TEAM CYMRU
INTELLIGENCE BEYOND BORDERS

Voice of a Threat Hunter Report 2024

EXECUTIVE SUMMARY

Introduction

As cyber threats continue to rise, organizations must evolve their security strategies to defend against increasingly sophisticated attacks. Team Cymru's "Voice of a Threat Hunter 2024" survey highlights the critical role of threat reconnaissance in this battle.

Despite having threat hunting programs in place, analysts emphasize the need for proactive defense measures, extending their efforts beyond organizational borders to detect undetected malicious activities.

This report explores the current landscape of threat hunting, the challenges security teams face, and the essential tools, strategies, and resources required for success. By providing these insights, we aim to empower organizations to enhance their security posture and respond more effectively to emerging threats.

David Monnier
Chief Evangelist | Team Cymru

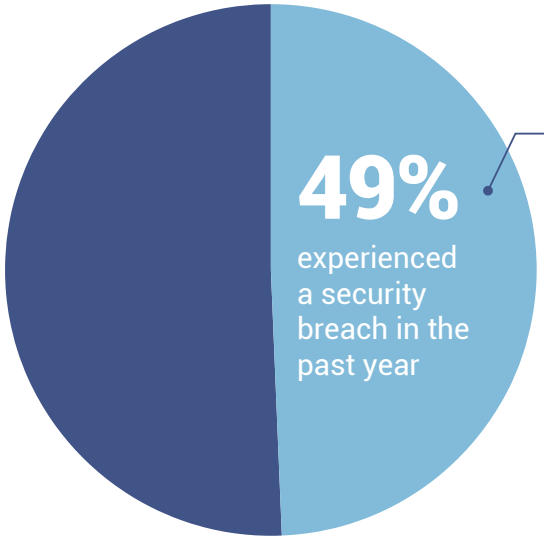
Overview

To learn more about the current state of threat hunting programs, our annual survey had 293 security practitioners share their threat hunting successes and challenges, how they anticipate improving them into the future, and what return on investment they're seeing, among other details.

We hope that the insights gleaned from this survey can help inform strategic decisions and guide you in implementing threat hunting and reconnaissance programs to improve cybersecurity defenses.

Advantages of Threat Hunting

Our survey reveals critical insights into the effectiveness of threat hunting programs. Despite significant breaches, many organizations find that threat hunting programs play a pivotal role in mitigating potential threats and enhancing overall security posture.



Of those that experienced a breach in the last year,

72%

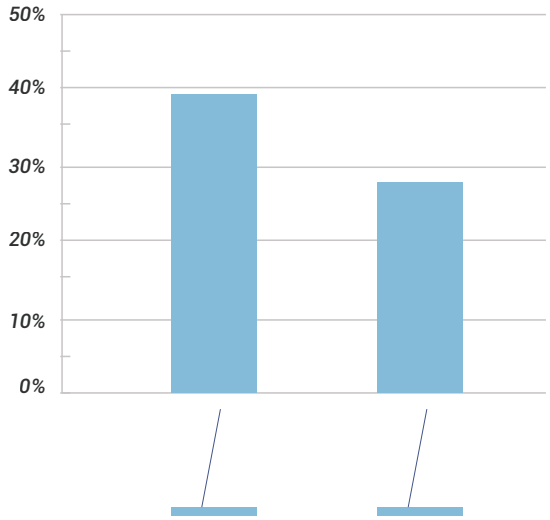
say threat hunting helped mitigate the impact of the breach

60% Say threat hunting programs help mitigate potential threats.

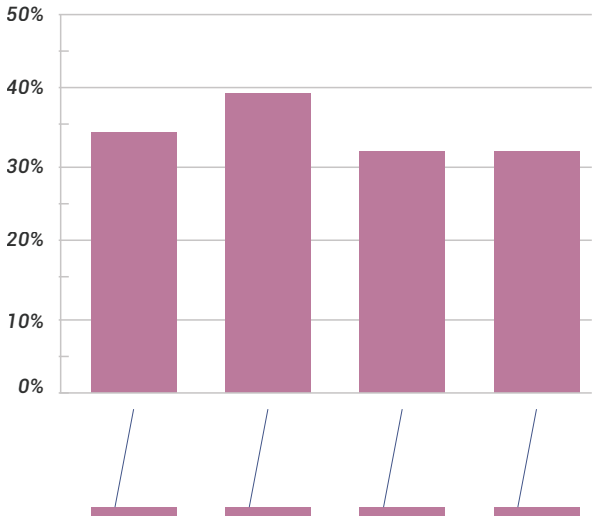
Challenges

Respondents shared the top obstacles to implementing an effective threat hunting program, including:

