to cover the majority of hunt missions. For a mature organization, a quarterly review of the threat hunting methodology is a reasonable expectation—more often than this is probably a sign that organizations may need to go back to the drawing board and redraft the methodology to make it suitable for a longer period of time.

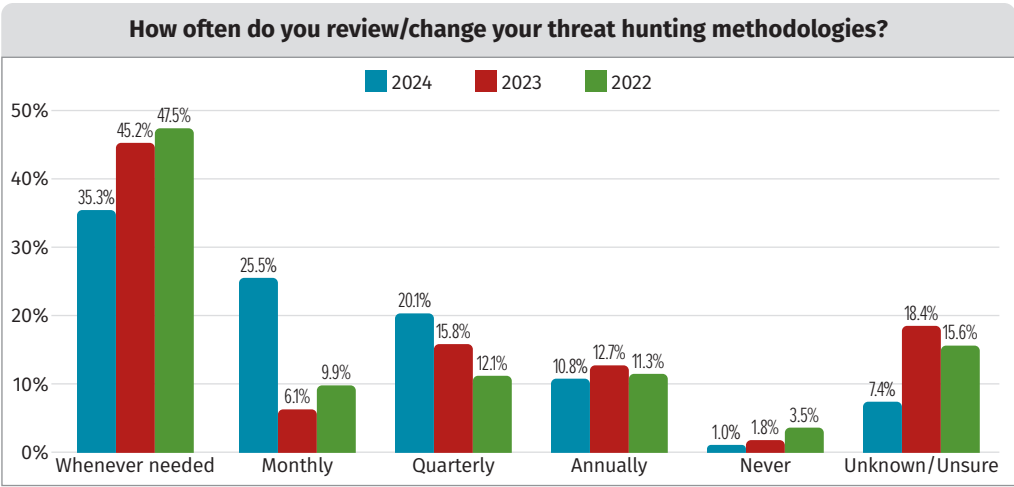


Figure 10. Frequency of Reviewing/Changing Methodologies

Building the Methodology

When asking respondents who contributes to their threat hunting methodology, the key contributors are notably diverse, indicating a multidisciplinary approach to shaping these critical procedures. The CISO emerges as the primary contributor with a significant 40% involvement. This level of contribution from the top echelons of cybersecurity governance may reflect a turning point in threat hunting, which is no longer merely a technical activity but a strategic one integral to the organization's overall security posture.

The data also reveals substantial input from external entities at 35%, suggesting a reliance on specialized knowledge and external perspectives to augment internal capabilities. Incident response (IR) teams are also pivotal contributors, involved in 33% of cases, due to their front-line experience and practical insights into the TTPs of adversaries. Note: the IR team has seen an overall increase in their contribution to developing a threat hunting methodology since 2023, when only 30% of respondents said that the IR team contributed.

Surprisingly, dedicated threat hunting teams or personnel are listed as contributors in only 21% of instances, which points toward the integration of threat hunting roles within broader security functions rather than as a standalone team.

Methodology Selection

The fluctuating statistics in threat hunting methodologies and staffing strategies over the past three years highlight the challenges organizations are facing in both areas. In 2024, there is a marked shift toward available human resources influencing the selection of methodologies, with 47% of respondents acknowledging this trend, a significant increase from 21% in 2023 and 23% in 2022.

This change suggests that organizations are becoming more resource-conscious, tailoring their threat hunting approaches to the skills and numbers of their available staff. This could reflect the growing skills gap in threat hunting, or even cybersecurity, with a more pragmatic adaptation of methodologies to suit the existing workforce capabilities and capacity.

