censys

The 2024 State of Threat Hunting

How Threat Hunters Are Adapting to Automation and the Rise of AI

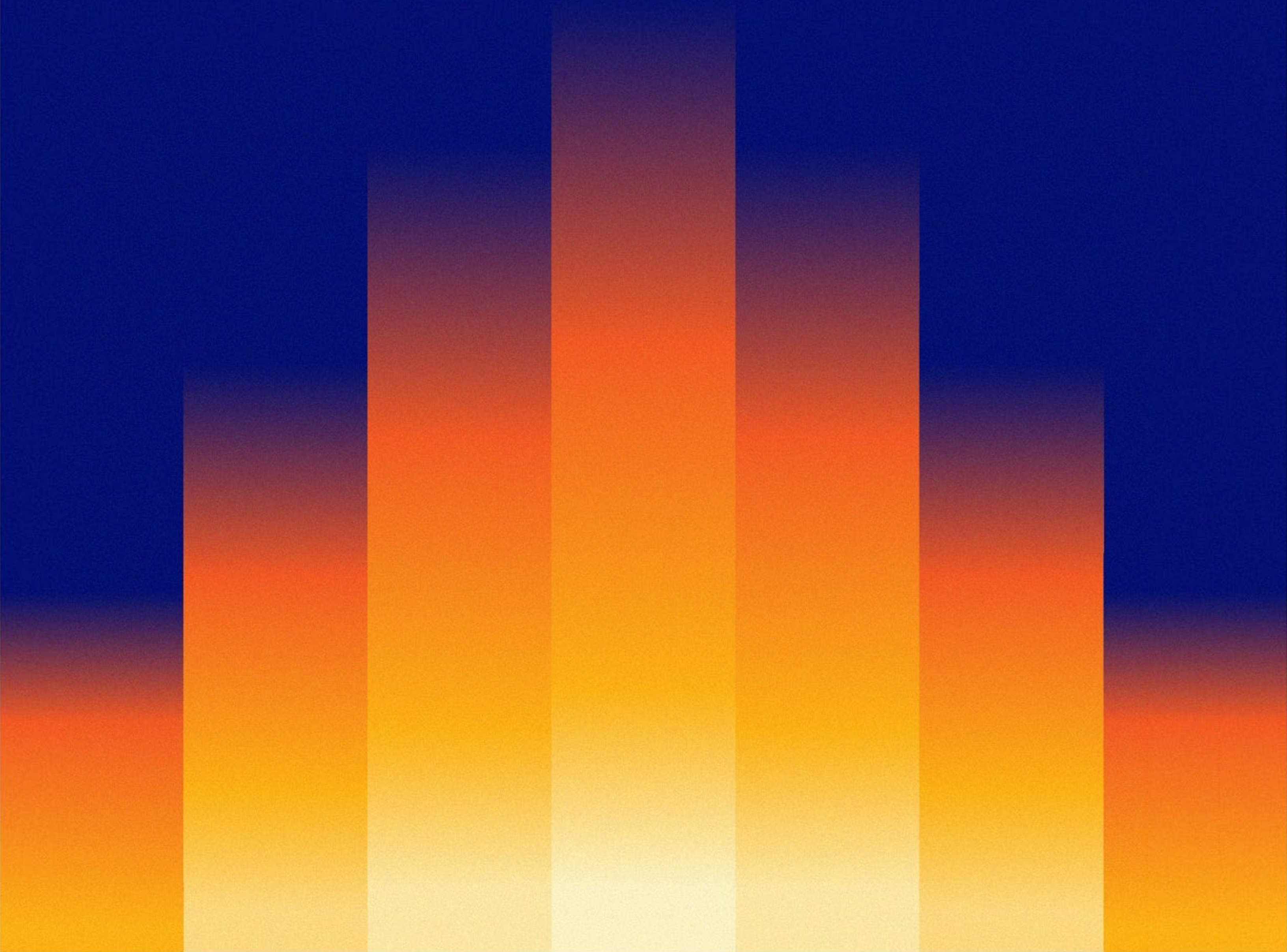

Table of Contents

Methodology

This late 2023 study utilized a blind quantitative survey to gather data from threat hunting practitioners about their current job responsibilities and work experiences. The study included respondents from both North America and Western Europe, professionally recruited from a well-screened panel of qualified technology workers matching titles specific to threat hunters.

A total of 214 responses were collected from across a broad range of industry sectors and various-sized commercial and public sector organizations. The great majority of respondents perform both offensive and defensive threat hunting as part of their work. Sixty percent are members of small threat hunting teams (no more than 10 people) – some even working alone – reflecting the typical organizational challenges of lean staffing for these kinds of necessary but high stress jobs.

Respondent Breakout

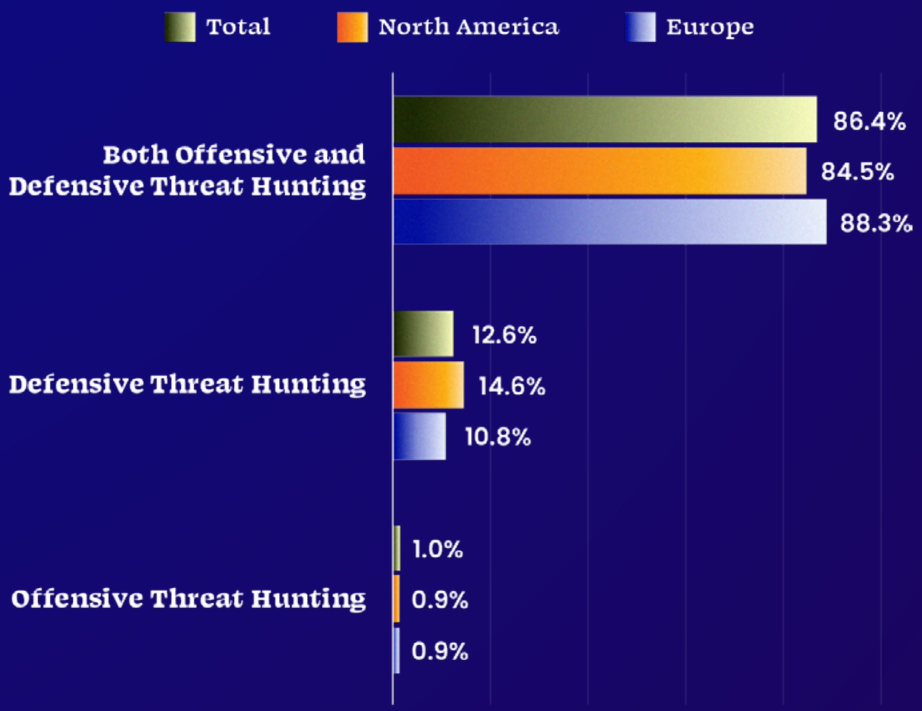

Figure 1: Scope of Threat Hunting Responsibilities

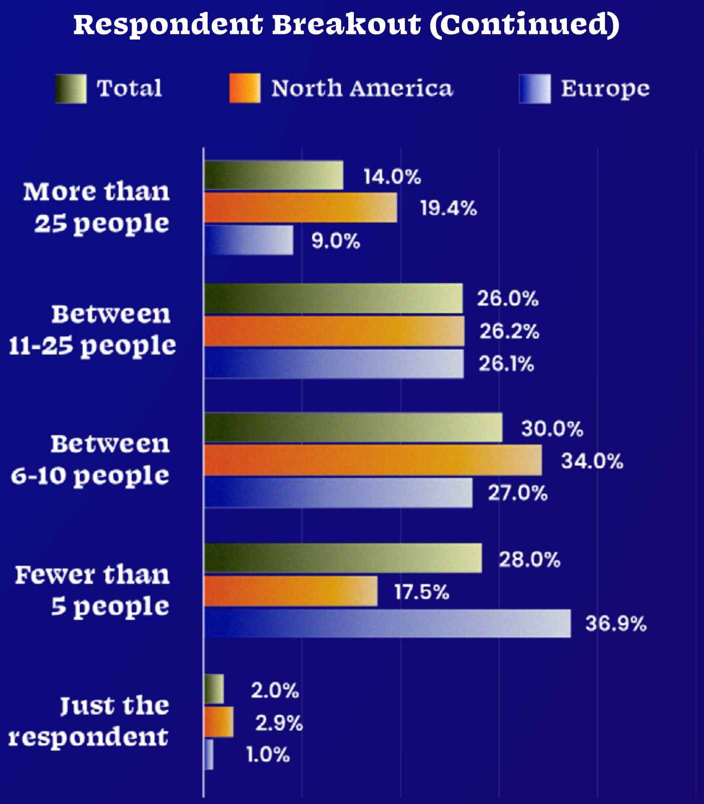

Figure 2: Size of Threat Hunting Team

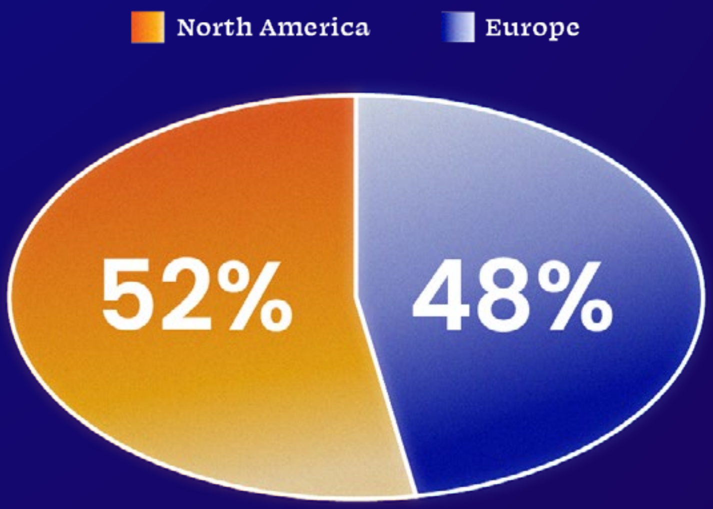

Figure 3: Primary Geographic Work Location

SECTION 1

Key Findings

Introduction

Threat hunters are tasked with the exceptionally challenging job of finding threats before threats find them. It's a tall order, and in many ways, the stakes have never been higher. Attackers are more sophisticated, attacks are more frequent, and the consequences of a successful breach more dire.[1]

In addition to navigating this increasingly aggressive threat environment, many of today's threat hunters are identifying best practices as they go along, relying on an array of different tools and techniques. As a traditionally individualistic, unstructured, and self-taught endeavor, it's no surprise that threat hunting lacks a standard set of practices for newcomers to follow.

