SANS | Research Program

Survey

SANS 2025 Threat Hunting Survey: Advancements in Threat Hunting Amid AI and Cloud Challenges

Written by **Josh Lemon**

March 2025

Google Cloud Security

©2025 SANS™ Institute

Executive Summary/Introduction

The 2025 SANS Threat Hunting Survey marks a decade of tracking how organizations evolve their threat hunting capabilities. This year's findings reinforce that threat hunting remains a critical function within security operations, with organizations prioritizing agility, methodology refinement, and better integration of intelligence sources. Although formal methodologies saw a slight decline, the trend toward structured approaches continues, indicating that organizations are balancing flexibility with repeatable processes.

One of the most significant shifts this year is the decline in organizations outsourcing their threat hunting, with more teams opting to build internal capabilities. This shift aligns with the broader push for in-house expertise, particularly in defining methodologies, collecting intelligence, and performing hunt missions. However, a shortage of skilled personnel remains a primary challenge, exacerbated by budget constraints, the increasing complexity of threat landscapes, and the persistent difficulties of cloud threat hunting. Visibility across cloud environments and hunting in diverse log sources continue to be pain points, alongside the struggle to normalize data across disparate security tools.

Organizations are continuing their focus on improving automation and AI-driven hunting, although the impact of AI-based techniques on uncovering threat actors remains limited. Despite this, organizations have a clear push to integrate AI into their processes, suggesting a strategic investment in future capabilities rather than immediate operational gains.

When it comes to adversaries, business email compromise (BEC) remains the most discovered threat when threat hunting. However, ransomware detections have declined, potentially due to improved mitigation strategies or faster attack execution by ransomware groups. Catching nation-state threats via threat hunting has slightly risen this year, highlighting a steady presence of nation-state threats in the cyber landscape. We also find that "living off the land" (LOTL) techniques remain the most prevalent tactic across all adversary groups, reinforcing the need for behavior-based threat hunting.

Key findings:

- 45% of organizations now update methodologies as needed, up from 35% in 2024.
- Organizations fully outsourcing threat hunting dropped to 30%, down from 37% last year.
- 61% of respondents cite skilled staffing shortages as a primary barrier to success.
- Ransomware detections declined from 63% to 46%, but targeted exfiltration remains a concern at 57%.
- 76% of organizations report seeing LOTL techniques in nation-state attacks, unchanged from last year.
- Organizations increasing staffing investment (10% or more) sit at 40%, with 31% not planning to make changes.

- The use of commercial tools for tracking the threat landscape declined to 58% (from 70%), with internally built tools rising to 48%.
- 76% of organizations are using vendor blogs and papers as a priority source for their threat intelligence and research.
- EDR/XDR remains the top-ranked tool for threat hunting, followed by SIEM and NDR solutions.

As threat actors evolve their techniques, organizations must ensure their threat hunting programs remain adaptable and intelligence-driven. This year's findings highlight key shifts in methodologies, tools, and adversary tactics, providing critical insights into how organizations are refining their hunts. For a deeper look into the evolving landscape of threat hunting, this year's report offers data-driven analysis and strategic recommendations to help defenders stay ahead. For a demographic snapshot of this year's respondents, see Figure 1.

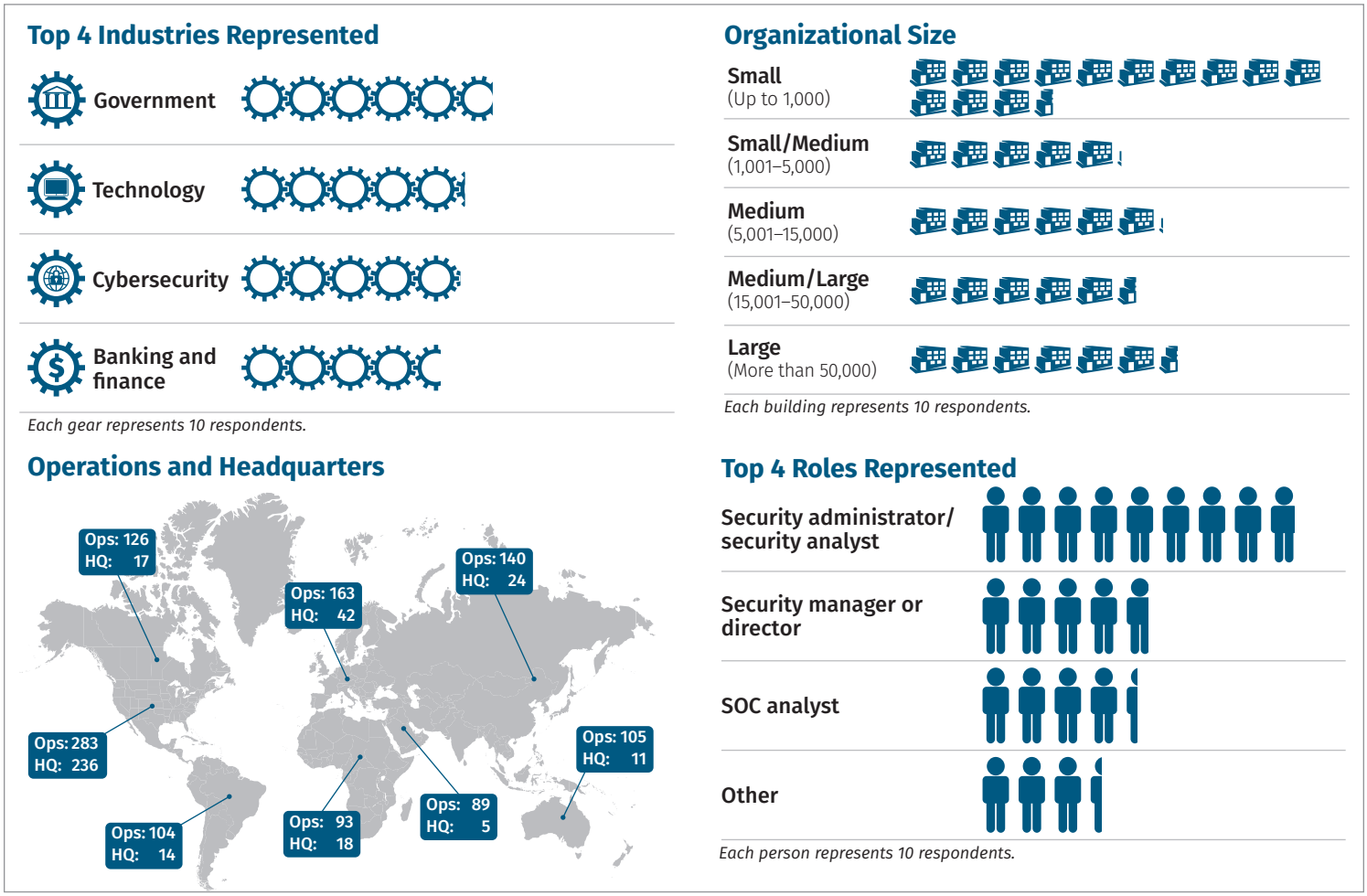


Figure 1. Demographics of Survey Respondents

Plan the Hunt, Hunt the Plan—or Just Wing It?

The 2025 data indicates a slight decline in organizations with formally defined threat hunting methodologies (46%, down from 51% in 2024), as shown in Figure 2. Although this remains a strong indication of maturity within the industry, the drop suggests that some organizations may struggle to maintain structured approaches to threat hunting. This could be due to operational challenges, shifts in priorities, or resource constraints. However, compared to 2023's 35%, the trend still reflects an overall positive shift toward more formalization within threat hunting. A defined methodology can help provide guidance and consistency when performing threat hunting. Having a methodology does not always mean that you need to stick to the same plan every single year. It is normal for concepts and approaches to threat hunting to change as threat actors change their tactics. However, it still is essential to maintain a plan when it comes to conducting threat hunting within an organization; otherwise, do you even know what you're hunting for?

One of the clear challenges we have seen from respondents over the years is that there is no formally accepted industry methodology for conducting threat hunting. There are many types of methodologies available for organizations to use; however, no one methodology has yet been adopted by a majority within our industry.



Figure 2. Types of Methodologies

Interestingly, the percentage of organizations relying on ad hoc methodologies (38%) has remained relatively stable, with only minor fluctuations over the past three years. This suggests that while some organizations recognize the benefits of structure, they haven't managed to land on a methodology that might work long term. Meanwhile, 12% of organizations plan to define their methodologies, a figure that remains consistent with 13% in 2024, but has improved significantly from 2023 (20%), signaling that many of those who intended to formalize their approaches have already done so. However, based on the math alone, it shows the number of organizations with no plans to formalize methodologies (4%) has more than doubled since 2024 (2%), though it remains an improvement over the 7% in 2023. This suggests that a small but persistent segment of organizations may still be struggling to see the value in a structured methodology or may simply be struggling to build a methodology. As adversaries evolve, organizations without a clear methodology risk falling behind, reinforcing the need for continued investment in structured, repeatable threat hunting practices.

When we look at who is building methodologies and who is performing threat hunting, there is a pretty large divide between these two groups. CISOs (53%) and external entities (49%) are the most prominent contributors to methodology development alone, reflecting a reliance on strategic oversight and external expertise in shaping how organizations conduct threat hunting. We also see 30% of incident response (IR) teams playing a significant role in defining methodologies, leveraging their hands-on experience with security incidents to refine detection and investigation strategies. Interestingly, only 15% of dedicated threat hunting teams contribute to methodology development, reinforcing the trend that hunting is often embedded across multiple security disciplines rather than operating as a standalone function. The 10% classified as "other" includes various cybersecurity teams such as SOC analysts and cyber threat intelligence groups, further emphasizing the collaborative nature of methodology design.