Conversely, the proportion of organizations reporting that methodologies affect staffing strategy has decreased over the years, dropping to 14% in 2024 from 18% in 2023 and 23% in 2022 (Figure 11). This could imply a shift away from idealized, methodology-driven staffing plans toward a more flexible, resource-driven approach, likely in response to the practical challenges of recruitment and training in cybersecurity. The decrease in the “unknown” category from 12% in 2023 to 7% in 2024 also reflects improved clarity and decision making within organizations about the drivers behind their threat hunting strategies. These trends underscore the evolving nature of threat hunting as organizations move toward adopting a methodology to suit the staffing and expertise they have, instead of a methodology to suit their attacks.

Organizations seem to vary widely in their methods, from structured, tool-reliant detection strategies and formal frameworks like the 4 A’s (assess, acquire, analyze, action) to more instinctual or ad hoc methods, highlighting the adaptability of threat hunting to different operational contexts. Several organizations lean on frameworks such as MITRE ATT&CK and PEAK, utilize a combination of automated software and manual query analysis, or engage external partners for managed detection and response. Methodologies are variously documented, from informal internal records to detailed documentation in platforms like Confluence or Jira, with some organizations allowing hunters considerable flexibility to deviate from established procedures when necessary. This flexibility is often contingent on the documentation of the rationale behind deviations, ensuring that although creativity is permitted, accountability and learning are maintained. Overall, the responses reflect a field that values both the rigor of structured methodologies and the agility to adapt to the nuanced and evolving nature of threat actors.

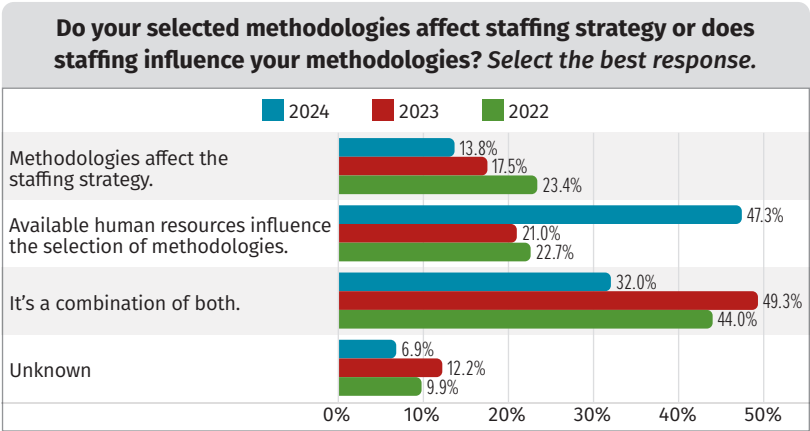


Figure 11. The Relationship Between Methodologies and Staffing

Do Organizations Still Want to Employ Threat Hunters?

The IT world uses a variety of sourcing strategies. Like in the 2023 SANS Threat Hunting Survey, we were interested in whether outsourcing threat hunting is a viable option for our respondents. Given that slightly less than half of our respondents claim that their threat hunting capabilities are mature or very mature (Figure 12), outsourcing might be a viable option.

Whereas in 2023, 63% responded that they didn't outsource threat hunting, this year only 45% don't outsource threat hunting. In contrast, 37% have outsourced threat hunting. The remaining 18% either do not know or are working for a consultancy that offers threat hunting to third parties (Figure 13).

So, what are the pros and cons of outsourcing threat hunting operations? One way to look at it is to split the evaluation into three categories: personnel, intelligence, and consistency.

- **Personnel**—The major point of outsourcing is that another company, and thus external people, are running the hunt. A big advantage to this is that these experts are exposed to a larger number of environments than internal personnel. Frequently, external threat hunters double as incident responders and are remarkably close to what threats and TTPs to hunt for. There are some downsides, though. One is that it might be more difficult and resource heavy to onboard the external entity to exactly what your company is doing and how IT impacts the value chain. Another is that threat hunting can be great training for internal security personnel like security analysts and SOC analysts. When you fully outsource threat hunting, there is no training effect, and SOC and threat hunting might not be integrated well.