While in the past threat hunting may have been seen as the focus of solo experts with the time and interest to hone their craft, today threat hunting is increasingly part of corporate cybersecurity programs tasked to practitioners with competing job priorities.

What does threat hunting look like for these front line defenders on corporate teams, and how are they navigating the challenges before them? Do these practitioners have the tools and training they need to be successful?

To find out, our *State of Threat Hunting* research surveyed over 200 corporate security practitioners across organizations in the United States and Europe with threat hunting responsibilities.

The report raises a number of interesting findings, which you'll read about in the pages to come. **However, one throughline that emerges is the need for reliable threat intelligence and its impact on threat hunters' ability to do their jobs well.** Threat intelligence, or lack thereof, is a commonality across the top challenges respondents identified. Access to threat intelligence also affects nearly every aspect of how respondents say they do their jobs.

As threat hunters navigate a dicey external landscape and make due with internal resource gaps and open source tools, progress in any direction will be contingent upon their ability to access accurate, reliable threat intelligence.

[1] IBM, 2023 Cost of Data Breach Report

Key Findings

Current threat hunting is as much art as science

Consistency and standardization in the threat hunting discipline are lacking. Threat hunters use a wide variety of methods and approaches. While there are many criteria that contribute to their confidence in threat assessments, there is no single input that provides enough certainty that an assessment is completely accurate. That void leaves threat hunters applying their own mix of tools and experiences to perform their ongoing work. As a result, a threat hunter's process is often unique, making it challenging to replicate in a corporate environment.

Many threat hunters believe that the discipline would be better served through a common, proven, and accepted standard for assessments, based on reliable threat intelligence, that could improve threat hunters' confidence and provide greater assurance to business decision-makers.

Threat hunting toolkits are a work-in-progress, but AI is a promising addition

Roughly a third of respondents are now using automated tools like Attack Surface Management (ASM) and Managed Detection and Response (MDR), in addition to more traditional tools. An overwhelming majority of respondents also say they've started using AI tools to aid their threat investigations, and see them as beneficial. Though many threat hunters are embracing these new technologies, there's still progress to be made. Access to better threat hunting tools tops the wish list for what would improve threat hunters' responsibilities, strengthening the case for automating many time-consuming and painstaking tasks. Leveraging more automated, AI-driven tools powered by superior threat intelligence could also lead to improved job satisfaction and less stress for these front-line defenders.

False positives pose a formidable challenge

An unfortunate fact of threat-hunting life: everyone experiences at least some false positives in their results. In fact, 32% of respondents found over 20% of their threat hunting results in the last six to 12 months were false positives. This reflects significant wasted resources and effort, and underscores threat hunters' need for more accurate threat intelligence. While it's not possible to completely eliminate these misleading results, decreasing them is another item on respondents' wish list.

Exposed assets are a pervasive risk

Almost everyone finds previously unknown assets during threat hunting, and 73% of respondents find them frequently or always during their threat hunting work. These forgotten, never documented, or even unapproved connections pose big risks to organizations. Exposed, unmonitored assets are attractive opportunities for adversaries to exploit, which is why identifying them is a critical responsibility for threat hunters on corporate teams. As organizations' digital footprints continue to expand, gaining a complete view of all of the assets that comprise their external attack surfaces will require near real-time discovery and monitoring. Yet, many threat hunters and their teams seem to lack the tools and data sources that would help them identify and monitor these unknown connections on a more continuous basis.

Threat hunters don't feel fully confident communicating to business stakeholders.

Threat hunters on corporate teams have the added responsibility of communicating out their findings to stakeholders across the organization. Many of these stakeholders don't understand or speak threat hunting parlance, which makes it even more critical for threat hunters to find ways to effectively share information with these groups. Unfortunately, respondents have work to do on this front. Respondents' confidence in communicating decreases the farther they get from their direct inner circle – to the point where less than half feel fully confident explaining threat hunting results to legal or public relations personnel, who may need to be informed enough to explain the situation to organizational outsiders. While respondents did not designate guidance to help them improve communication skills as a top priority, their lower confidence in this domain shows there is certainly a need. Addressing the prevalence of false positives and the need for better threat hunting tools may help respondents feel more confident in their findings, and in turn allow them to communicate more effectively to stakeholders.

SECTION 2

Detailed Findings

Threat Hunting Practices Vary Significantly

Threat hunting activities are often not proactive

While threat hunting is part of normal security responsibilities for the great majority of respondents, certain events trigger targeted action. As mentioned previously, threat hunting is often a single part of a security practitioner's day-to-day responsibilities, and as a result, may be put on the backburner when competing priorities inevitably arise.

When asked the question "what prompts your threat hunting activities?", our respondents mentioned a variety of triggers like known indicators, notifications of new zero days, new CVEs, and irregularities. This indicates that for many threat hunters, the act of threat hunting is not proactive and instead occurs after an incident or issue arises.

Another interesting statistic of note - 47% of global respondents and 60% of North American respondents report that they start an investigation when irregularities are detected by advanced analytics and machine learning, indicating growing adoption and acceptance of these tools across the threat hunting community.

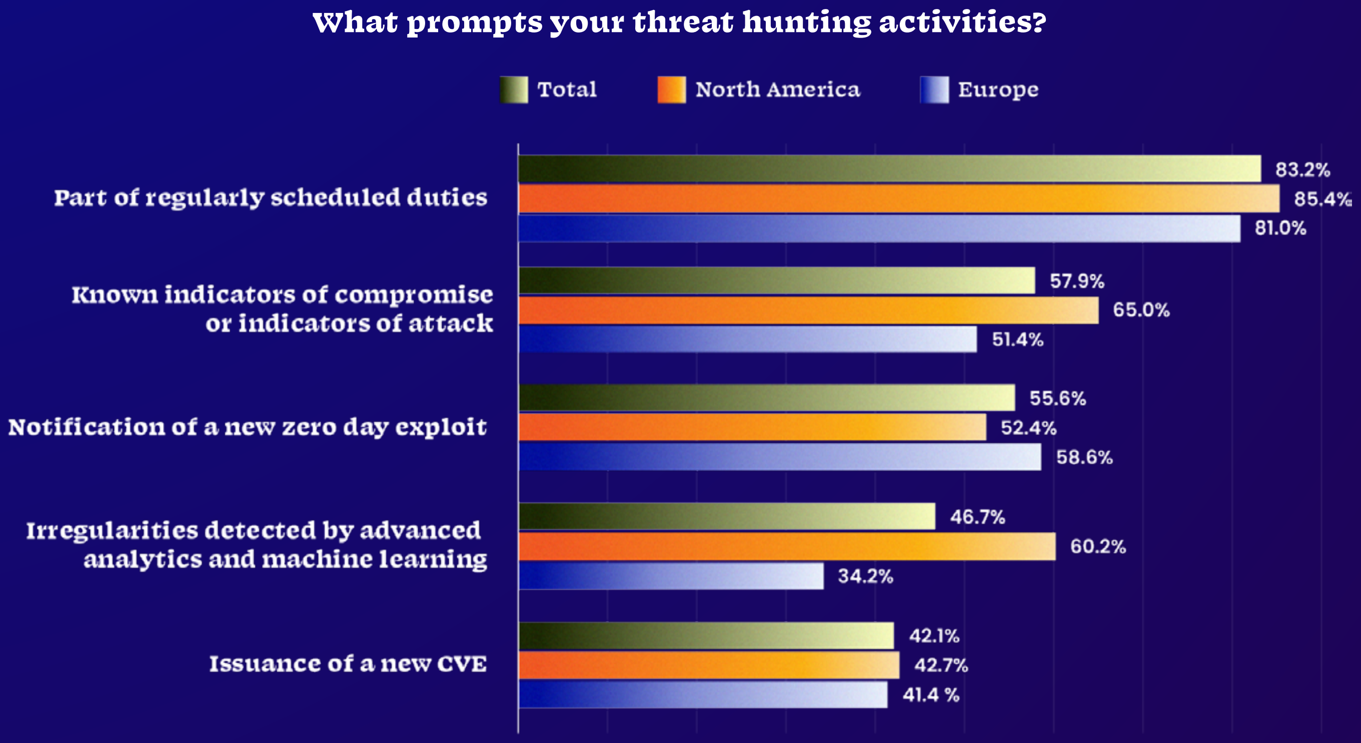

Figure 4: What Prompts Threat Hunting

Lack of proactive threat hunting activity is further reflected in threat hunters' response to how frequently they implement formal threat hunting processes. Only about 30% of global respondents say their organization continuously implements a formal threat hunting process for tracking and cataloging all connections that comprise its attack surface. Of this group, respondents in North America were more likely than their counterparts in Europe to say they conducted activities on a continuous basis. This may be explained by the higher volume of threats that threat hunters in North America encounter.

Third-party research finds that the United States also experiences the highest number of cyberattacks in the world – *twice as many as Europe.*[2] These threat hunters may simply have a greater need for constant vigilance given the volume of threats. When looking at these responses by team size, those on teams of 25+ were the most likely to say they continuously implement a formal process, suggesting that the larger an organization and team is, the more likely they are to invest in more sophisticated threat hunting methodologies.