When it comes to executing threat hunts, those with dedicated threat hunting teams are the most actively engaged group (62%), both performing hunts and contributing to methodology development. IR teams (40%) also have a strong presence in both areas, aligning with their responsibility for incident response and forensic investigations. It is possible this also may occur in some organizations that do not have dedicated threat hunting teams. External entities (22%) play a lesser role in execution compared to their contribution to methodology design, suggesting that while third-party intelligence informs strategy, most organizations prefer to retain hands-on hunting capabilities in-house. Interestingly, 10% of CISOs are directly involved in performing hunts!

When it comes to organizations updating their methodologies, we see a notable increase in those reviewing and adjusting them on an as-needed basis, rising to 45% from 35% in 2024. This shift suggests that many organizations prioritize agility, allowing them to adapt to emerging threats rather than adhere to fixed review cycles. Provided organizations are making these changes in a structured way, it can show a strong ability for the threat hunting team to be agile. However, if this is more the result of organizations changing plans due to a lack of a plan, then it might better demonstrate the need to have a plan. In contrast, monthly reviews have dropped sharply from 26% to 13%, and quarterly reviews also have declined from 20% to 14%. Meanwhile, annual reviews increased to 15% from 11%, reinforcing a possible trend toward less frequent but more strategic updates. Overall, these shifts may reflect threat hunting teams trying to stay on top of an evolving threat landscape.

This year's findings highlight a shift in how organizations balance their threat hunting methodologies with staffing strategies. Twenty percent of respondents report that methodologies now dictate staffing decisions, increasing from 14% in 2024 (see Figure 3). Although still lower than in earlier years, this uptick suggests that more organizations focus on structured methodologies first and then align their teams accordingly. In contrast, the percentage of organizations allowing available human resources to shape methodology choices has dropped sharply to 28%, down from 47% in 2024. This is a notable decline and, frankly, a welcome one. As commented on in previous reports, we want to see organizations develop the best approach and then try to staff that approach rather than trying to put a square peg in a round hole by cutting down a methodology due to resources. A growing number of organizations, 44% in 2025 compared to 32% in 2024, have indicated that staffing and methodologies influence each other, reinforcing the idea that neither should be considered in isolation. This year's data suggests a move toward more organizations taking a balanced approach, where methodology and staffing decisions evolve together rather than one leading the other.

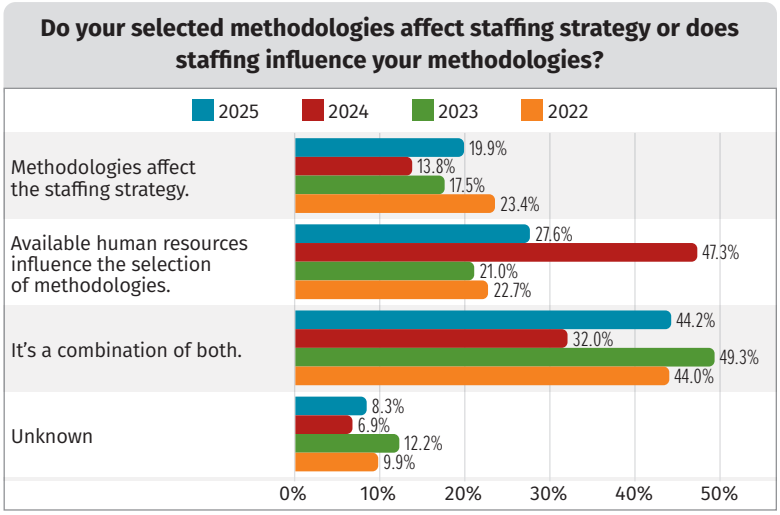


Figure 3. Methodologies vs. Staffing

This year, we again tried to get a sense of how organizations are threat hunting with an open-ended question. The responses highlight a diverse range of threat hunting methodologies, reflecting varying levels of maturity, structure, and adaptability across organizations. Many organizations appear to be leveraging hypothesis-driven approaches, often using frameworks such as MITRE ATT&CK™[1], PEAK,[2] TaHiTI,[3] and the Pyramid of Pain[4] to define hunts. Some responses emphasize a step-by-step process with limited deviation, while others allow hunters full autonomy to explore threats based on evolving intelligence and investigative instincts. There also appeared to be a strong reliance on threat intelligence feeds, network traffic analysis, endpoint detection tools, and behavioral analytics to identify anomalies and generate hunt hypotheses.

We also discovered that some organizations document every phase of their hunts in SOPs, internal wikis, or platforms like SharePoint, ensuring repeatability and knowledge retention, while others prefer a more ad hoc and reactive approach, allowing their hunters to pivot as new threats emerge. Additionally, organizations vary in their use of automation and AI, with some integrating XDR, SIEMs, and behavioral analytics tools, while others rely heavily on manual analysis and human-driven insights. The responses indicate that while structured methodologies provide consistency, adaptability appears to remain a critical factor in effective threat hunting, particularly in detecting threats that evade traditional security measures.

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

[2] "Introducing the PEAK Threat Hunting Framework," www.splunk.com/en_us/blog/security/peak-threat-hunting-framework.html

[3] "TaHiTI," www.betaalvereniging.nl/en/safety/tahiti

[4] "Enterprise Detection & Response: The Pyramid of Pain," https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Worth It, or Just a Wild Goose Chase?

Being able to show your success in threat hunting is essential. However, that is primarily centered around whether an organization is measuring that success. This year's data shows a decline in organizations that formally measure the effectiveness of their threat hunting programs, dropping to 51% from 64% in 2024 (see Figure 4). Although this remains an improvement over the 2023 responses (34%), the decrease raises concerns about whether organizations are deprioritizing structured performance assessments or struggling to implement effective measurement frameworks. At the same time, the number of organizations not measuring success is on the rise (38%), up from 28% in 2024, reversing the previous gains in accountability and effectiveness tracking. Without clear metrics, organizations risk inefficient allocation of resources, making it harder to justify continued investment in threat hunting.

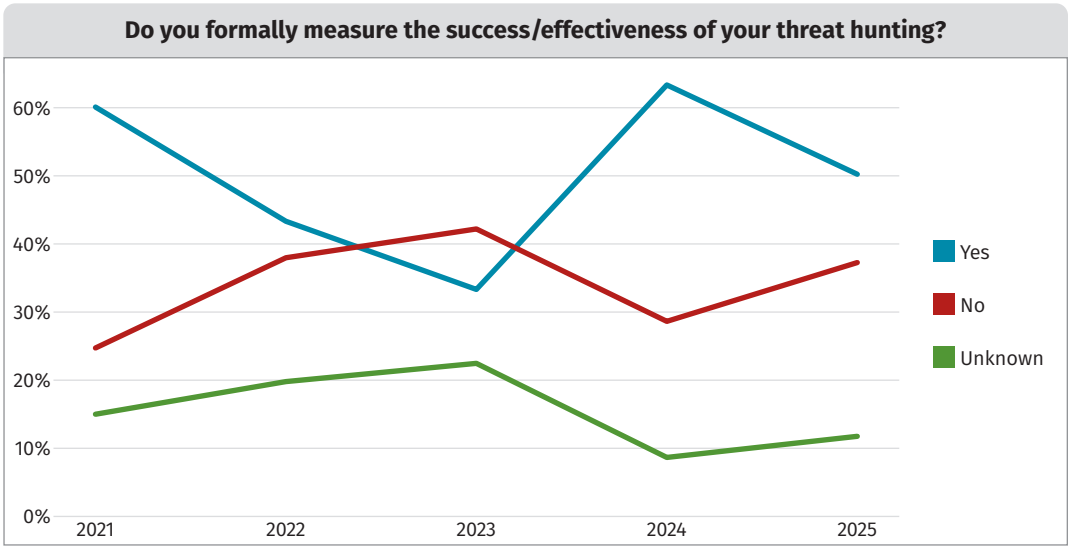


Figure 4. Formally Measuring Success

Manually tracking the effectiveness of threat hunting has rocketed to the top as the most used method, rising significantly to 61% from 43% in 2024. This is a surprising increase, given the results for manual tracking last year. However, it might start to show gaps that exist in the threat hunting world when it comes to trying to track its effectiveness. Within other areas of security operations, we have numerous tools for tracking metrics and statistics when it comes to detections and alerting. However, our industry has not really settled on a strong method for measuring, let alone tracking, effectiveness for threat hunting. This might explain why we don't see a wide range of tools or software that allows our threat hunters to track or measure their effectiveness. One of the challenges that exists within this area is having a methodology that is relatively static, so you can set measurements and metrics against that methodology. As mentioned earlier, we still don't see a strong majority of threat hunters sticking to a single methodology when it comes to conducting their hunt missions.

Automated tracking also saw growth, increasing to 52% from 41% in 2024, hopefully indicating that organizations are looking to balance structured documentation with efficiency-driven automation. Oddly, the reliance on legitimate alerts generated from threat intelligence as a success metric jumped to 55% from 37%, which is unusual because it would be more common for threat intelligence to originate from active incident response or externally supplied threat intelligence. Other notable increases include formal reporting (46%, up from 29%) and direct feedback from business owners (30%, up from 17%), signaling that threat hunting teams are bringing the rest of the organization along on the threat hunting journey, which hopefully will lead to better overall cybersecurity outcomes for organizations. However, the increase in ad hoc measurement approaches (28%, up from 15%) suggests that some organizations still lack a standardized framework, potentially leading to inconsistencies in assessing program success.