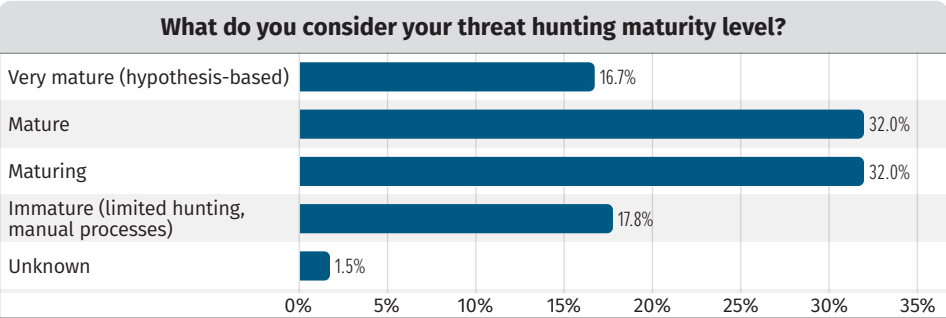


Figure 12. Threat Hunting Maturity

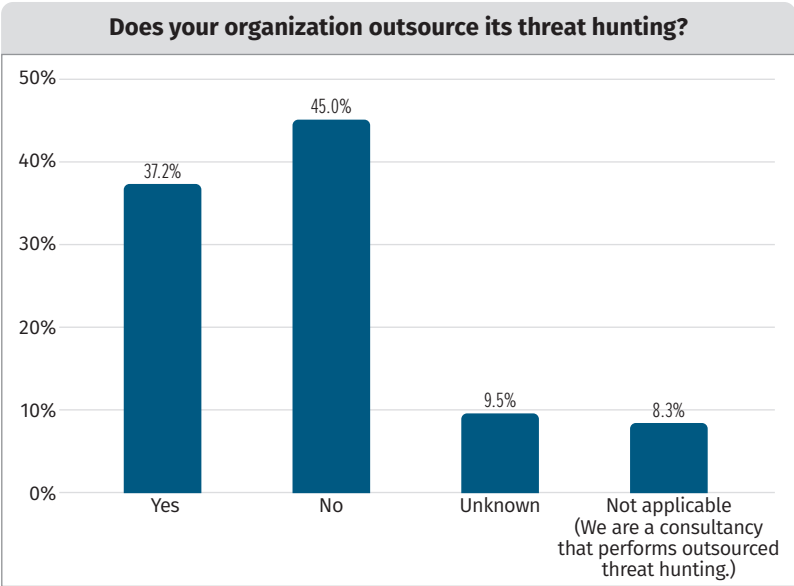


Figure 13. Outsourcing of Threat Hunting

- **Intelligence**—Regarding intelligence, again, both options have ups and downs. An external party might be better trained in accumulating and structuring time-sensitive threat intel. They will also be more exposed to current cyber breaches, because most companies that offer threat hunting are also engaged in incident response cases. What external parties might be lacking, though, is a clear understanding of what threats are most dangerous to your company. Usually, governments and peer groups are good intelligence sources for companies. External entities might not have access to that information. Sometimes companies might even be prohibited from sharing certain intelligence with their threat hunting provider. This results in coverage gaps in the threat hunting operations.
- **Consistency**—Although internal personnel are not necessarily stable—employees might only remain in the company for a few years—our experience has shown us that external entities tend to be more volatile. You might get different incident responders on every hunt based on the schedule of the external party. That does not help continuity. Even if all hunts are documented very well, documentation will never fully describe all parts of a threat hunting mission. When there is no continuity of personnel and strategy, you might miss finding skilled attackers quickly.

So, continuity is a major aspect of threat hunting, and it comes down to having a good strategy and following it. As already mentioned, external parties focused on threat hunting bring knowledge and experiences to the table that internal personnel may take longer to build. At the same time, internal personnel usually better understand how the company works. That allows for better adjustment of threat hunts that are being undertaken.