Remarkably, 18.3% of global respondents are only implementing a process on a monthly basis – a frequency that pales in comparison to the rapid pace at which attackers look to exploit exposures. Studies have shown that approximately every three minutes, unknown and potentially malicious entities are performing their own scans of the internet to potentially identify opportunities for exploit.[3] Though tracking and cataloging connections may be only one of many threat hunting processes, responses here suggest opportunity for more continuous, automated processes across the board.

[2] Imperva, Cyber Threat Index, 2022

[3] Greynoise, A Week in the Life of a Benign Scanner, 2022

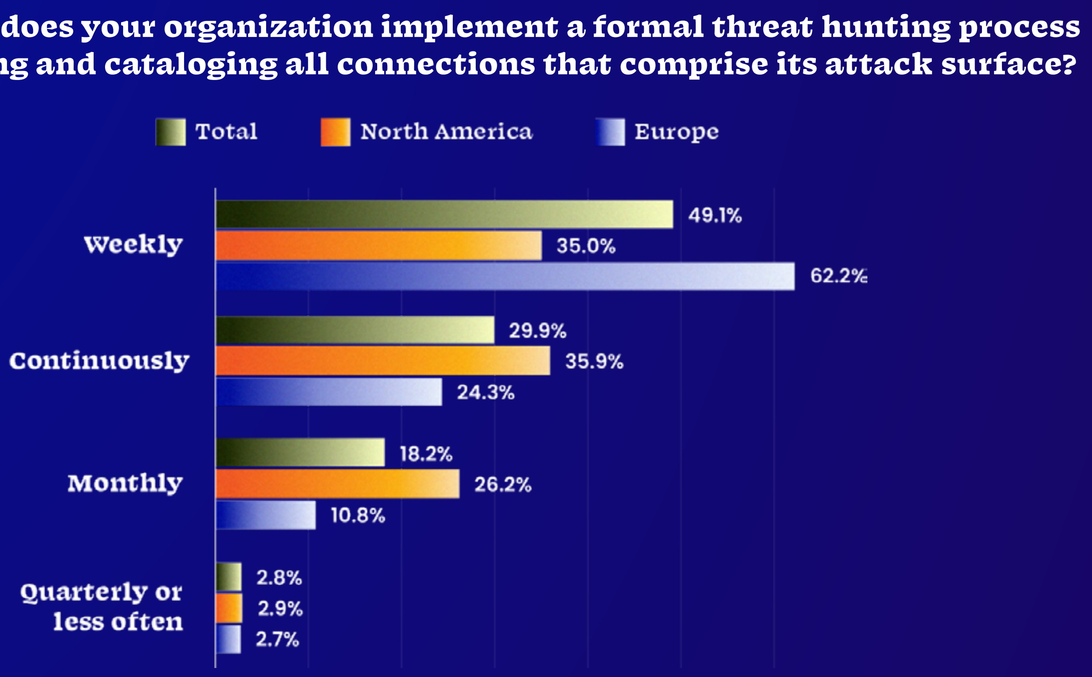

Figure 5: Frequency of Tracking/Cataloging Connections in the Attack Surface

North American threat hunters are more likely to trigger a hunt based on world events

During their threat hunting efforts, a majority of respondents look for specific indicators of intent that increase risk. Most obvious are issues flagged in particular networks, but macro issues, like disruptive world events, also escalate concern.

Interestingly, Americans look for such external indicators more than Europeans, and show greater concern for several triggers like world events and data breaches. Americans' outward-looking focus may be the result of a number of factors, including that given its role on the world stage, the United States is often more involved in, or directly impacted by, geopolitical events. As mentioned earlier, the United States also experiences the highest number of cyberattacks in the world – twice as many as Europe.[4] This research also indicates that when measured by the Cybersecurity Exposure Index, Europe has the fewest exposures per country of any region in the world - perhaps a consequence of its stricter data privacy laws, like the GDPR, which could push threat hunters to be more proactive about managing exposures.[5]

4 & 5 Imperva, Cyber Threat Index, 2022

In North America, however, the higher volume of threats may prompt threat hunters here to take a more expansive view of the threat landscape, and look beyond the internal indicators that threat hunters in Europe lean on more heavily.

Moving from the macro indicators of world events to the micro indicators of network anomalies, threat hunters were also asked about bitcoin nodes, and whether their unexpected presence in a network serves as an indicator of malicious intent. Bitcoin has historically been bad actors' bank of choice, and was used in nearly all ransomware attacks in 2023.[6] Despite the persistent increase in ransomware attacks around the world,[7] only 20% of threat hunters say that they look for unexpected bitcoin nodes as indicators of malicious intent. However, it is still likely that discovering a bitcoin node combined with an additional indicator like a suspicious access request would be perceived as a much more urgent issue.

Which if any indicators of intent do you look for as part of your threat hunting efforts?

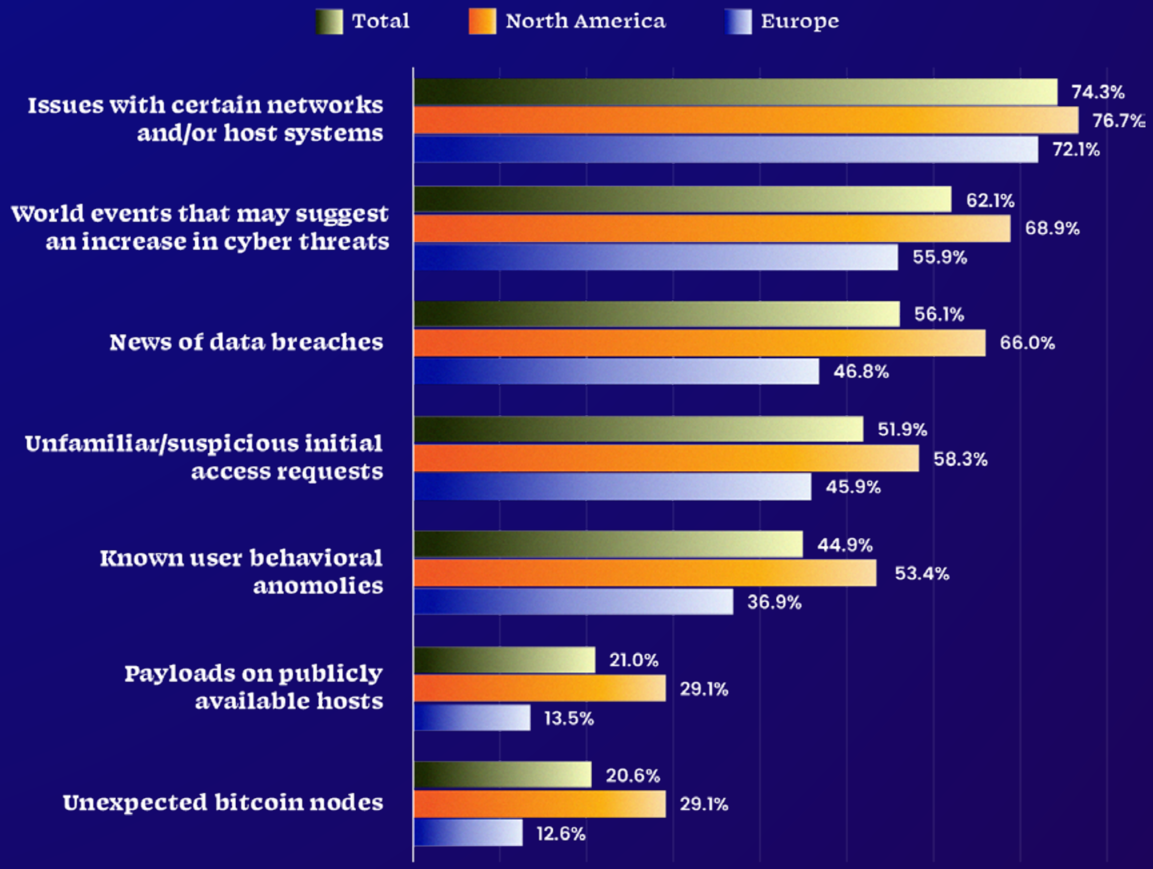

Figure 6: Indicators of Intent Sought by Threat Hunters

[6] & [7] Reuters, Crypto ransom attacks rise in first half of 2023

Data accuracy is the most important factor in assessment confidence

When asked about the criteria that influenced their level of confidence in threat assessments, the largest percentage of respondents said that accuracy of threat data is most important. This was particularly true for threat hunters in Europe, who were more likely than threat hunters in North America to say that data accuracy is very important to their confidence in threat assessments. Greater focus on data accuracy in Europe may be the result of the EU's more stringent regulations on data, which, among other aspects, emphasize corporate accountability.[8]

Interestingly, the largest percentage of threat hunters in North America (65%) said that access to a backward-looking timeframe or access to historical lookup is very important to their assessment confidence. Given the higher frequency of attacks in North America, greater interest in historical data may speak to the need for these threat hunters to acquire as much additional context as possible about adversaries' tactics and patterns, and identify commonalities across successful attacks.

Beyond these takeaways, responses indicate that threat hunters still rely on a mix of factors, further suggesting a lack of domain leadership or a standardized approach that could benefit the entire threat hunting discipline.