Respondents this year reflect a generally positive trend in how organizations perceive the impact of threat hunting on their overall security posture. The most significant increase is in the +25% improvement category, rising to 29% this year, suggesting that more organizations are seeing moderate but meaningful security gains from their threat hunting efforts (see Figure 5). Similarly, +10% improvements grew to 18% from 13% last year, reinforcing the idea that incremental enhancements are being realized across a broader segment. Larger improvements of a +50% increase in the overall security of an organization (15%) and +75% (11%) remained consistent with past years, indicating that while some organizations experience major gains, the overall impact is more measured than transformational. Encouragingly, negative perceptions of threat hunting have dropped significantly, with organizations reporting –50% or worse declining from 7% in 2024 to 4% in 2025, showing that fewer organizations feel threat hunting has negatively impacted security. Sadly, we still see 12% of respondents report no improvement, underscoring that although threat hunting is proving valuable for many, challenges remain in fully integrating and optimizing its effectiveness. Overall, this year's sentiment shows a shift to the right of our graph, which we hope indicates that threat hunting is becoming more common in organizations and slowly growing with positive improvements. It also means that organizations who conduct threat hunting are seeing an overall—and growing—improvement to their organization's security posture. If you haven't started threat hunting within your organization, these are powerful statistics to show the improvement it will have.

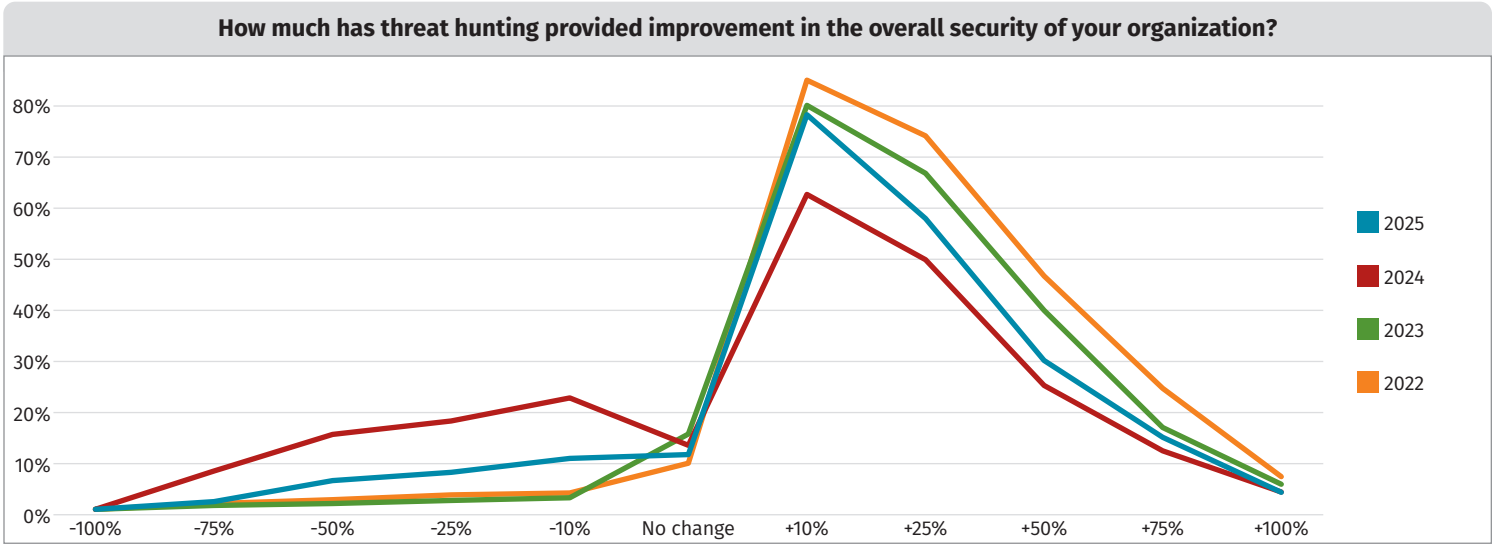


Figure 5. Improvement of Overall Security

What Threat Hunting Is Catching in 2025

This year, we added a new question to better understand from our respondents what areas they feel are most important to conduct threat hunting in, as well as the most difficult areas for them to conduct threat hunting within their organization. This was designed to understand what technical areas organizations feel are most important to catch threat actors and those that pose the biggest challenges. We found a clear distinction between the areas organizations prioritize for effective threat hunting and the environments where threat hunting is most challenging. Servers (26%) and workstations (25%) rank as the top priorities, reflecting their critical role in daily operations and the high-value data they store (see Figure 6). This, of course, makes sense as these are the locations where threat actors typically enter an organization and where they embed themselves once they are in an organization.

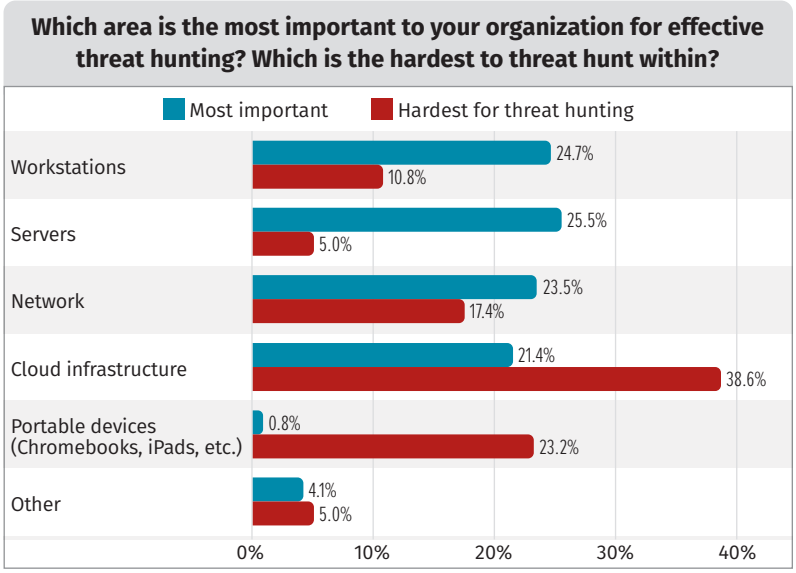


Figure 6. Threat Hunting Focus Areas

The network (24%) follows closely, highlighting the need to monitor lateral movement and attacker activities within internal infrastructure. Interestingly, cloud infrastructure (21%) remains a growing priority, aligning with the widespread migration to cloud-based environments. However, when it comes to difficulty conducting threat hunts, cloud environments present the biggest challenge, with 39% of respondents citing them as the most complex area in which to conduct threat hunting. This likely reflects the vast difference in conducting threat hunting on host systems compared to cloud-based infrastructure, and threat hunters having to context switch between hunting on an on-premises system to cloud infrastructure that requires different types of tooling and techniques. As a simple example, if a threat hunter were looking at authenticated logs on an on-premises system, then looking at authentication logs in the cloud, they would be in different formats, require different tools to collect and analyze them, and likely express the same data differently.

Portable devices (23%) rank high in difficulty, likely due to device mobility, varied operating systems, and challenges in conducting remote-based threat hunting. Although our respondents showed that a little under 1% conduct threat hunting on these types of devices, they are likely a device type that will require close monitoring as workforces become more mobile and agile in the future. Although workstations (11%) and networks (17%) pose some challenges, they appear more manageable than cloud and portable-device environments. These findings suggest that while organizations prioritize traditional IT assets for hunting, they continue to grapple with visibility and control in increasingly cloud-based and portable infrastructures, which require new tools, techniques, and knowledge to detect threats within these environments successfully.

We've seen a shift in the types of attacks being uncovered through threat hunting this year, with some notable declines and emerging trends. Business email compromise (BEC) remains the most detected attack type, although it has decreased to 64% from 68% in 2024 (see Figure 7). This suggests that although BEC remains a significant threat, improved detection and mitigation strategies may be reducing its overall prevalence. The other significant difference to catching BEC threat actors is that their tactics rarely change, so they typically become an easy threat to find when you go hunting for them.