Ultimately, someone needs to be in the driver's seat. We wanted to know who is in that driver's seat for our respondents who claimed that they outsource threat hunting. The results are interesting. In 2023, 52% stated that threat hunting would be done together with the outsourced team, and 23% left the field completely to the outsourcing partner; however, the numbers have changed. This year, the tables turned toward the outsourcing providers. Now, a good third of respondents (35%) hand over all threat hunting to the third party. The shared approach dropped to 45%. We can only speculate as to what is causing this change. From the authors' experience, it might be that more companies understand the value of threat hunting. At the same time, they are unable to hire the right personnel on short notice, which might make them outsource threat hunting. Because they are new to the field, the tendency to fully outsource might be higher than for more experienced organizations.

To summarize, outsourcing threat hunting can present significant challenges compared to utilizing internal skilled staff. One primary concern is the potential for a disconnect between the outsourced personnel’s understanding of the organization’s unique systems and culture and the nuanced threat landscape they face. Internal staff typically have a more intimate knowledge of the organization’s network architecture, historical security incidents, and specific business risks, which is crucial for effective threat identification and response. Moreover, in-house teams are generally better positioned to facilitate rapid communication and coordination with other internal stakeholders during a security incident—if and when your hunting team uncovers one. Outsourcing can also introduce issues of data governance and security, because sensitive information must be shared with third parties, increasing the risk of data breaches or leaks. There is also the matter of continuity and investment in personnel; internal staff development leads to the accumulation of institutional knowledge and a dedicated, consistent approach to cybersecurity, which could be diluted when relying on external entities that may change personnel or priorities over time.

Hunting for an Impact Within Your Organization

Showing the importance of threat hunting is only helpful if you’re measuring its success within your organization. Data from the last four years reveals a change in the overall trend, with a significant increase in organizations now measuring success or effectiveness for their threat hunting missions (64%). This suggests that organizations increasingly recognize the importance of quantifying the effectiveness of their threat hunting activities.

This significant rise from 34% in 2023 (see Figure 14) indicates a maturing field where the value of metrics and KPIs in guiding and improving threat hunting practices is better appreciated. It also demonstrates a shift toward more strategic and results-oriented cybersecurity operations, where success is not just assumed but evaluated against specific objectives, such as reducing breach detection times, increasing the accuracy of threat detection, or improving response times. In combination with the increase in outsourcing threat hunting, organizations may also be ensuring they are measuring their outsourced vendor against their engagement. Time will tell if this trend is tied to outsourcing or just further improvement in recognizing how threat hunting contributes to the posture of an organization’s cyber defenses.

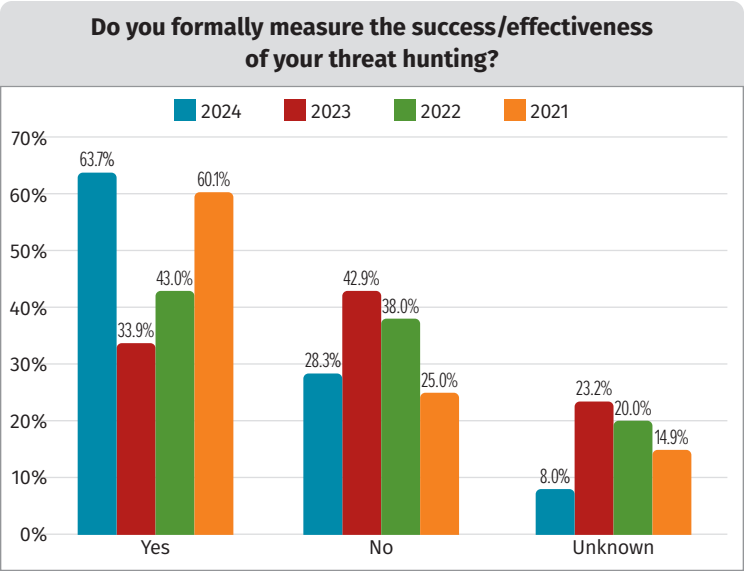


Figure 14. Formal Measurement of Threat Hunting Efforts

Conversely, the proportion of organizations that do not measure the effectiveness of their threat hunting has seen a notable decrease over the past year, from 43% in 2023 to 28% in 2024, which aligns with the increased adoption of measurement practices. This change suggests there is a movement away from informal or ad-hoc threat hunting approaches to more structured methodologies that prioritize accountability and continuous improvement.

