censys

EXECUTIVE SUMMARY

The 2024 State of Threat Hunting

Overview

The 2024 State of Threat Hunting Report provides a comprehensive analysis of the current threat hunting landscape in the face of evolving cyber threats, the integration of artificial intelligence, and automation tools. Our study surveyed over 200 threat hunting professionals from North America and Western Europe to reveal critical insights into their challenges, practices, and the tools they rely on.

Their responses paint a picture of a discipline rich with opportunity - including the opportunity to standardize, leverage better tools and intelligence, and benefit from more organizational support.

Key Findings

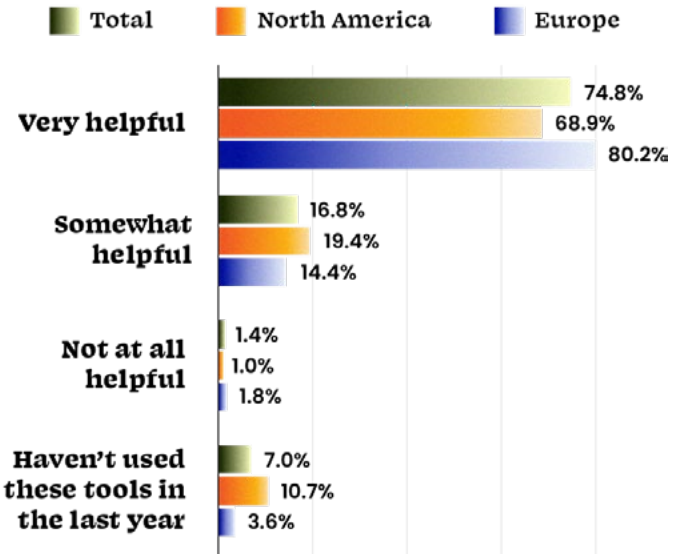
Threat Hunting Practices Vary Significantly:

Our findings highlight the lack of consistency and standardization in threat hunting practices. Threat hunters employ a variety of methods and approaches, with many relying on a mix of tools and personal experiences. For example, 50% say they implement a formal threat hunting process for tracking their attack surface on a weekly basis, while 20% implement a formal process on a monthly basis. Only 30% implement a process on a continuous basis. This kind of diversity underscores the need for a common, reliable standard that could enhance confidence and effectiveness in threat assessments.

AI and Automation Are Rising:

A significant portion of respondents have started incorporating AI and automated tools such as Attack Surface Management (ASM) and Managed Detection and Response (MDR) into their workflows. Nearly 75% of respondents said that AI-enabled threat hunting tools were "very helpful" to their work in the past year. These technologies are seen as beneficial, promising to automate time-consuming tasks and improve job satisfaction by reducing stress for threat hunters.