[8] EU, What Is GDPR?, 2020

> **Threat hunting is more of an art for me. It's a combination of personal experience with false positives, plus intuition and sharp eyes, when you are able to suspect connections between things that are not explicitly connected.**
>
> – Threat Hunter, Mid-Sized Organization

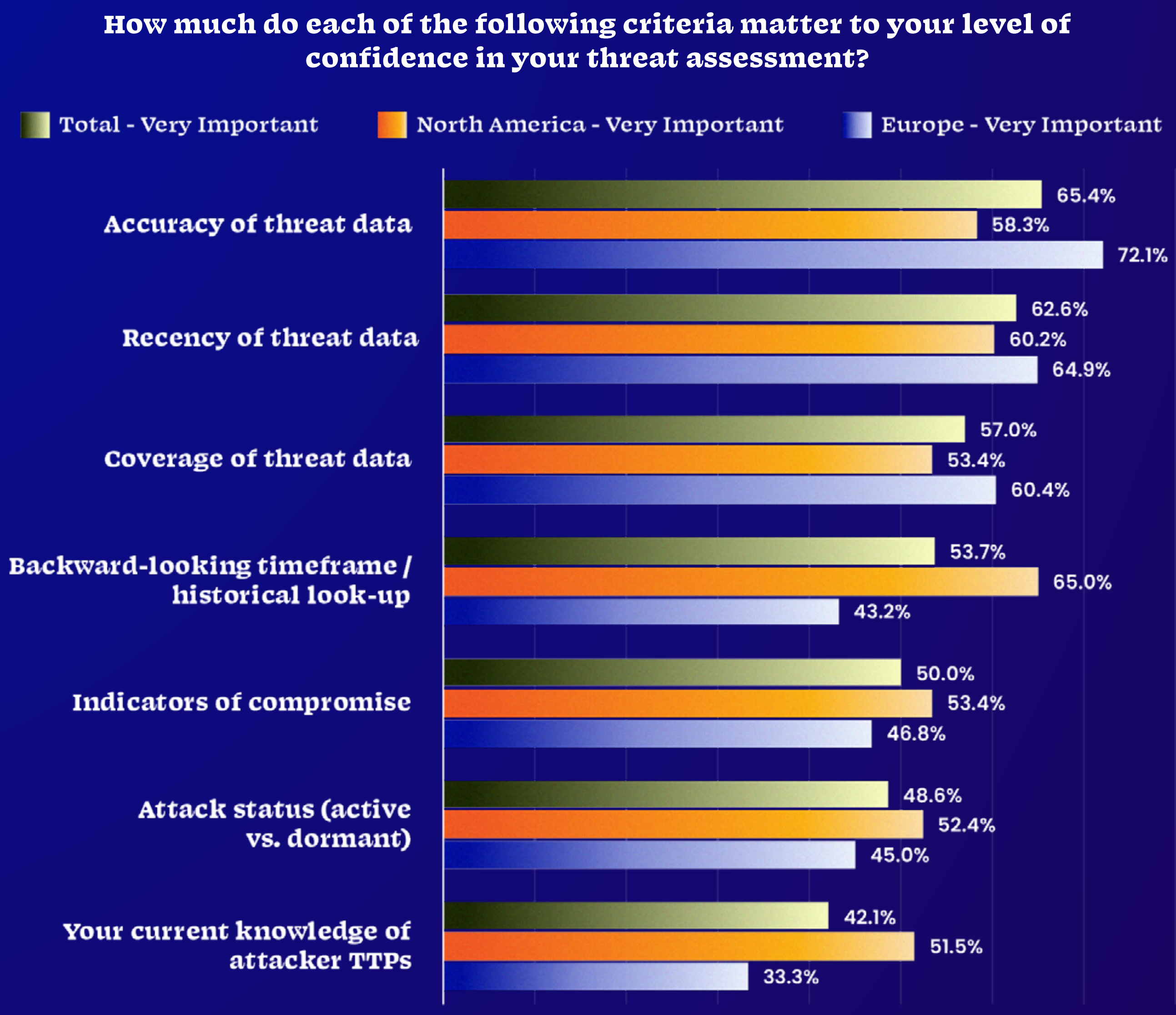

Figure 7: Criteria for Confidence in Threat Assessments

Automation and Artificial Intelligence Are Becoming More Valuable to Threat Hunters

Most threat hunters rely on traditional tools, but North American threat hunters use more automation

Respondents use a wide range of tools for threat hunting, with the great majority using traditional security monitoring tools. **Newer tools that leverage automation, like Attack Surface Management (ASM) and Managed Detection and Response (MDR), are more widely adopted by threat hunters in North America than by their European counterparts.** Nearly 50% of threat hunters in North America are using ASM tools, whereas only 20% of threat hunters in Europe say the same. This adoption disparity can also be seen in respondents' answers about search tools, which are used more than three times as often by threat hunters in North America.

Though the reasoning for this disparity in tech adoption isn't clear from this report's findings, it may be due in part to the different threat volumes faced by each region. As mentioned earlier in this report, the United States experiences on average twice as many threats as Europe, which may explain the interest in and need for more automated security solutions. Additionally, in the U.S. the Biden Administration recently set forth explicit directives for affected organizations to implement continuous asset discovery, which can be achieved through ASM tools.[9] These requirements are mandatory for federal organizations and are strongly recommended to civilian organizations.

Further, differences in North American and European toolkits may be the result of distinct attitudes about cybersecurity. Reporting suggests that the U.S. sees cybersecurity as a matter of national security, whereas countries in Europe view cybersecurity as a means to "protect privacy and ward off economic danger."[10] Though both points of view underscore the need for stringent cybersecurity, U.S. attitudes may prompt additional focus on and funding for advanced security tools.

[9] CISA, BOD 23-01, 2022

[10] CEPA.org, Europe Upgrades Its Cybersecurity Arsenal, 2023

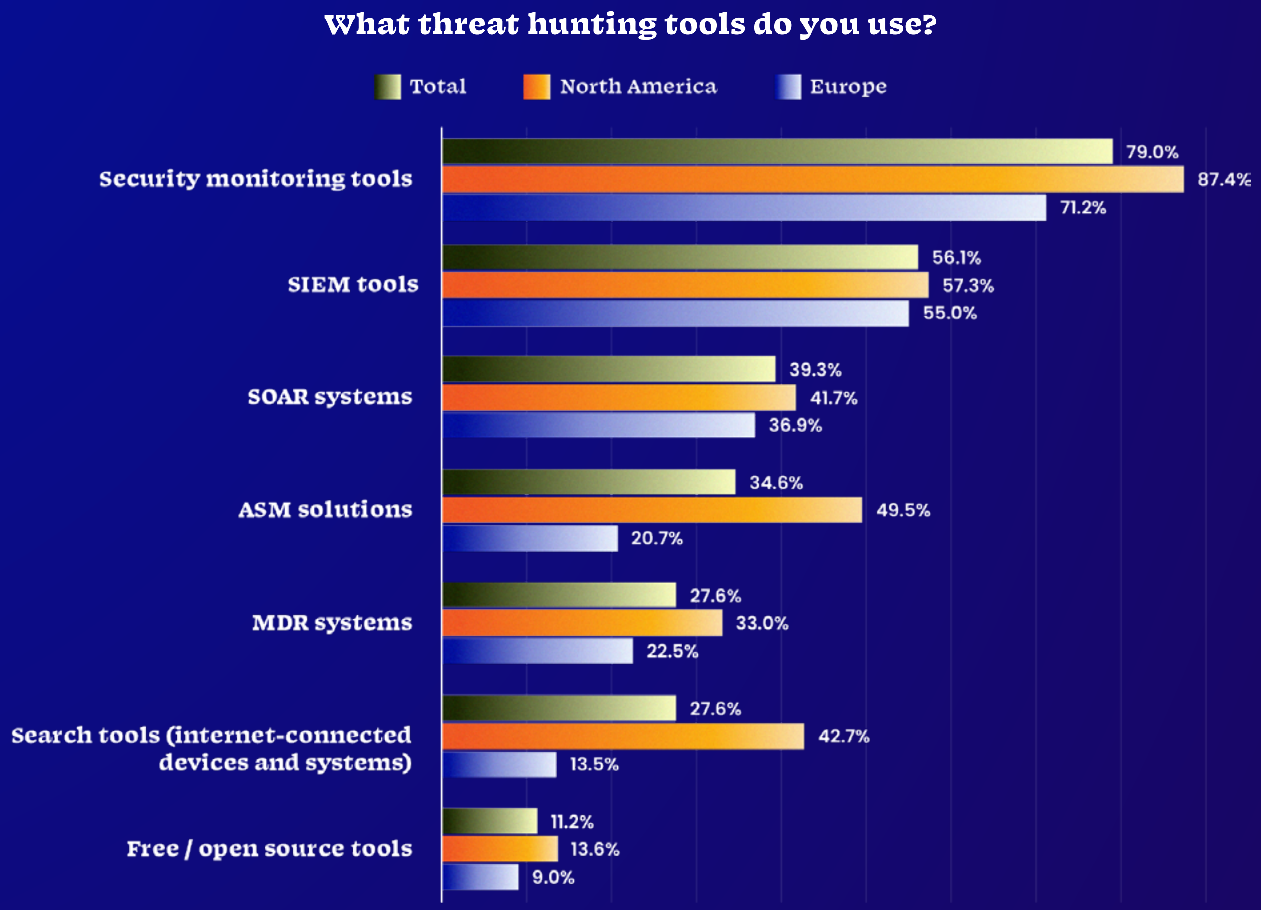

Figure 8: Threat Hunting Tools and Technologies Used

Some open-source tools lack needed functionality

Of those respondents who use open-source or freeware tools, their primary challenge is the variety of tools required due to their limited functionality. This limited functionality is most keenly felt by North American respondents, who were also significantly more likely than European respondents to say that they have difficulty integrating open source tools into their existing tech stacks. It may be the case that North American respondents expect more from their open source tools, or have more complex use cases and more robust tech stacks than their European counterparts.

Of note, a third of global respondents see these tools as producing a lot of false positives, limiting their value. False positives can be a huge headache for threat hunters, who invest time and effort investigating – and sometimes base decisions around – a threat that turns out to be benign. As you'll see later on in this report, threat hunters say that reducing false positives is one of the top three things that would make their jobs easier.

Many open-source tools produce false positives because they rely on outdated, disparate data streams that provide a fragmented view of the threat landscape. The quality of internet intelligence fed into these open source tools is a critical factor. If the foundational internet intelligence open source tools use doesn't reflect a full, contextualized view of global internet infrastructure, accuracy will be a challenge. Also, while the research did not differentiate, it is possible that open source tools that are backed by vendors supplying proprietary intelligence or leveraging higher quality intelligence would minimize the risk of false positives.