When it comes to the measurable improvement that organizations are seeing, compared to last year, those that saw some improvement roughly fell within a very similar pattern. This is somewhat useful in that we’re seeing an overall trend in how effective threat hunting is for organizations. Overall, 63% of organizations see some measurable improvement to the security posture of their organization. That’s a brilliant outcome! However, a concerning 23% reported a negative impact, which could reflect challenges in effectively implementing threat hunting strategies. The 14% reporting no change might suggest either a mature security posture where threat hunting didn’t provide additional benefits or possibly a lack of effective measurement of threat hunting outcomes. Although the data reflects a predominance of positive outcomes, it also underscores the complexity of threat hunting and the variability in its execution and impact.

When it comes to where organizations are seeing improvements, this year, compared to 2023, we see a wider spread across all the areas we poll respondents on (Figure 15). Reducing attack surge exposure on the network and endpoints is one of the two areas with the greatest improvement, at 49%. The category “creation of more accurate detections and fewer false positives” also saw the same level of significant improvement with 49%. For organizations tracking the benefits of threat hunting, there are significant operational cybersecurity improvements. We also saw the areas with no or unknown improvement start to shrink, obviously due to the gains in other areas. It’s likely that as organizations mature further, they are getting better at tracking metrics across multiple improvement areas.

So, what issues are troubling our threat hunters or organizations wanting to do threat hunting? Comparing 2024 and 2023 results, there is a noteworthy shift in the perceived barriers to threat hunting. Although the lack of skilled staff remains the top challenge, it has seen a significant decrease from 73% in 2023 to 50% in 2024, suggesting that either the talent gap is slowly being addressed or organizations are finding alternative solutions to manage this issue.