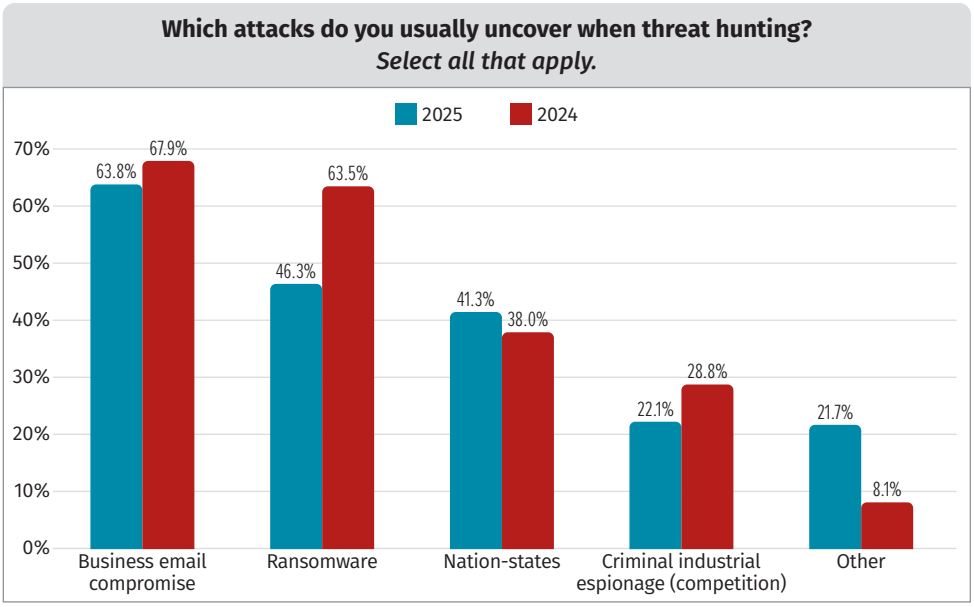


Figure 7. Types of Attacks

Ransomware detections have dropped significantly, falling to 46% this year from 63% in 2024, which could indicate either that organizations are preventing attacks earlier in the kill chain or that ransomware actors are shifting tactics to evade traditional hunting methods. The other, more concerning possibility is that ransomware threat actors are becoming faster at compromising and ransoming organizations, giving threat hunters little chance to catch them. In contrast, nation-state threats have slightly increased, rising to 41% from 38% in 2024, reinforcing the ongoing geopolitical tensions that drive state-sponsored cyber activities. Criminal industrial espionage detections have also declined from 29% in 2024 to 22% this year, possibly reflecting changes in adversary focus or improved internal security controls. The "other" category has risen significantly to 22% from 8%, showing that organizations are detecting a broader variety of emerging and atypical threats, from more generalized cybercrime acts, insider threats, and misconfigurations.

When we focus on what our threat hunters are discovering when they uncover nation-state threat actors, the persistence of LOTL techniques remains the most observed tactic in nation-state attacks at 76%, unchanged from 2024 (see Figure 8). This highlights that nation-state threat actors favor built-in system tools to evade detection and blend into legitimate background activity. Similarly, off-the-shelf tools (like Cobalt Strike, Brute Ratel, and Sliver) remain high at 62%, showing that adversaries still leverage publicly available frameworks for post-exploitation and lateral movement. However, the use of custom malware has declined to 56% this year from 64% in 2024, potentially indicating a shift toward lower-cost, reusable tools rather than bespoke malware development.

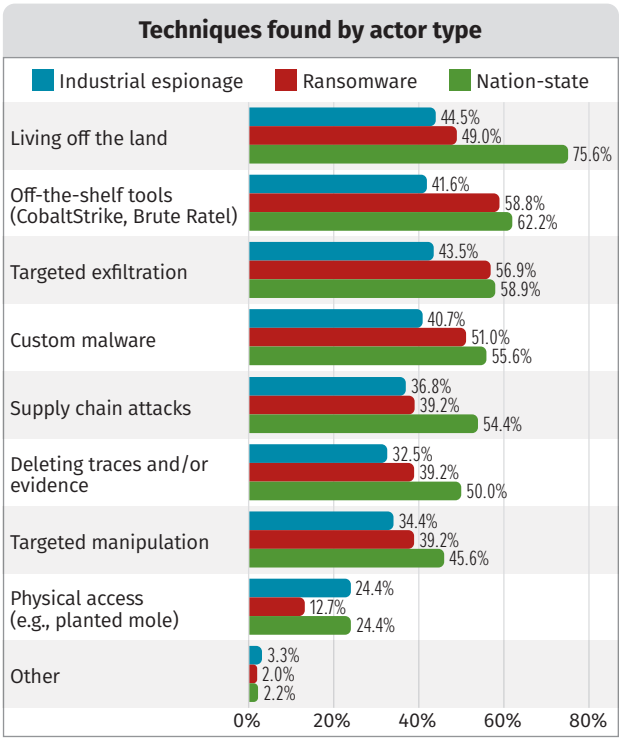


Figure 8. Techniques by Actor Type

When you consider frameworks like the Pyramid of Pain—which revealed back in 2014 that it was challenging for threat actors to alter the tools they were using when conducting a compromise—it makes sense for nation-state threat actors to pivot to using off-the-shelf tooling to make it faster for them to adapt, if and when their tools are caught within a victim's network. Targeted exfiltration has increased to 59% from 54%, suggesting a greater focus on data theft and espionage, particularly as data-driven attacks become more strategic (see Figure 9). Interestingly, nation-state actors appear to focus more on operational security, as deleting traces and evidence rose sharply to 50% from 41%, reinforcing adversaries' intent to cover their tracks and extend dwell time within compromised networks. Meanwhile, targeted manipulation (46%) and supply chain attacks (54%) have remained relatively steady, emphasizing that long-term access and supply chain infiltration remain key nation-state strategies.

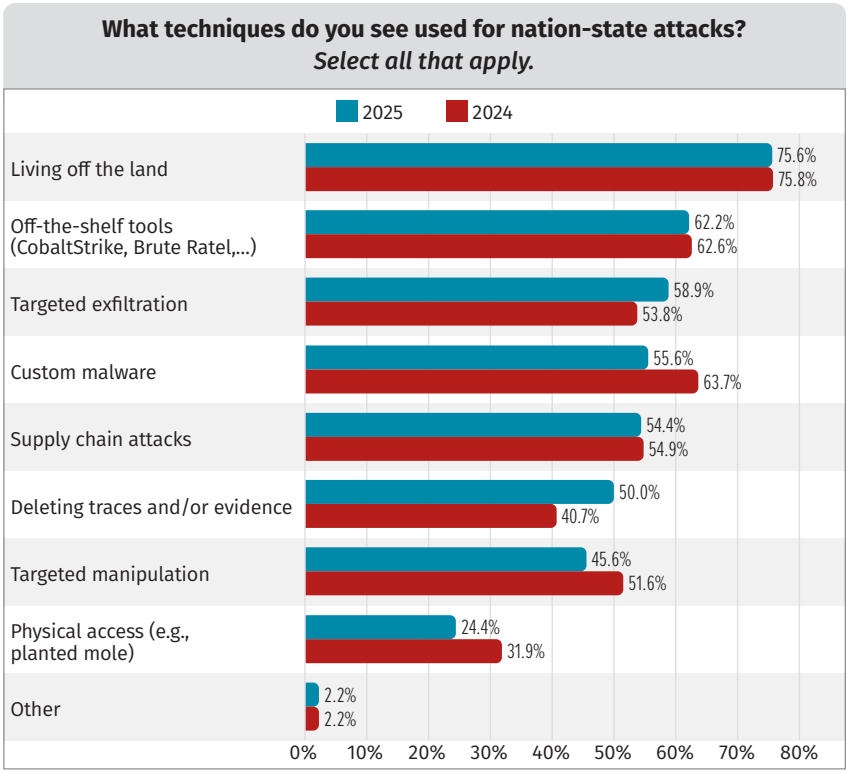


Figure 9. Nation-State Techniques

Ransomware attack techniques continue to emphasize off-the-shelf tools and frameworks as their preferred technique (59%), reflecting ransomware groups' preference for readily available post-exploitation frameworks to evade detection and establish persistence (see Figure 10). In another sense, it also shows a lack of creativity and the need for speed when it comes to being able to compromise a victim rapidly. Targeted exfiltration remains high at 57%, emphasizing that modern ransomware attacks are predominantly about data theft. Interestingly, the use of custom malware has declined to 51% from 61% in 2024. A notable increase in LOTL (49%, from 42% in 2024) signals that ransomware groups are refining their techniques to blend into the background of a system, making detection harder and further emphasizing the need for conducting threat hunting on behavioral techniques. At the same time, deleting traces and evidence has jumped to 39% from 27% in 2024, reinforcing that adversaries are investing more in anti-forensic measures, like what we're seeing in nation-state threat actors. Supply chain attacks have risen slightly to 39% from 34% in 2024, underscoring the expanding attack surface as ransomware operators exploit third-party vulnerabilities to infiltrate victims. From the threat actors' perspective, this provides a broader scope of potential victims that will pay their ransom fee.