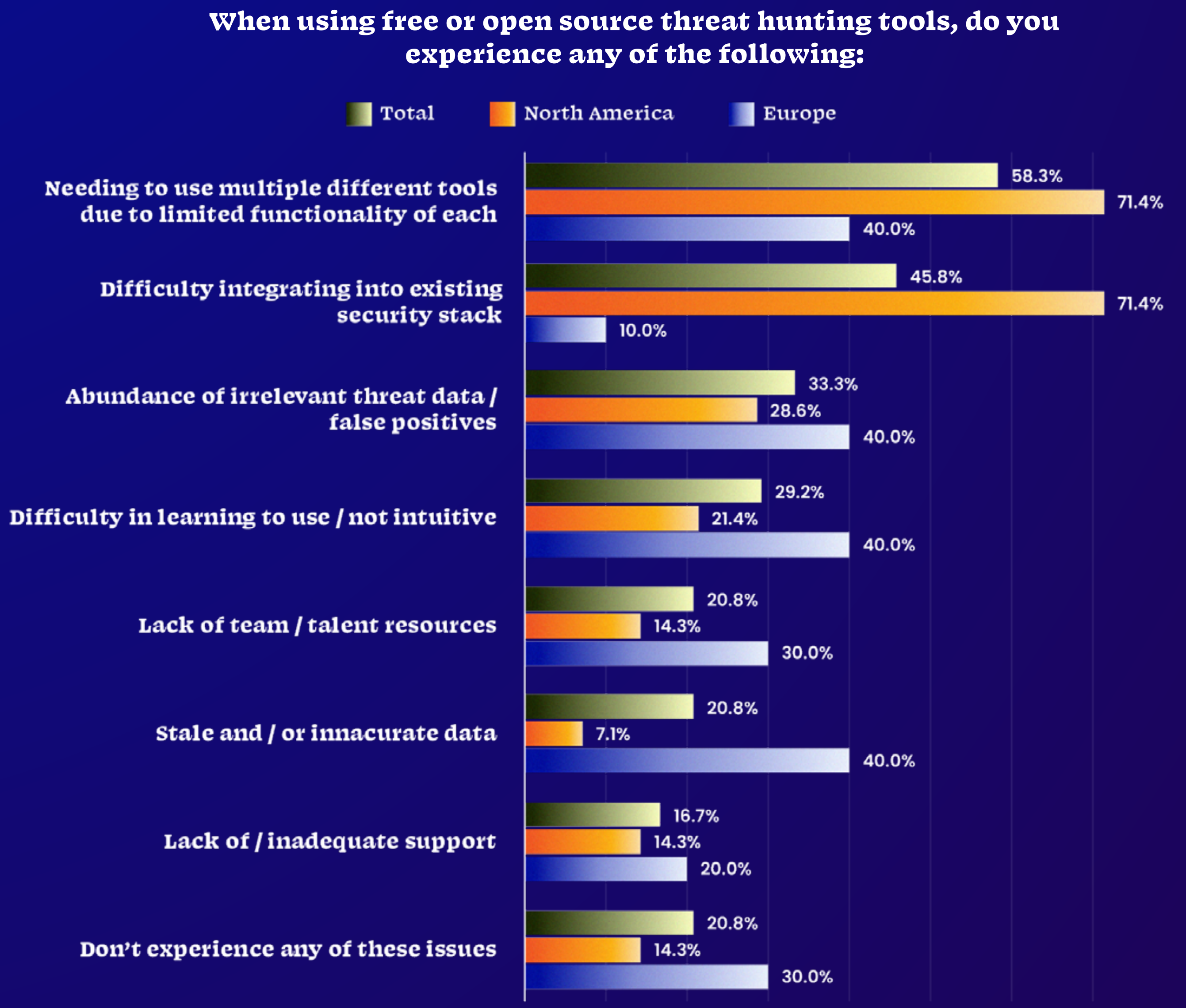

Figure 9: Challenges with Free / Open Source Tools

But wait...AI-based tools are gaining ground

Though the majority of respondents are using traditional security monitoring tools, that doesn't mean they've turned a blind eye to all new tech. Most say they're also making use of AI-based tools in their threat hunting efforts, and finding them very helpful.

Threat hunters' use of AI is likely a response to the significant rise in AI-fueled cyberattacks. Recent research finds that 85% of cybersecurity leaders say that the increase in cyberattacks they've seen within the last year can be attributed to bad actors' use of AI.[11] Not only does AI present a way for attackers to launch sophisticated attacks at scale, AI can also learn and adapt to new defenses – making it easier for adversaries to avoid detection and harder for threat hunters to find them before they strike.

As adversaries turn to AI, threat hunters appear to be doing the same to keep pace.

How exactly are threat hunters leveraging AI? AI's automation and self-learning unlock new efficiencies that help threat hunters accelerate investigations in multiple ways. The sheer rate at which AI can analyze the massive swaths of data that threat hunters typically have to parse offers significant value in and of itself.

[11] Deep Instinct, Generative AI and Cybersecurity Report, 2023

> **Censys profiles the entire internet, so you can just ask to be shown all of the connected systems that run a particular product or software version where a new zero day has been found. It gives you the advantage of not doing it with any special privileges of being on the inside of the network. You're doing it as an attacker would, with the same perspective. *That's really valuable.***
>
> – Threat Hunter, Mid-Sized Organization

Threat hunting use cases for AI include:

- Generating automated threat hunting queries
- Analyzing threat intelligence feeds
- Identifying patterns and IOCs
- Using predictive analytics to forecast potential future threats

As noted earlier, nearly half of threat hunters say that their investigations are prompted by irregularities detected by AI-powered tools.

In addition to standalone AI tech, AI features are enhancing existing threat hunting tools. Censys Search, for example, now includes a CensysGPT feature that translates natural language searches into Censys queries, creating a low barrier-to-entry for threat hunters and accelerating investigations.

As is the case in many professions today, AI-based tools are giving threat hunters the opportunity to aid and advance, rather than replace, their critical work. That said, the extent to which AI will influence threat hunting's traditionally human-centric approach – reliant on threat hunters' curiosity and creativity – in the long term remains to be seen.

In the last year, how effective have you found AI-enabled threat hunting tools to or technologies to be in aiding your threat detection and response capabilities?

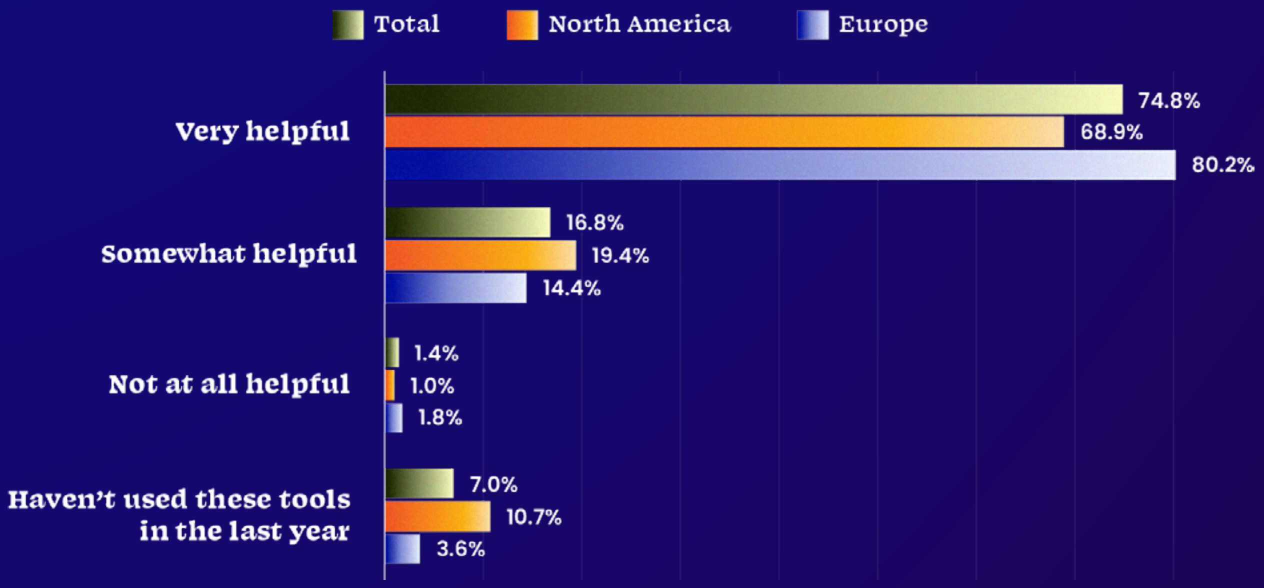

Figure 10: Value of AI-Based Tools

False Positives & Unknown Assets Pose Formidable Challenges

False positives are prevalent

False positives are an unfortunate threat hunting reality. All respondents encounter at least some, but the greatest percentage are finding that between 6% and 20% of their results are inaccurate. **Almost one-third of respondents are finding that over 20% of their results are false positives.** This reflects considerable unproductive effort as threat hunters waste valuable time and resources investigating benign activity. Threat hunters who frequently encounter false positives also risk alert fatigue, and as a result overlook true positives that actually pose a threat to their organization.

> **False positives are the main stressor for me. When it happens [the threat report provided to management turns out to be inaccurate due to false positives], I feel real shame.**
>
> – Threat Hunter, Mid-Sized Organization

Though all respondents encounter false positives, those in North America experience higher rates of false positives than their European counterparts. Respondents in North America were significantly more likely to say that more than 20% of the threats they identified were false positives. This difference is most pronounced among respondents who experience 50% or more false positives: 5.4% of respondents in Europe said that more than 50% of their threats were false positives, whereas 17.3% of respondents in North America said the same.