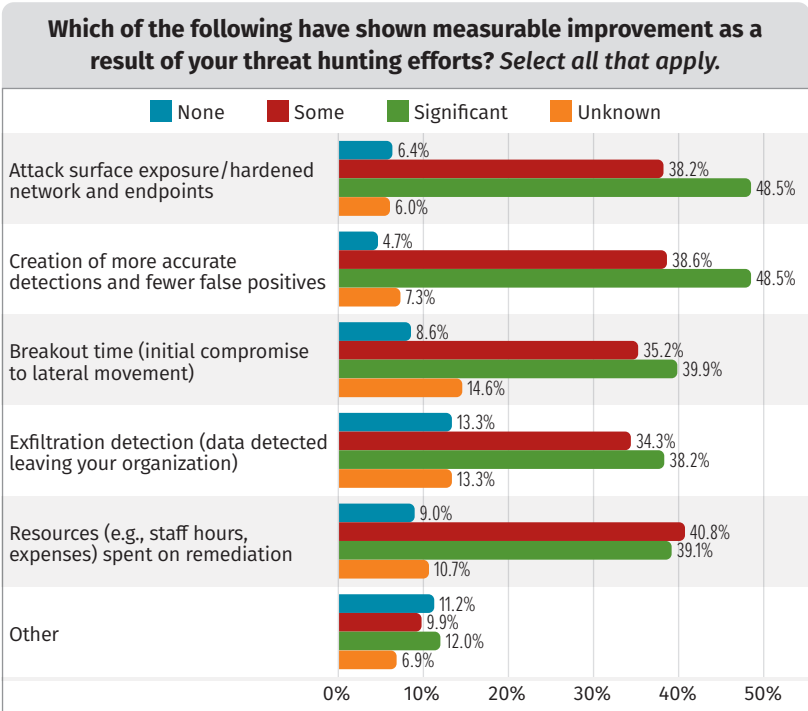


Figure 15. Improvements Resulting from Threat Hunting

Budget constraints have decreased from 54% in 2023 to 40% in 2024, due to organizations finding funding to train internal staff or hire externally skilled staff. Data quality and/or quantity has become this year's rising concern, increasing from 34% to 44%, which may reflect an ever-growing flood of cybersecurity data and the associated complexities of processing and leveraging this information for threat hunting purposes. Interestingly, the concern regarding the lack of data standards or common data types has grown from 26% to 33%, which could signify a growing awareness of the importance of data interoperability in threat detection and analysis.

There is also a decrease in the percentage of respondents who cite limitations of tools/technology, lack of defined processes, and budget constraints as primary barriers, indicating possible improvements in these areas or a shift in focus toward other challenges. These trends suggest that although progress is being made in some areas, there are still challenges around skills and a growing burden of data. Oddly enough, skilled staff may be able to fix the growing data burden further, assuming we find or train skilled staff.

Conclusion

The SANS 2024 Threat Hunting Survey provides insights that reflect not only an industry in evolution, but also one that is actively seeking enhancements to its cyber defense capabilities. Organizations recognize the need for improved contextual awareness in their threat hunting efforts, with 51% planning to refine their ability to discern and respond to nuanced threats through better data sources and tools. Furthermore, 47% of organizations aim to integrate artificial intelligence (AI) and machine learning (ML) into their threat hunting apparatus, acknowledging the growing complexity and volume of threats that demand smarter and more autonomous responses.

Investment in both staff and tools is on the agenda for many organizations, with a notable percentage planning to increase their investment by more than 10% (20% for staff, 23% for tools) or by more than 25% (15% for staff, 19.0% for tools) within the next 24 months. This prospective financial commitment underscores the strategic importance placed on threat hunting as a discipline within the cybersecurity industry. Conversely, a minority of organizations anticipate a decrease in investment, with less than 2% expecting a 100% change in staff and in tools, potentially indicating a shift away from threat hunting to a different security strategy—definitely a place for further questions next year.

Addressing the primary barriers to threat hunting, the survey indicates a decrease in concerns over the limitations of tools/technology and budget constraints, which could suggest an industry that is finding its footing with the existing technological advancements and available resources. However, the gap in skilled personnel remains a prominent challenge. Organizations are looking to fortify their teams with more internal staff possessing investigative skills, as indicated by 39% of respondents, aiming to bolster their search capabilities and enhance scalability across the enterprise.

In summation, the survey reveals a cybersecurity landscape in transition, with organizations not only recognizing the indispensable role of threat hunting in a robust security posture but also committing to significant investments in both human and technological capital. As the threat landscape continues to advance, so does the recognition of the need for greater sophistication in threat hunting capabilities, from AI integration to better data management and staff expertise. These strategic priorities will undoubtedly shape the future of cybersecurity defense mechanisms.

Sponsor

SANS would like to thank this survey's sponsor:



Product Briefing

Threat Hunting with Splunk: Insights from the 2024 SANS Institute Survey

March 2024

Today's complex and fast-changing threat environment means security professionals need highly advanced threat hunting technologies to ensure that they're always one step ahead of the bad actors out there. This year's edition of the annual SANS Institute threat hunting survey shows increasing enterprise recognition of the importance, and the challenges, of this essential security discipline.