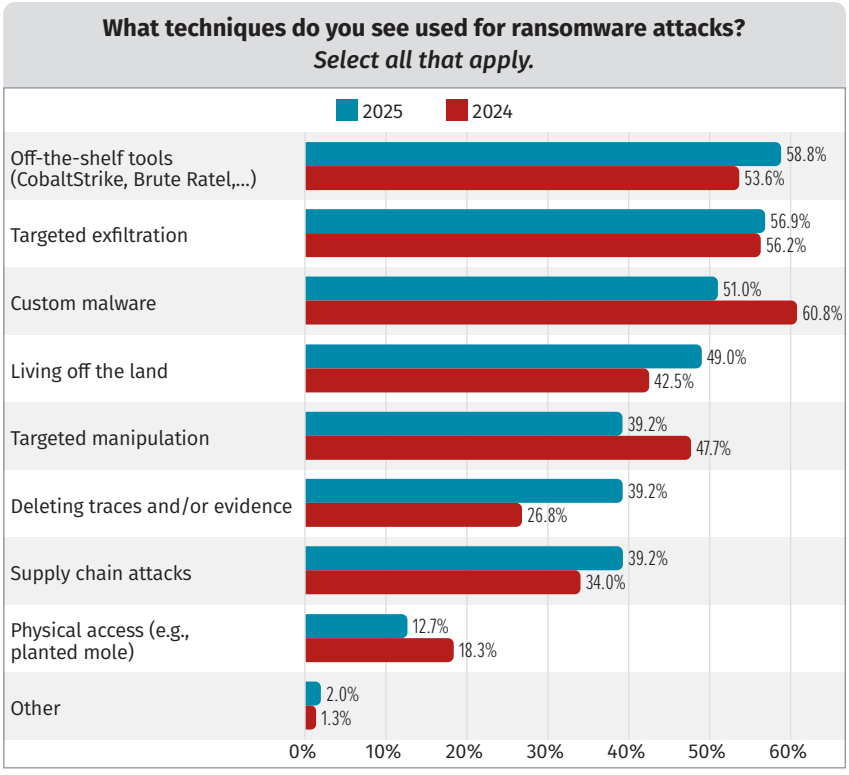


Figure 10. Ransomware Techniques

As seen with our other threat actors caught by threat hunters, LOTL also has seen a notable rise from 32% in 2024 to 45% in 2025 by criminal actors engaging in industrial espionage (see Figure 11). This suggests that espionage groups are also increasingly leveraging legitimate or built-in system tools to evade detection rather than deploying malware that might trigger security controls. Targeted exfiltration (44%) remains a top method, emphasizing that data theft is the primary objective of these actors. Off-the-shelf tools (42%) also have slightly increased, reinforcing the trend of espionage groups adopting widely available penetration testing tools over building their own custom malware, which has declined to 41% from 47% in 2024. Supply chain attacks (37%) by organized crime groups have increased significantly from 2024 (27%), pointing to a growing focus on infiltrating organizations through third-party vendors or service providers.

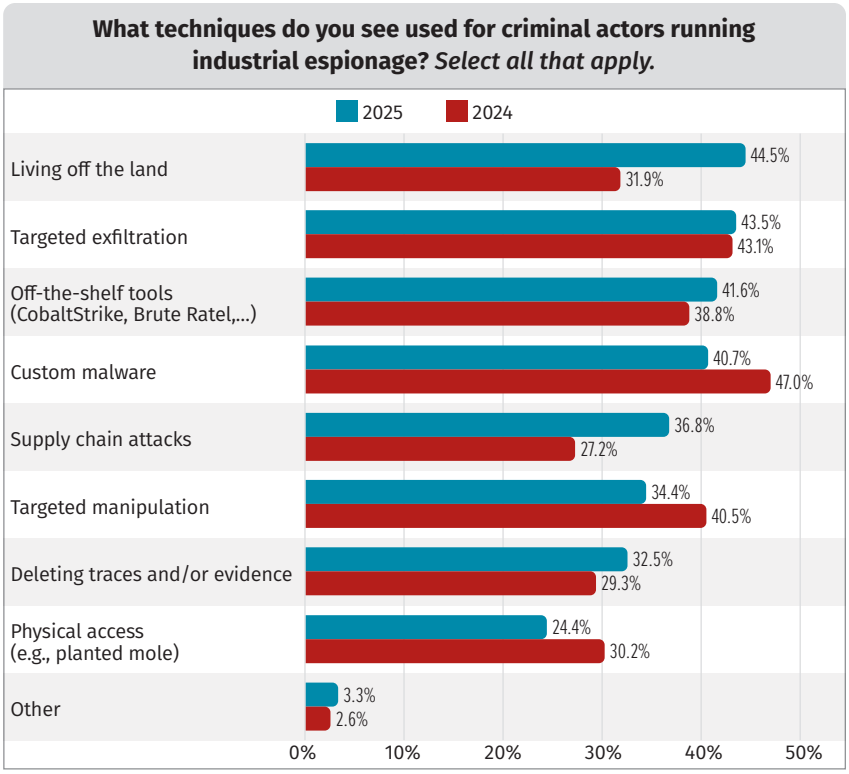


Figure 11. Espionage Techniques

Tracking Threat Actors in the Digital Wild West

This year, we see a notable shift toward automation in threat hunting strategies, with 37% of organizations now automatically generating new hunts based on evolving threat intelligence, up from 30% in 2024. However, those relying on an ad hoc approach have dropped from 64% in 2024 to 54% this year, suggesting a shift toward automation, likely due to a growing recognition of structured methodologies that allow for more automation. Interestingly, the number of organizations that do not factor in threat landscape changes at all has doubled, reaching 6%. Although this represents only a small number of respondents, it is a concerning trend given the speed at which threat actors adapt and change in response to defenses we may build around our organizations. As adversaries continue to adapt, the move toward proactive and automated responses is likely to be a key differentiator in threat hunting success.

Since last year, we have tried to understand where threat hunters are collecting information to aid them in their hunt missions, including sources of threat intelligence to develop their hunting scenarios. This year, we find a continued shift toward internal intelligence gathering, with 51% of organizations supplementing vendor-provided threat intelligence with their own research, up from 47% in 2024. Similarly, 34% primarily rely on their own intelligence, using vendor data only as a secondary source, reflecting an increase from 30% in the previous year. This trend suggests that organizations are striving for greater autonomy in their threat hunting efforts, recognizing the need to tailor intelligence to their unique threat landscape. It is also possible, with the significant increase in automation, that many cybersecurity teams are now experimenting with developing and managing their own threat intelligence, as it may have become easier over time. Conversely, those entirely dependent on vendors for threat landscape tracking have dropped to 10% (down from 14%), indicating that blind reliance on external intelligence may be seen as a growing risk. The number of organizations outright rejecting vendor intelligence remains at 4%, suggesting that although internal capability development is a priority, vendor insights remain valuable to most organizations.

DIY Threat Hunting—The Trend of Keeping It In-House

The percentage of organizations outsourcing their threat hunting dropped from 37% in 2024 to 30%, reflecting a shift toward building in-house threat hunting capabilities (see Figure 12). At the same time, the number of organizations managing threat hunting internally rose to 58%, a significant increase from 45% in 2024, suggesting that organizations are prioritizing internal expertise, visibility, and operational control over their security investigations.

Since 2021, when we began asking the question about organizations that outsource their threat hunting, we are starting to see a slow decline in organizations outsourcing threat hunting. This is a positive sign that organizations recognize that threat hunting is generally best conducted by internally knowledgeable staff who understand the organization's IT environment and likely better understand the organization's threat landscape. Despite the slow decline, outsourcing remains a viable strategy for many organizations, particularly those with limited in-house resources or those seeking to augment their teams with external expertise.

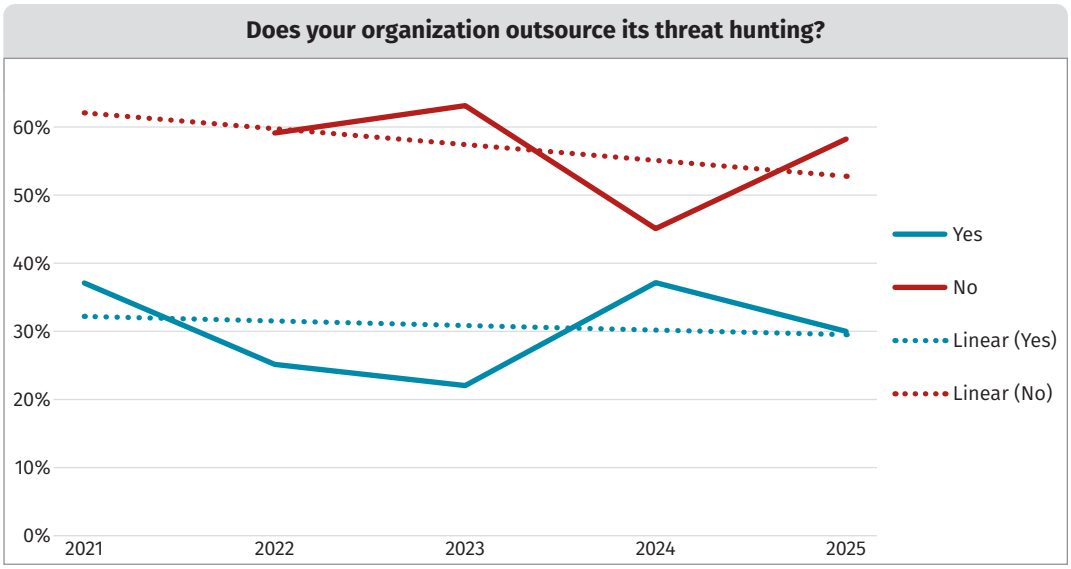


Figure 12. Year-Over-Year Outsourcing

You also may notice within this data that the organizations outsourcing their hunting and those not outsourcing it may not be moving accurately together. This is because two other options are offered. When we asked respondents this question, we included options for unknown (5% this year) and those who say outsourcing is not applicable (8% this year). This is why the data within Figure 12 may not appear to be moving in synchronization.

For those organizations that are outsourcing threat hunting, half of them (50%) reported that their threat hunting operations were defined through a collaborative effort between internal teams and outsourced providers, a slight increase from 45% in 2024 (see Figure 13). For organizations that are outsourcing their threat hunting, this does ensure that internal teams can retain strategic oversight while benefiting from the specialized skills and scalability offered by third-party providers. It is positive to see the reliance on external entities alone defining hunting parameters decreased to 30%, down from 35% in 2024. It's beneficial to see the move in this direction, with organizations giving their internal team greater control over how hunts are scoped and executed. At the end of the day, the internal team will know their environment better than a third party will.