Why do threat hunters in North America encounter more false positives? Though this report didn't discern, the contrast could be explained by Europe's far stricter data regulations, which may prompt threat hunters to focus more on finding ways to minimize their risk of false positives, such as by seeking out more accurate sources of data or leveraging more reliable threat detection solutions. Or, these regulations may have the opposite effect, discouraging threat hunters from reporting as candidly about the extent to which they struggle with subpar data.

That said, whether based in Europe or North America, respondents share the sentiment that false positives are a problem. As noted later in this report, achieving fewer false positives is one of the top things that threat hunters feel would help them the most.

Approximately what percentage of the threats you have identified in the last 6-12 months have turned out to be false positives?

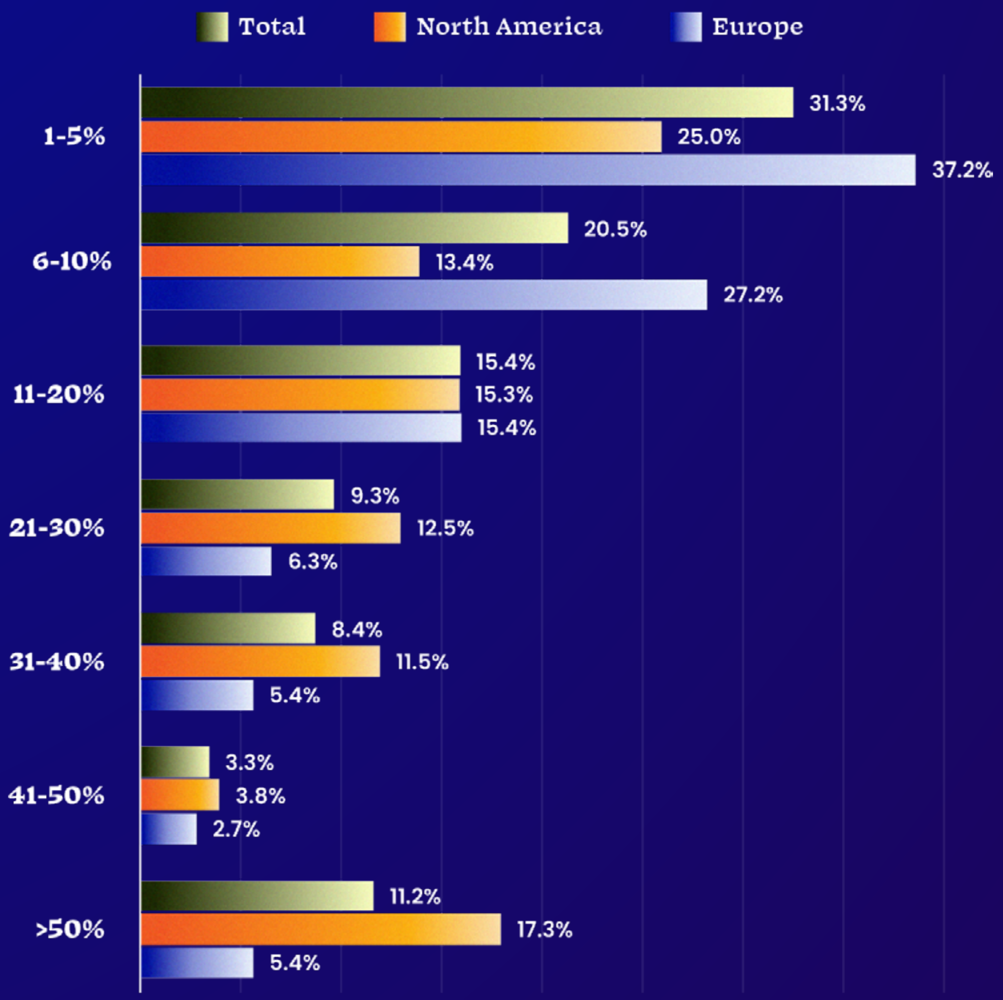

Figure 11: Frequency of False Positives in Last 6-12 Months

Nearly three-fourths of respondents often find unknown assets

In the process of identifying the full attack surface during threat hunting, the majority of respondents always or frequently discover previously unknown assets, highlighting the pervasive risk of these unauthorized or forgotten connections. Respondents in Europe were more likely to say that they always or frequently encounter unknown assets, which could be attributed in part to the fact that these respondents were also less likely than their counterparts in North America to use automated tools like ASM, which discover assets continuously.

These responses underscore the need for more accurate and continuous Attack Surface Management. Organizations without an Attack Surface Management strategy can push the important work of asset discovery into the laps of their threat hunting teams.

Have your threat hunting efforts uncovered internet-exposed assets and/or services of which your organization was previously unaware?

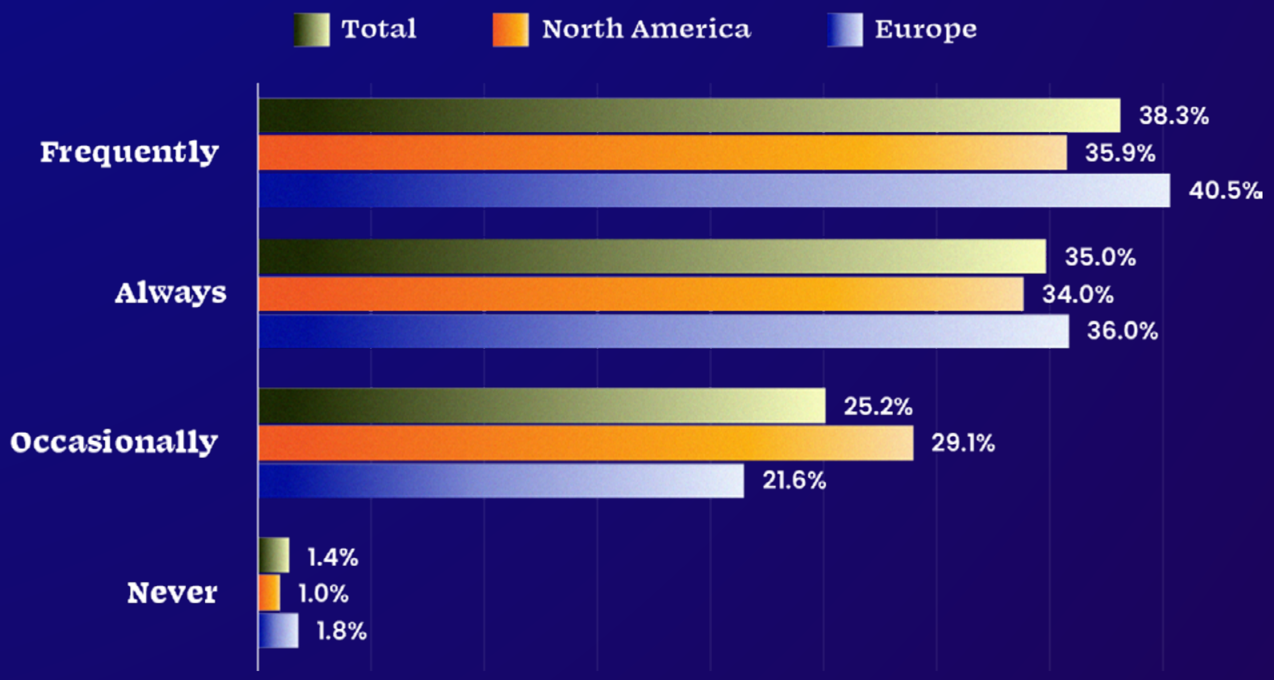

Figure 12: How Often Respondents Discover Unknown Connected Assets During Threat Hunting

Soft Skills Matter, But Are Lacking

Less than half are comfortable communicating with legal/PR

Respondents can use help communicating to various stakeholders about threat hunting results that negatively impact their organizations. Across stakeholders, threat hunters say they are most comfortable sharing news with their direct managers. This isn't surprising given that threat hunters likely have more established relationships with these leaders and benefit from a shared technical foundation. That said, only 68% of respondents say they are "fully confident" communicating with this group.

Communication confidence drops off for other stakeholder groups. Less than 50% of respondents feel "very confident" reporting negative findings to stakeholders in legal or public relations roles and more respondents selected "minimally confident" or "not confident at all" for this group of stakeholders than for any other.

These stakeholders arguably have the greatest need to understand a threat's potential impact to the organization; yet, it's likely for this very reason that threat hunters feel less confident communicating with these stakeholders. Public relations teams need to understand the impact on customers and partners, while legal teams are focused on liability and exposure – the information shared with these groups can set forth actions with broad repercussions. And, given these stakeholders don't have technical backgrounds, threat hunters have a bigger gap to bridge when explaining their findings.

This data also raises a possibility that the known amount of negative information and threats are *perceived* as fewer than the actual instances, because threat hunters cannot communicate them effectively. This possibility should invite threat hunters and their teams to think more critically about ways to build confidence and bridge communication gaps.