The Splunk Platform

Splunk offers a comprehensive data platform designed to offer end-to-end threat visibility, from the network to the cloud to security operations centers (SOCs) at every level of threat hunting maturity. The platform, delivered flexibly as a fully managed offering in Splunk Cloud Platform or a customer-managed offering in Splunk Enterprise, makes it possible for SOC teams to proactively explore, analyze, visualize, and—most importantly—act on threat data, with capabilities to support their available personnel and skill sets. These capabilities range from advanced analytics to custom boards and visualizations to artificial intelligence (AI) and machine learning (ML) toolkits. The Splunk platform capabilities are extended by the Splunk App Ecosystem, which includes thousands of free add-ons, and the Machine Learning Toolkit (MLTK) and Data Science and the Deep Learning (DSDL) app. The range of the Splunk platform capabilities is crucial, because the company—like the majority of respondents to this year's SANS Threat Hunting survey—recognizes that the difficulty of attracting and retaining skilled personnel is the single greatest problem enterprises face in addressing a rapidly evolving threat environment. To address this challenge, Splunk's SURGe security research team¹ developed the PEAK Threat Hunting Framework² that includes the Hunting Maturity Model (HMM),³ which enables enterprises and their security organizations to determine what their current threat hunting capabilities are, what they need them to be, and what they'll have to do to get there. The result: SOC teams can identify and mitigate security threats, rapidly, efficiently, and cost-effectively—and also use the lessons learned in the process to develop more and more sophisticated threat hunting capabilities, advance the enterprise's overall security maturity, drive continuous improvement in their security posture, and justify budget requests for further advances. As SOC teams continue to mature, Splunk also offers premium security solutions to strengthen digital resilience with unified threat detection, investigation, and response.

Key Finding from the 2024 SANS Threat Hunting Survey



The need for skilled personnel remains the key obstacle to improved threat detection and response, with fully 50% of the survey respondents identifying it as their No. 1 challenge.

It's worth noting that this result represents a significant decrease from the previous year's 73%. This may reflect greater overall awareness of the importance of threat hunting in the security industry and its attractiveness as a career path—but shows that attracting and retaining necessary skills is still a critical problem industrywide.

It also suggests a need to reduce the reliance on manual processes by techniques like automation, AI and ML wherever appropriate.

¹ www.splunk.com/en_us/surge

² www.splunk.com/en_us/form/the-peak-threat-hunting-framework

³ Bianco, David J., "A Simple Hunting Maturity Model," October 2015, <https://bit.ly/HuntingMaturityModel>

The Splunk platform approach to threat hunting begins with its proprietary SPL query language, which includes rich and highly expressive data analytics capabilities. This means Splunk doesn't simply stop at searching for threats, but it allows a hunter to quickly and easily create new detection techniques, taking advantage of both Splunk's speedy search and SPL's extensive analysis capabilities—in essence, giving hunters quick answers to their questions and allowing them to rapidly ask newer and better questions. The result is that threat hunting becomes faster, more efficient, and more cost-effective; and the SOC's threat hunting capabilities become dramatically more mature.

The first step in advancing a SOC's threat hunting maturity is, of course, to determine its current level of maturity. The HMM, an integral part of the PEAK Threat Hunting Framework, uses threat hunting results to establish the enterprise's current state, identify its current and future requirements, and determine the skills and technologies that will be needed to address those requirements. See Figure 1.

Figure 2 shows the steps an enterprise and its security organization may take along the path to more and more advanced threat hunting maturity, and what Splunk does at each step.

This is, of course, an iterative process, and one that builds on its successes and its other outcomes. Security professionals need to recognize that threat hunting isn't just about identifying and addressing existing security events.

It's also about driving continuous improvement across an organization's entire security posture. Threat actors are becoming ever more sophisticated, and their threats are becoming ever more widespread. SOCs simply can't scale to address those threats using their current labor-intensive techniques. They need tools and techniques—notably including AI and ML—that will enable them to both protect the enterprise and show their value to its most senior decision-makers.

To learn more about Splunk's threat hunting capabilities, visit www.splunk.com/security.