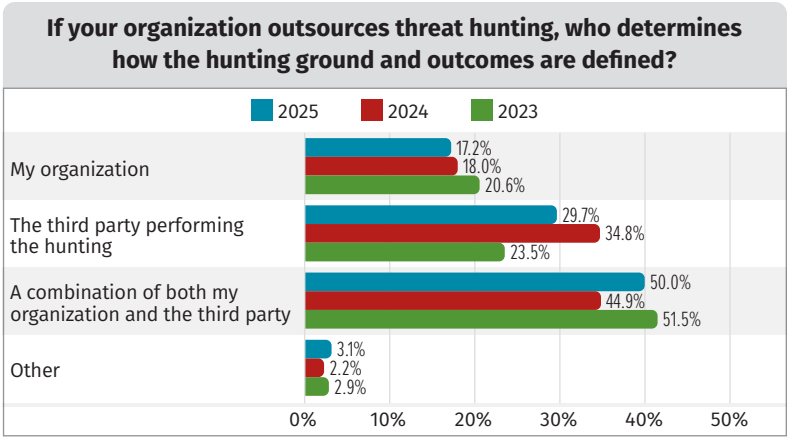


Figure 13. Outsourcing Approaches

On the other hand, those organizations being solely in charge of defining their own hunting parameters dropped slightly to 17%, continuing a downward trend from 18% in 2024 and 21% in 2023. This may reflect the increasing complexity of the threat landscape, where external expertise is seen as a valuable complement to in-house security operations. It's also possible that it is simply faster to use the skills of a third party, who may conduct threat hunting in many environments regularly. The data suggests that organizations aim to balance internal knowledge with external resources. For those organizations using a third party, this will ensure that hunts are tailored to their specific environments.

Organizations with substantial documentation to support their hunt missions, along with solid threat intelligence and documentation of their findings, generally have a more efficient threat hunting team. This year's data showed organizations demonstrated a shift toward greater reliance on internally built tools for tracking threat landscape insights, with the use of internally built tools rising to 48%, up from 33% in 2024 (see Figure 14).

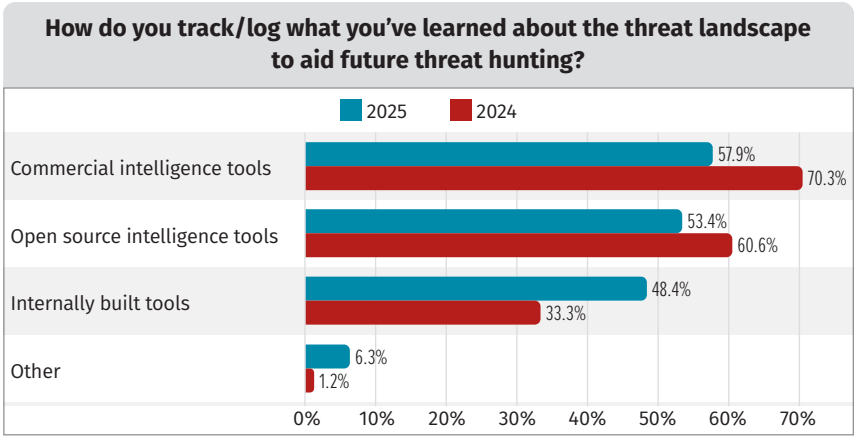


Figure 14. Threat Tracking Tools

This increase suggests that security teams invest more in tailored solutions that align closely with their specific environments and operational needs than in purchasing commercial tools or using open source tools for these tasks. At the same time, reliance on commercial intelligence tools declined to 58%, down from 70% in 2024. Similarly, the use of open source intelligence tools dropped to 53%, compared to 61% in 2024, though these tools remain a widely adopted resource. It is important to point out that when it comes to organizations building their own tooling, it is not always done to reduce costs. There is still the cost of staff resources to develop and maintain that tool internally. So, although organizations appear to be moving toward building their own tooling, this does not necessarily indicate they are moving to cut costs.

Threat hunting tools are always a hotly debated topic among professionals. Again this year, we have asked those conducting threat hunting what they consider their most critical tools to perform a hunt mission. Hopefully, this settles the debate, at least for another year. Here's the list, prioritized from most important to least:

1. **EDR/XDR—**This reinforces threat hunters' role as the frontline defense in detecting and responding to modern threats.
2. **SIEM—**This highlights the enduring value of centralized log management and correlation in uncovering malicious activity. There is some debate, though, that if you can collect logs, it's very possible you're able to generate automated detections against those logs, which may be a better long-term investment than conducting threat hunting on data you already have.
3. **NDR—**This indicates that organizations increasingly rely on network visibility.
4. **Built-in OS scripting (e.g., PowerShell, WMI, Bash, etc.)—**This showcases the necessity of native system capabilities for deeper investigations and possible areas of missing functionality within some of the EDR tools available.
5. **Full PCAP—**Once considered a cornerstone of forensic investigations, this tool ranked fifth, suggesting that although valuable, it is less frequently used in proactive hunts. This also may be a side effect of the sheer quantity of data that would need to be collected for full PCAP analysis.
6. **Native cloud logs—**Very surprisingly, this tool ranked sixth, which may show more of the challenges for threat hunters to use cloud logs. As discussed earlier in this report, cloud infrastructure is seen as the most challenging place for threat hunters to conduct a hunt mission.
7. **Memory analysis—**Memory analysis placed last, reinforcing the notion that it's just tough to perform threat hunting in memory with the tools available today and the sheer size of memory, not to mention the challenge with even accessing it with operating system vendors locking it down further.

Keeping Up with Evolving Threats

Organizations significantly increased their reliance on a diverse range of sources to stay ahead of evolving attacker techniques over the past year, with the most notable growth in vendor blogs and papers, rising from 59% in 2024 to 76% this year (see Figure 15). This shift underscores a growing dependence on vendor-led threat intelligence and research, likely due to their access to telemetry and specialized insights from multiple customers and a wide view of the threat landscape globally. Independent blogs and papers also saw a notable increase, reaching 69%, suggesting a continued trust in community-driven research and niche expertise.

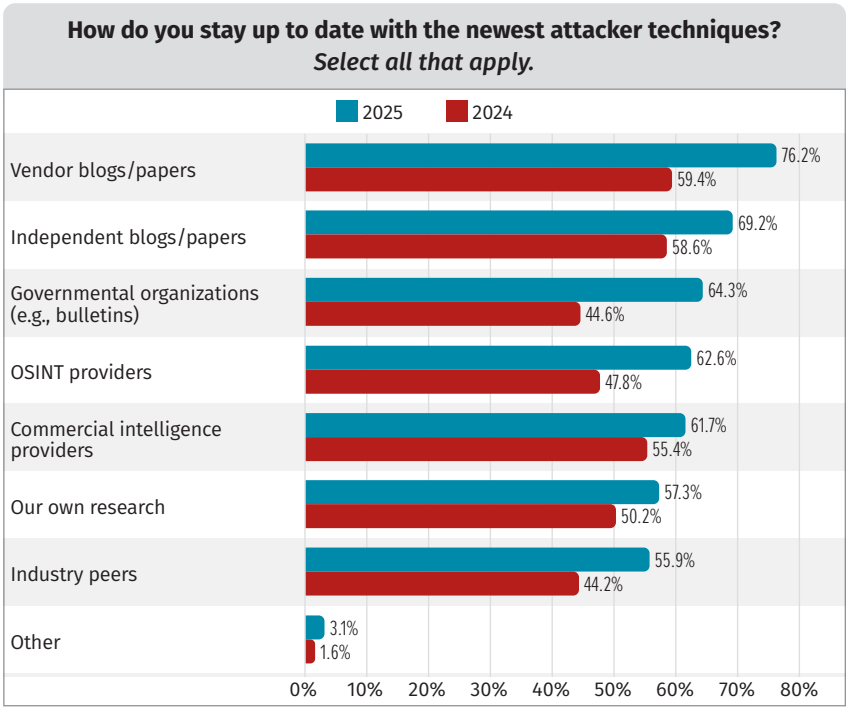


Figure 15. Sources of Intelligence

Governmental bulletins and advisories saw the most dramatic rise, jumping from 45% in 2024 to 64% this year, reflecting the growing credibility of government cybersecurity initiatives. This also may be a slight nod to government agencies providing more timely information to the cybersecurity community. Similarly, OSINT providers grew from 48% in 2024 to 63% this year. Commercial intelligence providers (62%), in-house research efforts (57%), and industry peer collaborations (56%) all gained traction, although they are all very close to each other in terms of how used they are by organizations for threat hunting. That means it's possible their ranking may move around slightly depending on the threats you may be trying to defend against.

The Roadblocks and Workarounds for Threat Hunts

Over the past year, the most pressing challenge in threat hunting has remained the shortage of skilled personnel, cited by 61% of respondents—an increase from 50% in 2024, but still lower than the 73% reported in 2023. This persistent issue highlights the ongoing struggle to recruit and retain trained professionals. Skilled personnel shortages are further exacerbated by budget constraints, which surged to 49%, up from 40% in 2024, reflecting organizations' financial challenges in expanding their threat hunting capabilities. This also may explain some of the findings around organizations trying to further automate threat hunting rather than use manual-based tooling or processes.