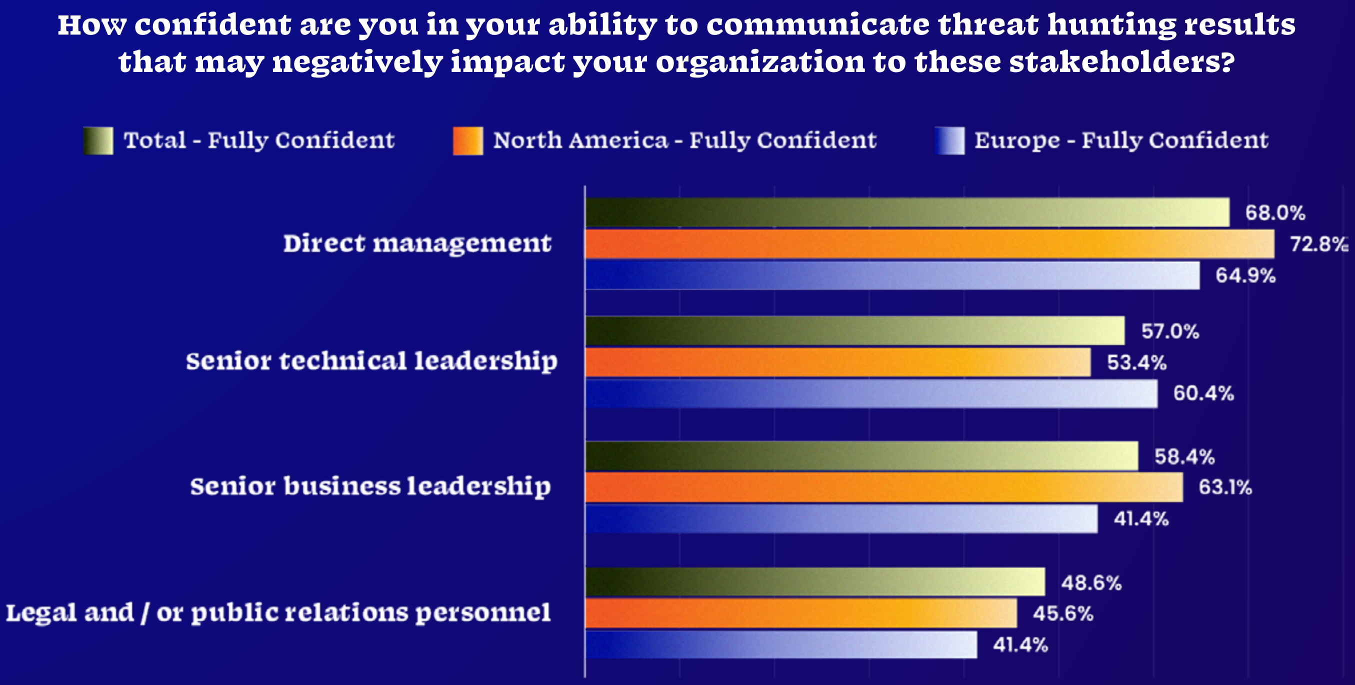

Figure 13: Confidence Levels in Communicating Bad News to Key Stakeholders

Feelings About the Job and Landscape Are Mixed

Work stress prevails, but the right resources offer relief

Respondents indicate that better tools and comfort in their own skills help to decrease work stress. However, forces like the increased number of threats and bigger attack surface, plus intense job pressure, counteract that by increasing stress.

Notably, nearly one-fourth of respondents from North America said that they feel close to burnout. Only 14.4% of respondents from Europe said the same. Higher rates of burnout among threat hunters in North America as compared to Europe may well be attributed to differing attitudes toward work. Studies consistently find that Americans work hundreds of more hours a year than those in other industrialized countries.[12] However, for threat hunters in North America, the most acute cause of burnout may be the high volume of threats they face. As discussed earlier in this report, the U.S. experiences twice as many cyberattacks as Europe. Similarly, respondents in North America were also more likely to say that increased threats and broader attack surfaces have increased their work stress.

[12] International Labor Organization, Working Time and Work-Life Balance Around the World, 2023

> **The stress comes from not knowing what you may not have uncovered yet, to feel confidence that the work being done is not going to be destroyed again. If there's something there you haven't seen or aren't aware of, it can set you back severely. This is where Censys becomes very useful in helping identify all of the assets that are connected, even when people say they're not.**
>
> – Threat Hunter, Mid-Sized Organization

Respondents in North America may be struggling with more threats and higher rates of burnout, but they do feel that better tools are decreasing stress. Over 60% of respondents in North America said better tools are helping, whereas just over 45% of respondents in Europe said the same. This aligns with earlier responses about the tools threat hunters are using; respondents in North America are more likely to have adopted newer tools that leverage automation.

When it comes to threat hunters' skill sets, the majority of respondents said that their skills and capabilities are keeping things manageable. However, over 15% of respondents in both Europe and North America said that concern about their skills and capabilities is causing significant stress. When taken into account with other responses about burnout and increased threats, it's clear that a notable portion of today's threat hunters could use additional support from their organizations.

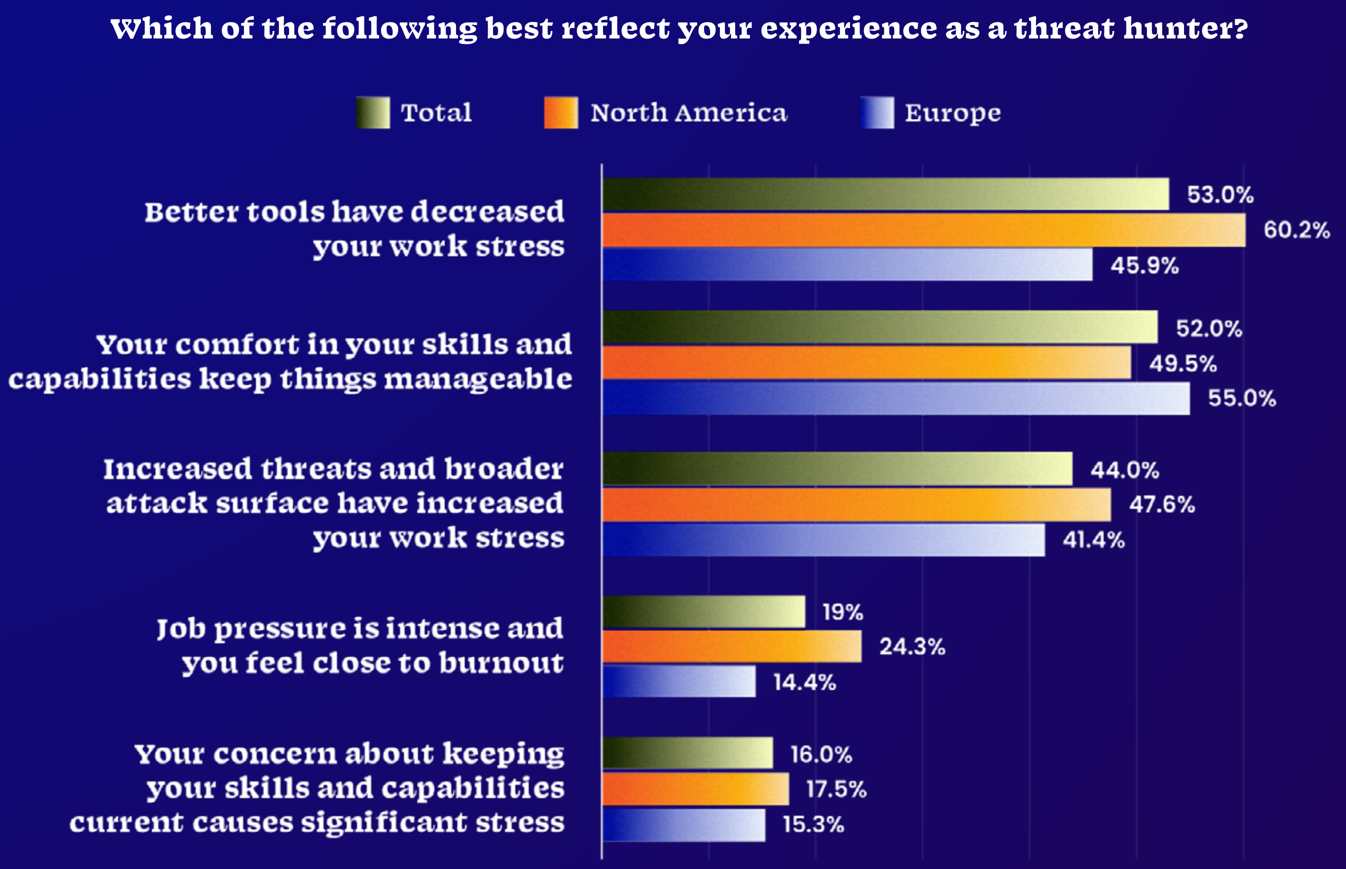

Figure 14: Occupational Perceptions

Threat hunters want better tools and intelligence

What would make threat hunters' lives easier? Access to better threat hunting tools tops threat hunters' wish list, followed by better threat indicators to investigate, and encountering fewer false positives. All three items reflect respondents' interest in improving the quality and integrity of their threat investigations, and direct attention to the impact that reliable threat intelligence, or the absence of it, may have. **Without adequate threat intelligence – required to power threat hunting tools, surface threat indicators, and minimize false positives – threat hunters may struggle to see improvements on these fronts.**

The top 3 things that would most help improve threat hunting*:

1. **Better threat hunting tools**
2. **Better threat indicators to investigate**
3. **Achieving fewer false positives**

*Same across all geographic areas surveyed

Outlooks are divided

Threat hunters may agree on the things that would help improve their jobs, but their views differ when it comes to how the threat landscape is changing. Respondents are close to evenly split on their perception of the threat hunting landscape being better or worse than it was a few years ago, with respondents from Europe feeling more optimistic than those from North America. Disparity in threat volume may again be a relevant explanation as to why respondents in North America are less likely to say that the threat landscape has improved.

Overall, it appears that new technologies fueled by automation and AI are helping, but broader threats and attack surfaces, along with false positives and unknown assets, are making the job of the threat hunter more challenging. With a lack of standard methods for approaching the threat hunting task, continually changing attack vectors, and an endless supply of clever attackers, the field remains a Wild West relying on threat hunter creativity, ingenuity, past experience, and probably a bit of luck.