SANS 2024 Threat Hunting Survey: Hunting for Normal Within Chaos represents the ninth edition of SANS Institute's survey of security professionals engaged in or impacted by this proactive approach to identifying and remediating previously unknown or undetected security threats. The sponsors of this year's survey all offer advanced threat hunting capabilities that we believe will be of interest to SANS' clients, and, for this reason, we're presenting product briefings on their relevant product and service offerings. Note that SANS Product Briefings do not represent a SANS endorsement of a sponsor or its products, but rather an overview of its offerings and their capabilities.

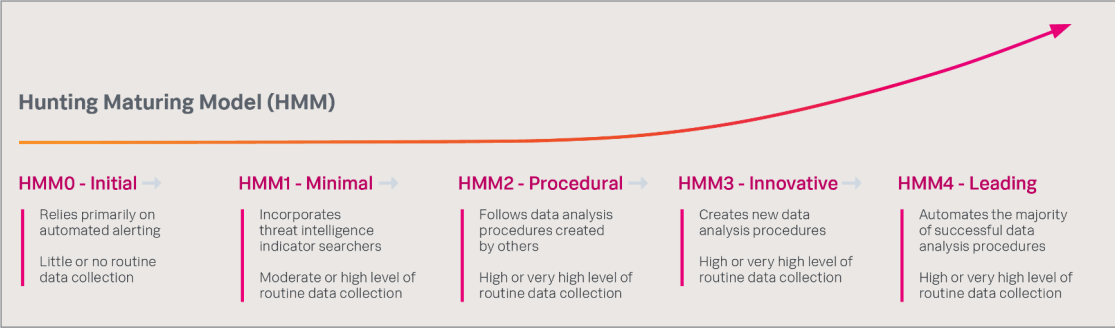


Figure 1. The Hunting Maturity Model (HMM)

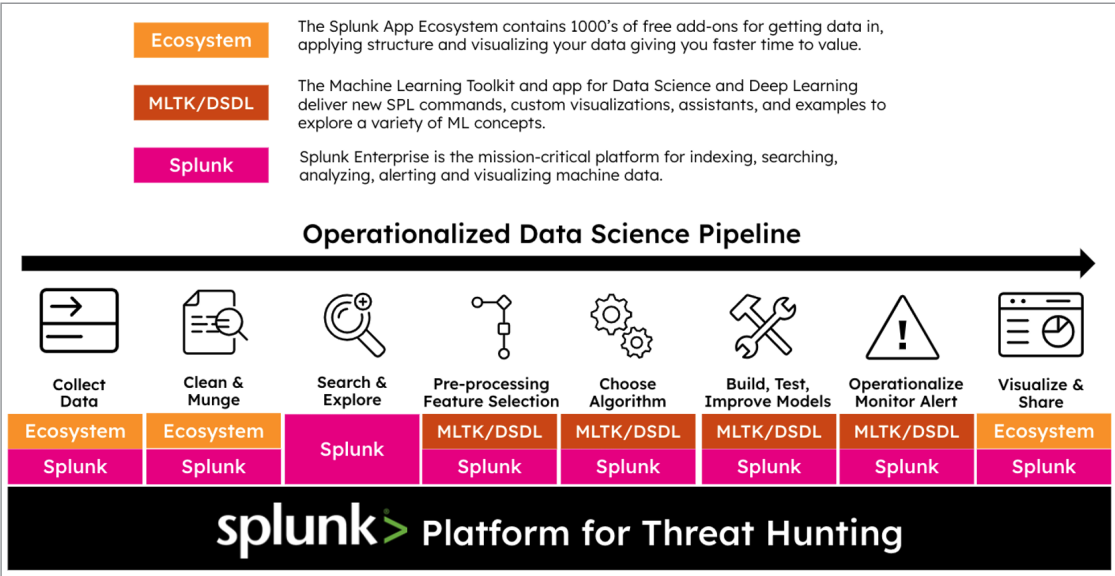


Figure 2. Splunk's Operationalized Data Science Pipeline