Although limitations in tools and technology (41%) and a lack of defined processes (39%) remain significant obstacles, both have slightly improved compared to previous years, suggesting that organizations are progressing in refining their methodologies and adopting better tooling. This is also further supported by some of the findings on how organizations are handling threat hunting methodology provided earlier in this report. Concerns around data, in terms of both its quality (41%) and the lack of standardized formats (28%), persist, indicating a broader issue in data integration for effective hunting. Management hesitancy (25%) and legal constraints (13%) remain lower-tier concerns, although both can impact long-term investment in proactive security strategies.

Integrating AI and machine learning (ML) into threat hunting tools remains a key priority, with 48% of organizations aiming to enhance automation and improve detection accuracy, an increase from 47% in 2024. Although AI and ML have not stood out in many of the other areas we asked respondents about, it appears that organizations still desire threat hunting teams to try and incorporate these tools. Efforts to expand internal expertise also have gained traction, with 43% of respondents seeking to increase the number of staff with investigative skills, up from 39% in 2024. This makes sense, given the challenges that our respondents have reported when it comes to retaining skilled personnel. We also see organizations prioritizing improvements in scalability (36%) and cloud-compatible tools (38%), reflecting the continued challenge these areas present as well as the continued shift by organizations toward cloud-based infrastructure. Data integration and normalization have seen noticeable growth, with 35% emphasizing better cross-source integration and 31% focusing on standardizing security data across devices. Notably, reducing "noise" in security data (27%) and improving intuitive data visualization (25%) have become more significant priorities, highlighting our industry's struggle with managing overwhelming amounts of telemetry.

Nearly 40% of organizations reported no planned changes in their investment in threat hunting staff in the next 12 months, a significant rise from 27% in 2024 (see Figure 16). This suggests that many organizations may have reached a steady state in their staffing levels or are focusing on optimizing existing resources rather than expanding.

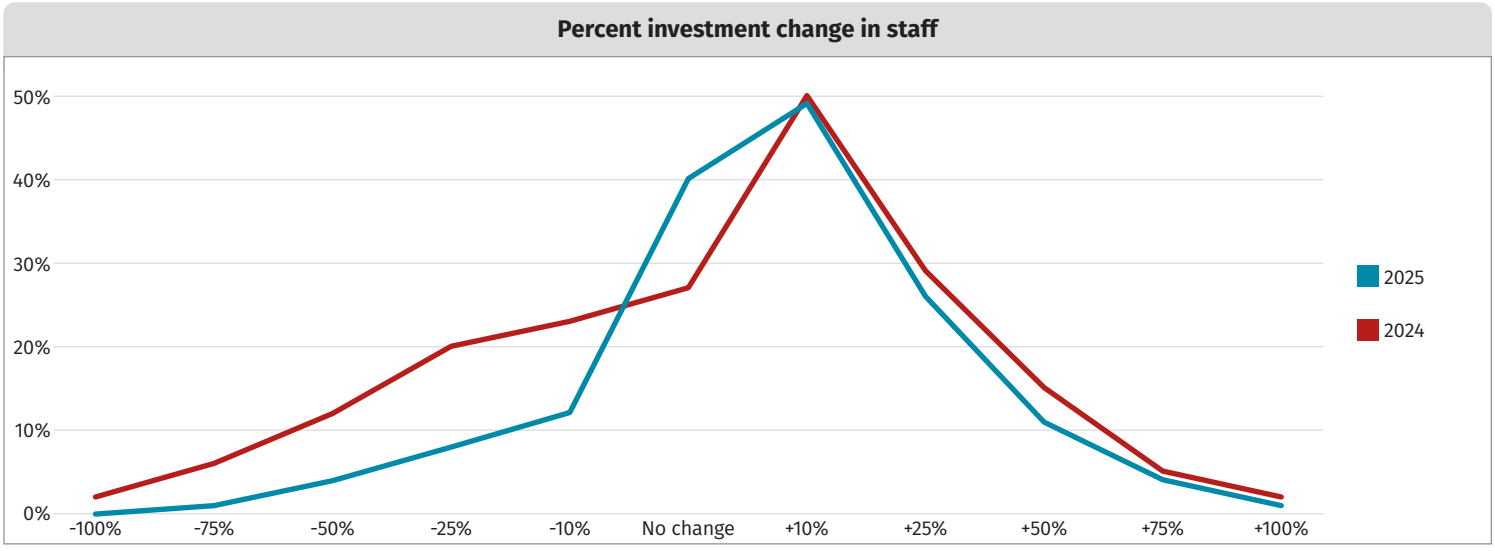


Figure 16. Staff Investment

However, there is still investment growth for some, with 22% of organizations planning at least a 10% staffing budget increase and at least 15% of organizations targeting a 25% increase, both remaining consistent with 2024 levels. Thankfully, planned reductions in staffing investment have significantly declined. Organizations planning more than a 75% cut dropped from 5% in 2024 to just over 1% this year, while those planning a 50% reduction fell to 2% this year. Hopefully, this indicates that fewer organizations are scaling back their threat hunting capabilities, reinforcing the notion that threat hunting remains a strategic priority despite economic uncertainties.

When it comes to investing in tooling for threat hunting, 31% of organizations reported no planned changes in their tooling investment, a notable increase from 22% in 2024 (see Figure 17). This reflects a similar increase in no changes to staffing investment previously mentioned. Despite this, a substantial portion (21%) still plan a 10% increase, and another 20% of organizations anticipate a 25% investment increase, showing a sustained commitment to improving capabilities.

Notably, reductions in investment have significantly diminished this year. No organizations reported an investment reduction of 75% for their threat hunting tooling, and those planning a 50% reduction dropped from 4% in 2024 to just 1% this year. This is starting to show that budget cuts for threat hunt tooling are becoming increasingly rare. However, it's crucial for organizations to remember that they need to have skilled staff to run their shiny new tools as well.

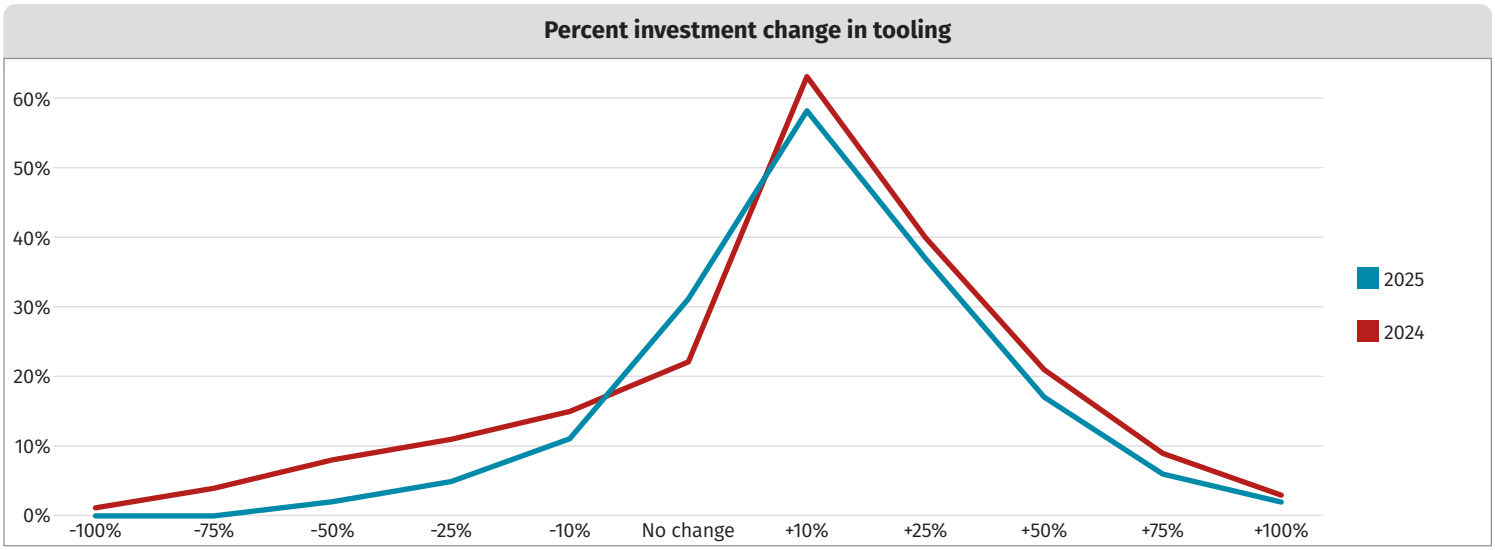


Figure 17. Tool Investment

Conclusion

The 2025 SANS Threat Hunting Survey highlights the ongoing evolution of threat hunting as organizations refine their methodologies, enhance their tooling, and balance internal expertise with outsourced support. Although the formalization of methodologies has fluctuated, organizations strongly prefer agility, ensuring they can respond to an increasingly dynamic threat landscape. This year's findings reinforce that threat hunting is not a one-size-fits-all approach, nor is it providing benefits only for large corporate enterprises, as we also see small businesses benefit from threat hunting. Some organizations continue to rely on structured frameworks, while others lean toward hypothesis-driven and adaptive methods to identify threats.

The investment trends uncovered this year suggest that organizations remain committed to strengthening their threat hunting capabilities despite what might appear to be incoming economic constraints in the next 12 months. Although staffing levels have stabilized for many, there is a continued push for automation, improved data integration, and better investigative tooling. The rise of internally built solutions indicates a shift toward customized approaches, complementing commercial and open source options. At the same time, organizations are broadening their intelligence sources, with vendor research, OSINT providers, and governmental bulletins all playing a critical role in staying ahead of adversary tactics.