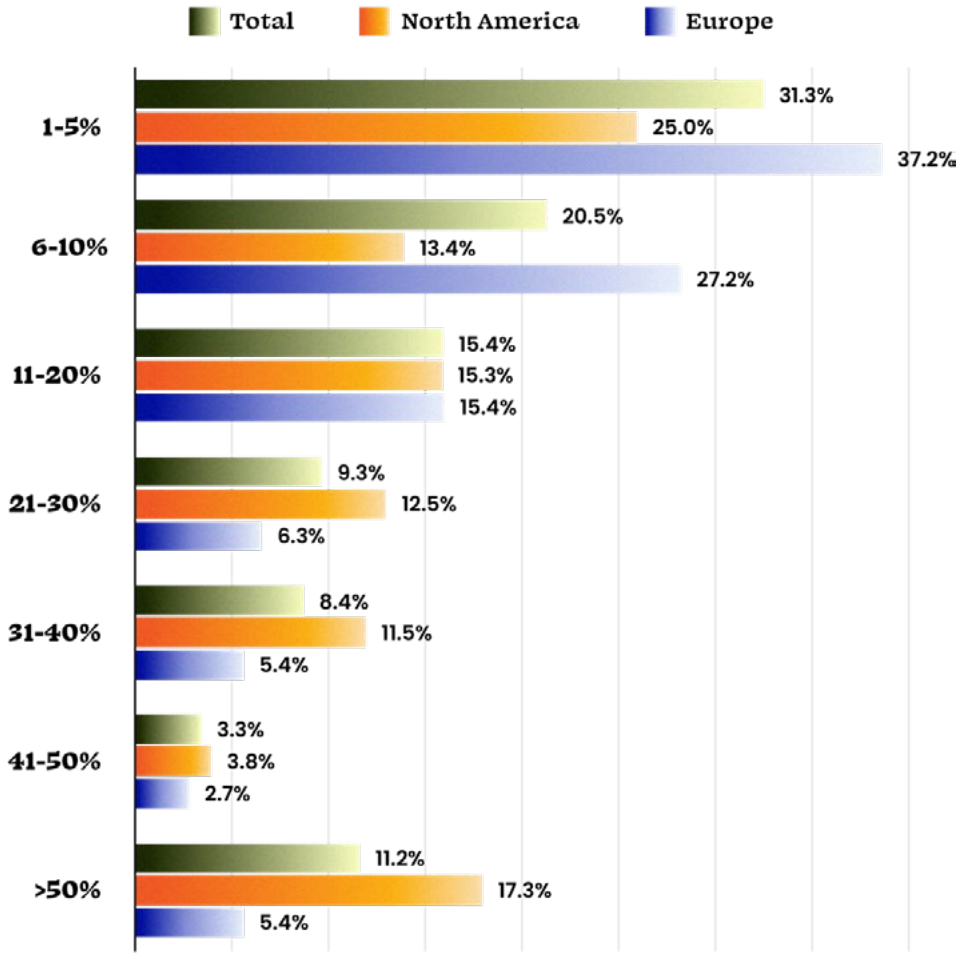
In the last year, how effective have you found AI-enabled threat hunting tools to or technologies to be in aiding your threat detection and response capabilities?



Challenges with False Positives and Unknown Assets:

False positives and the discovery of previously unknown assets are major challenges for threat hunters. Over 30% of respondents reported a high rate of false positives in their findings, indicating a substantial waste of resources. Moreover, 73% frequently encounter unknown assets, highlighting the risks of unmonitored and potentially vulnerable points in networks.

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



Communication & Soft Skills Are Lacking:

Many threat hunters express a lack of confidence in communicating their findings to non-technical stakeholders. Less than half are confident in sharing news with legal and public relations teams. This gap in effective communication can hinder the broader understanding and response to cybersecurity threats within organizations.

Mixed Feelings About the Job:

Our report reveals mixed sentiments among threat hunters regarding their roles. While better tools and skills contribute to lower stress levels, the increasing volume of threats and the expansive nature of attack surfaces are sources of concern. Notably, a portion of threat hunters, especially in North America (25%), report feeling close to burnout.

5 Ways Organizations Can Empower Threat Hunters

To empower threat hunters and enhance cybersecurity practices, organizations should:

1. **Invest in Superior Threat Intelligence:** Accurate and reliable threat intelligence is crucial for effective threat hunting. It enables hunters to make informed decisions, reduce false positives, and identify unknown assets more efficiently.
2. **Adopt Automated Tools:** Tools that automate the discovery and monitoring of assets can alleviate some of the manual burdens on threat hunters, allowing them to focus on more strategic activities.
3. **Embrace AI Technologies:** AI-driven tools offer significant advantages in analyzing vast amounts of data and identifying patterns that might elude human analysts. Organizations should support the integration of AI into threat hunting practices.
4. **Provide Adequate Training:** Ensuring that threat hunters have the necessary skills and knowledge is essential for managing stress and preventing burnout. Training programs and continuous learning opportunities can bridge skill gaps.
5. **Improve Communication Skills:** Organizations must help threat hunters develop the ability to communicate effectively with various stakeholders. This can involve training in soft skills and providing tools to facilitate clear and impactful reporting.

Conclusion

The evolving landscape of cybersecurity, marked by sophisticated threats and the potential of AI and automation, presents both challenges and opportunities for threat hunters. By addressing the gaps in standard practices, tool availability, and skill sets, organizations can better support their cybersecurity teams.

Interested in more insights? Read the full report.