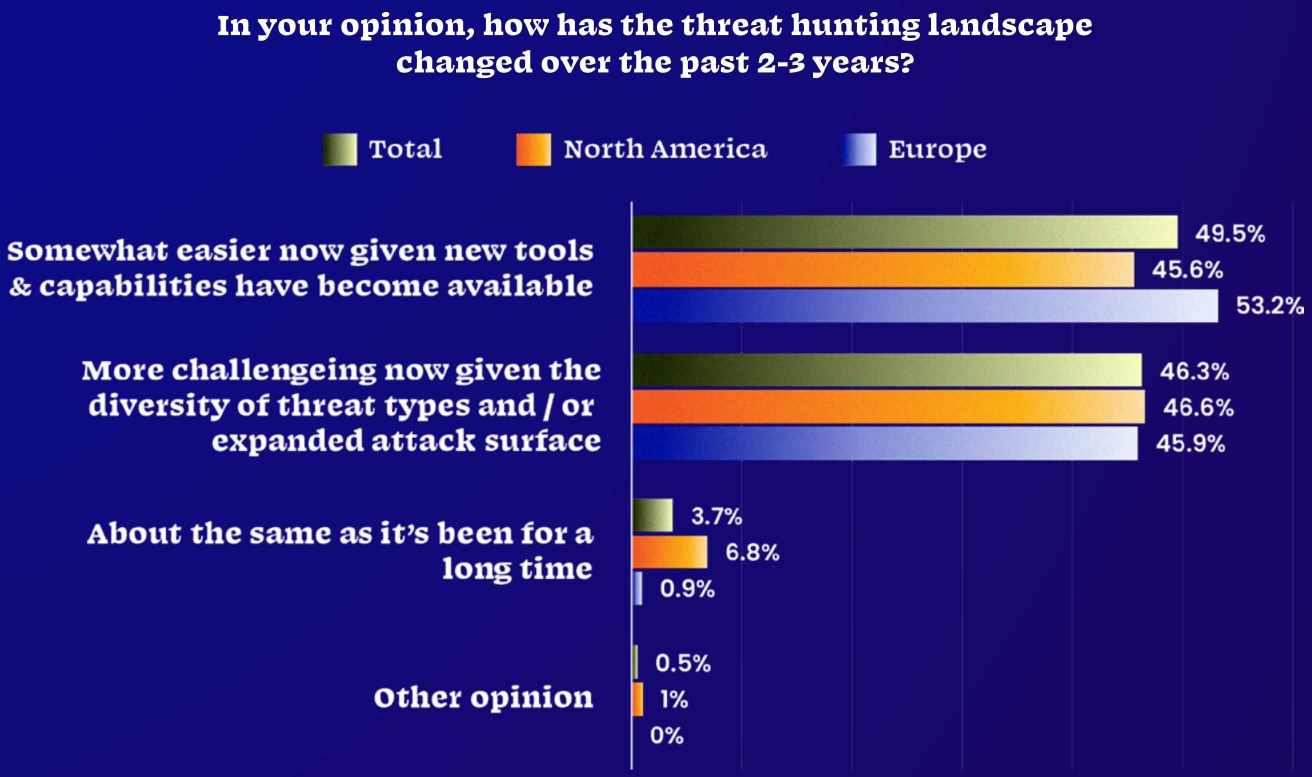

Figure 15: Perceptions of Threat Hunting Landscape

> **The landscape is much better. There are a lot more people looking at threats and making sure they are well-known and publicly-disclosed. It forces people to act.**
>
> – Threat Hunter, Mid-Sized Organization

SECTION 3

Turning Insights Into Action

5 Key Ways Organizations Can Empower Threat Hunters

As cybersecurity teams increase their focus on threat hunting, support for individual practitioners must keep pace. As our findings show, the practice of threat hunting is far from formalized. In the absence of standard practice and ubiquitous tech, organizations should focus on supporting threat hunters with the resources that are available. Lack of support is only to the detriment of organizations' cyber defenses.

1. Invest in superior threat intelligence

Threat hunters need reliable threat intelligence. Our report's findings underscore this reality from a number of perspectives. Accuracy of threat data is the most important factor for respondents' confidence in their threat assessments. Respondents also identify false positives and the discovery of previously unknown assets as significant and pervasive challenges. For approximately one-third of respondents, false positives account for at least 20% of their findings. Respondents say false positives are a common limitation of some of the open source tools they often rely on, too.

Additionally, three-fourths of respondents say they always or frequently come across unknown assets associated with their organization during their threat investigations. Respondents also put better threat indicators and fewer false positives on their wish list of improvements, both of which are contingent on reliable threat intelligence. We know that threat hunters struggle to confidently communicate their findings to stakeholders, particularly to those without technical roles. The more threat hunters trust the intelligence that underpins their findings, the more confident they may be in sharing those findings with key stakeholders.

Cybersecurity teams and leaders should therefore ensure that threat hunters have reliable sources of threat intelligence at their disposal, and that tech platforms in use are powered by accurate data. Threat intelligence sources should offer a near real-time view of global internet infrastructure, and provide rich context to facilitate investigations and reduce false positives. Censys, for example, provides proprietary internet intelligence based on predictive scanning across all 65K ports and daily refreshes of all 3B+ services in its dataset. Threat hunters can also rely on Censys to discover new services that come online 140% faster than the closest competitor.

Asking threat hunters to make due with inaccurate intelligence makes it that much harder to stay ahead of adversaries.

2. Adopt automated tools like ASM

Only one-third of surveyed threat hunters say they've adopted new automated tools like ASM; the majority are reliant on traditional security monitoring tools. Threat hunters can unlock significant efficiencies in their work with the support of automation. Finding opportunities for efficiency is particularly important for threat hunters on lean teams who balance multiple job responsibilities – recall that 58% of respondents are part of teams less than ten.

ASM tools in particular, like Censys Attack Surface Management, can reduce threat hunters' discovery of unknown assets and continuously monitor an organizations' attack surfaces for new exposures that attackers could exploit. The majority of respondents (74%) said that they frequently or almost always discover unknown assets on their attack surface in the course of their work; this manual discovery and management takes time away from more proactive threat hunting efforts. Automated ASM solutions that offer continuous asset discovery can bridge the gap here and ensure that threat hunters don't have to spend time discovering and then managing these unknown assets on their own.

3. Embrace the rise of AI

Certain automated tools may not yet be widely adopted, but threat hunters say they are using AI-based tools, and are reporting that these tools are delivering benefits. Nearly half say that their investigations are triggered by anomalies detected by AI-powered tools, and almost 75% describe AI tools as "very helpful" to their threat hunting work. The use cases for leveraging AI in threat hunting investigations are vast, and growing. Threat hunters will likely continue to seek out AI-driven tools to further accelerate their threat hunting investigations.

This gives organizations the opportunity to not only ensure that the use of these tools align with corporate policy, but that more importantly, threat hunters have the resources they need to access the right tools. Organizations should partner with their practitioners to identify and invest in the kinds of AI-based tools that can save their practitioners valuable time and further optimize their investigations. Organizations can also keep in mind that, as mentioned in the report, AI isn't just a standalone option; tech providers are integrating AI-driven components throughout their product suites, as Censys has done with the new CensysGPT feature available in Censys Search.

4. Ensure adequate training

When it comes to managing the stress of the job, only 52% of respondents say that comfort in their skills and capabilities are keeping things manageable. More than 15% say that concern about their skills and abilities causes significant stress, and a quarter of threat hunters in North America are burned out.

To prevent burnout and improve retention, organizations should support practitioners with adequate training, particularly practitioners who are taking on threat hunting responsibilities for the first time or who are part of lean security teams. This training could come in the form of access to conferences, webinars, peer training, boot camps, and more. As threat hunting evolves from a more niche endeavor to a solidified aspect of corporate cybersecurity, organizations and their practitioners will need to find creative ways to bridge skill gaps.

5. Help threat hunters communicate more effectively with stakeholders

Stakeholder communication emerges as a key area of opportunity for threat hunters in this report, even though threat hunters themselves don't identify communication as one of their top challenges. However, not even three-fourths of threat hunters say they are "very confident" about sharing negative findings with their direct management. Less than half feel confident communicating with public relations and legal teams. Understanding the scope and potential impact of a threat is a critical need for stakeholders across the business, and gaps here can have wide-ranging consequences.

Organizations should work with threat hunters to ensure they have the skills and supporting tools to confidently and effectively communicate with stakeholders. This might mean creating more opportunities for threat hunters to interact with stakeholders on a recurring basis, to deepen relationships, or it may mean more support from direct managers who can partner together with threat hunters when sending out communications or fielding questions. It may also warrant investing in tools that can help threat hunters track, summarize, and report on their findings, so that stakeholders can refer to a concrete artifact of supporting evidence when learning about a new threat.

Conclusion

Our research demonstrates that as threat hunting becomes a fixture of modern cybersecurity, opportunity abounds for organizations and their practitioners to bring structure and consistency to the discipline. Today's threat hunters resourcefully tap into a number of available technologies, including open source tools and AI-based tech, but still acknowledge there are gains to be made when it comes to conducting threat investigations with greater accuracy and confidence. As organizations consider ways to support the practitioners they've tasked with threat hunting responsibilities, investment in the right resources – particularly superior threat intelligence – will be paramount.

Additional Resources:

The 2023 State of Threat Hunting: How Threat Hunters Are Navigating a Transforming Cybersecurity Landscape
https://go.censys.com/The-2023-State-of-Threat-Hunting_On-Demand.html

Profiles in Threat Hunting: Finding Threats by Observing Behaviors
https://censys.com/profiles-in-threat-hunting-finding-threats-by-observing-behaviors/

The Total Economic Impact™ of Censys EASM: Analyst Deep Dive
https://censys.com/the-total-economic-impact-of-censys-easm-analyst-deep-dive/

censys

About Censys

Censys is the leading Internet Intelligence Platform for Threat Hunting and Attack Surface Management. We provide governments, enterprises, and researchers with the most comprehensive, accurate, and up-to-date map of the internet to defend attack surfaces and hunt for threats. Censys discovers new services 140% faster than the nearest competitor.

Founded by the creators of ZMap, trusted by the U.S. Government and over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the Internet.

For more information, visit www.censys.com.