Organizations must continue evolving their detection and hunting strategies as threat actors refine their techniques, from nation-state espionage to ransomware and supply chain compromises. The findings demonstrate that while progress is being made, challenges persist, particularly in cloud visibility, skilled personnel shortages, and measuring the impact of threat hunting programs. However, the overall trajectory for threat hunting into the future remains positive, with more organizations recognizing the value of proactive threat hunting as a critical pillar of their cybersecurity defenses.

Sponsor

SANS would like to thank this survey's sponsor:

Google Cloud Security

SANS | Research Program

Product Briefings for Threat Hunting

The 2025 Threat Hunting Survey represents the latest edition of SANS Institute's poll of security professionals. The sponsors of this year's survey all offer advanced capabilities that we believe will be of interest to SANS' clients, and, for this reason, we're presenting the following product briefing on a relevant offering.

Google Cloud
Security

SANS | Research Program

Product Briefing

Threat Hunting with Google Threat Intelligence:
Insights from the 2025 SANS Institute Threat Hunting Survey

March 2025 | By Sophie Keats

Managing the overwhelming influx of threat feeds and alerts is a constant struggle for security teams. Prioritizing threats can feel like a game of chance, and time is precious for security teams. To maintain an advantage over potential threats, today's organizations need a proactive threat management stance.

Google Threat Intelligence: Actionable, AI-Driven Insights

Google Threat Intelligence delivers comprehensive and timely threat intelligence that enhances visibility and response capabilities for security teams worldwide. Supercharged by AI-driven insights and powered by Mandiant expertise, VirusTotal crowdsourced intelligence, and Google insights, organizations can proactively set their security strategy and respond to threats in minutes. See Figure 1.

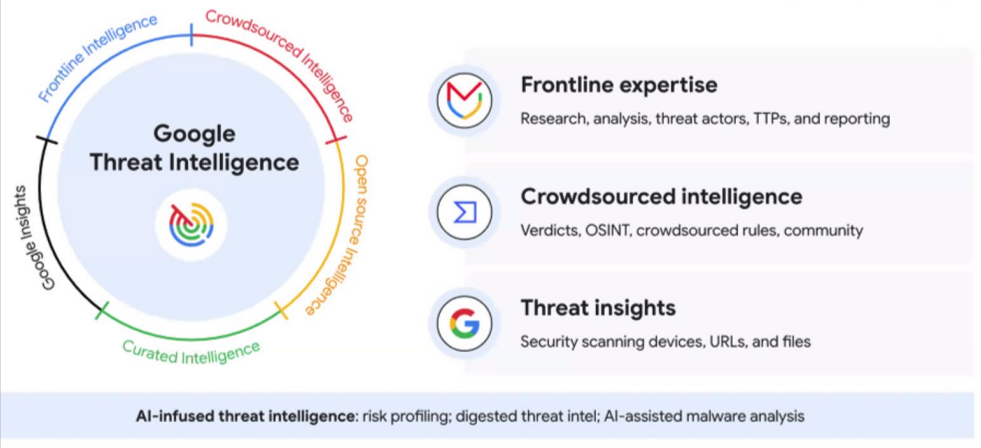
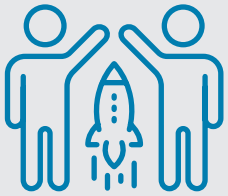


Figure 1. Google Threat Intelligence Features

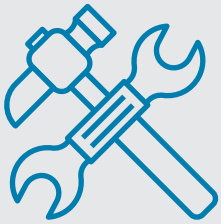
Key capabilities of Google Threat Intelligence:

- **Vendor-agnostic integration—**Easily connects with SIEM, SOAR, and other security tools.
- **AI-powered threat intelligence—**Saves time and reduces complexity when researching threats. Leverages Gemini, an always-on AI collaborator, to help distill intel information and generate concise intelligence summaries.
- **Comprehensive threat actor tracking—**Maps tactics, techniques, and procedures (TTPs) using MITRE ATT&CK,™ enabling proactive security measures.
- **Automated alert prioritization and indicators of compromise (IoC) enrichment—**Reduces alert fatigue by correlating threat intelligence with real-world attack data.

Key Findings



61% of respondents cite skilled staffing shortages as a primary barrier to success.



76% of surveyed organizations report seeing Living Off the Land (LOTL) techniques in nation-state attacks, unchanged from last year.



Organizations increasing staffing investment by 10% or more sit at 40%, with 31% making no planned changes.

- **Advanced threat hunting—**Supports custom workflows, YARA rules, and interactive threat analysis for enhanced detection.
- **External threat detection—**Monitors for phishing campaigns, brand impersonation, and leaked credentials to prevent exploitation.
- **Vulnerability intelligence—**Prioritizes patching based on risk ratings, exploitations state, and vulnerable products, ensuring a risk-based security strategy.

Google Threat Intelligence offers exceptional visibility into the global threat landscape. The platform highlights threat actors and details phishing campaigns that spread new malware. Users can evaluate malicious files to understand their behavior and code, and employ expert, crowdsourced, or automated detection rules to hunt for suspicious activities.

It provides attack narratives that show if malware is being used across different campaigns and allows for natural language queries to access AI-powered summaries from Mandiant reports and open source intelligence (OSINT). Users also can track new threat actors in one place.

Additionally, the system automatically generates reports and machine-readable intelligence about threat actors and their tactics, which can be shared with executives and security operations center (SOC) teams to facilitate informed threat hunting.

Google Threat Intelligence provides diverse intel sources, providing unmatched depth and breadth (see Figure 2). The solution empowers incident response and forensic investigators with in-depth and actionable insights for effective threat analysis. The tool features exceptional technical pivoting capabilities, a blend of curated and crowd-sourced threat intelligence, and interactive graph visualizations. Security teams can swiftly evaluate incident severity and uncover additional IoCs, context, and attribution.

Key benefits of Google Threat Intelligence:

- **Unmatched threat visibility—**Leverages Google-scale data for real-time threat detection.
- **Faster incident response—**Combines AI insights with expert-driven intelligence for rapid response.
- **Proactive threat hunting—**Supports custom detection rules, advanced analytics, and MITRE ATT&CK mapping.
- **AI-driven summaries—**Gemini AI turns vast amounts of threat intelligence into digestible insights.
- **Seamless security integration—**Uses existing security tools to enhance visibility and response.
- **Threat actor attribution—**Tracks adversaries, tactics, techniques, and procedures (TTPs), as well as emerging attack campaigns.
- **Optimized resource allocation—**Helps security teams prioritize efforts based on real-world attack data.
- **Expert support from Mandiant—**Provides direct access to intelligence analysts for guidance and training.

According to the 2025 SANS Threat Hunting Survey,[1] organizations are increasingly shifting to proactive security strategies, but challenges remain. More than half of organizations believe that staffing shortages are the biggest challenge to improving threat detection in cybersecurity. Additionally, 76% of those surveyed have observed Living Off the Land (LOTL) techniques in nation-state attacks, a statistic that has remained steady over the past year. In response to these evolving threats, some organizations are increasing their hiring and training efforts, while others have no plans to make any changes to their security teams.

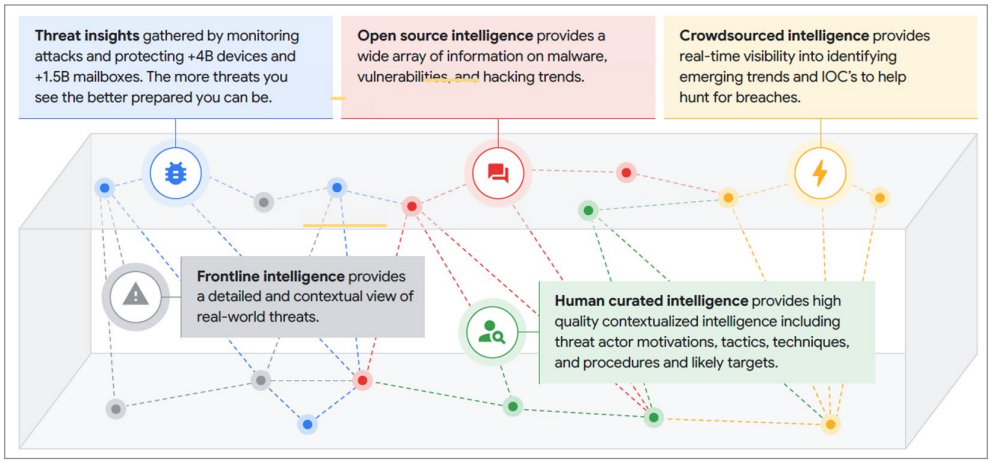


Figure 2. Sources for Google Threat Intelligence

Google Threat Intelligence serves as a vital partner for security teams. It can significantly enhance your organization's capacity to proactively defend against cyber threats. By enabling rapid responses to emerging risks, it empowers teams to effectively manage and mitigate risk. As a result, organizations can rise to the challenge and actively combat the ever-evolving waves of cyber threats.

To learn more about Google's comprehensive and timely threat intelligence solution, visit **https://cloud.google.com/security/products/threat-intelligence**.

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.

[1] "SANS 2025 Threat Hunting Survey: Advancements in Threat Hunting Amid AI and Cloud Challenges," March 2025, www.sans.org/white-papers/sans-2025-threat-hunting-survey-advancements-threat-hunting-amid-ai-cloud-challenges