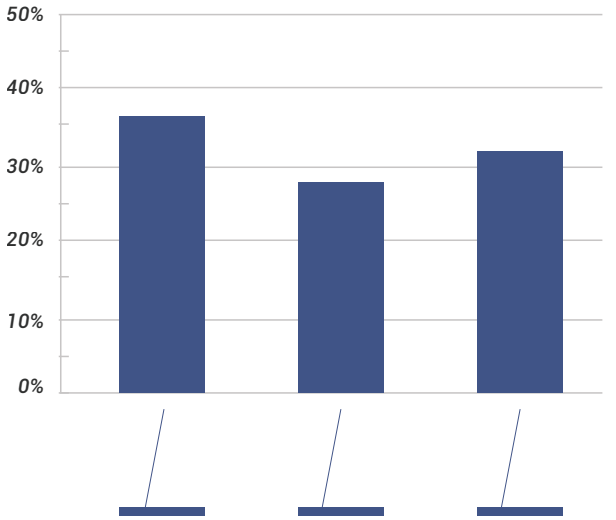
Finance & Funding



Tools

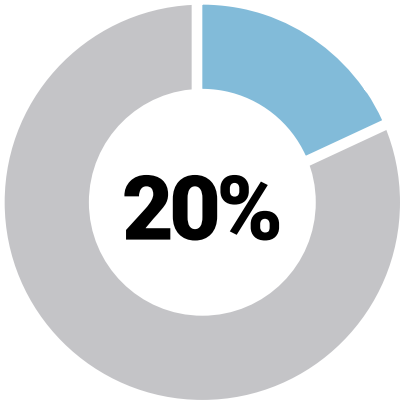


Resources

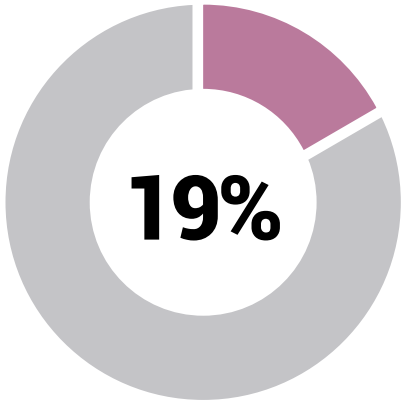


Top Identified Threats

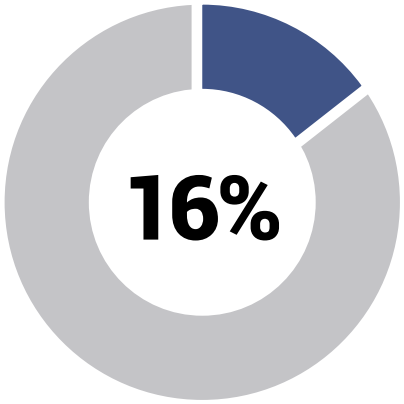
Our survey highlights diverse range of threats most successfully identified by threat hunting programs, including:



Ransomware related activity

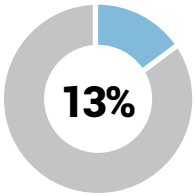


Advanced persistent threats

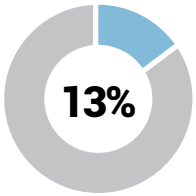


Phishing attacks

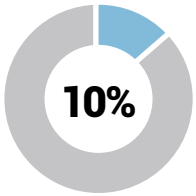
Other threats include:



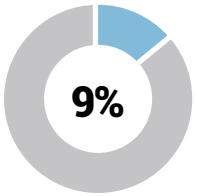
Malware Infections



Unauthorized Access Attempts



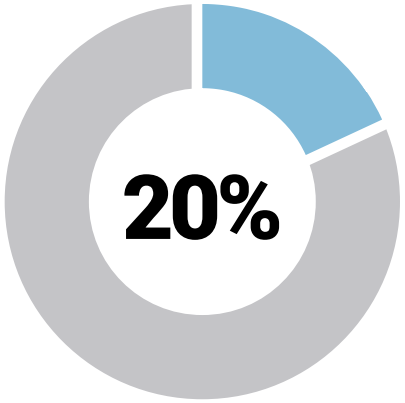
Distributed Denial-of-Service (DDoS) Attacks



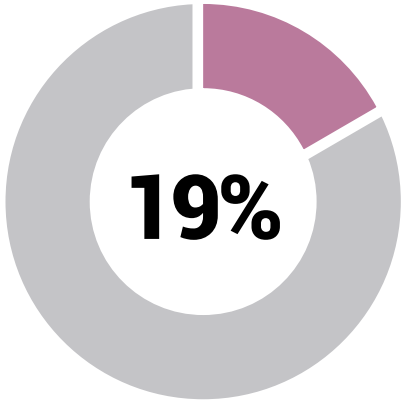
Insider Threats

Objectives

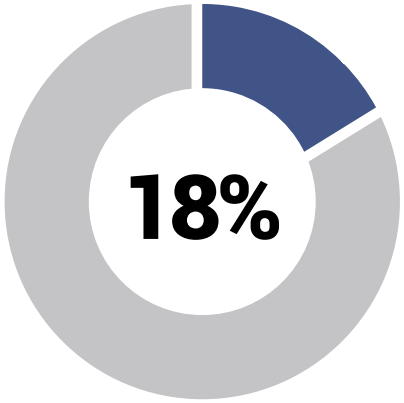
Respondents outlined their primary goals for implementing threat hunting programs.



Proactive detection of previously unknown threats

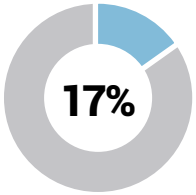


Monitoring third parties for indicators of compromise or risk

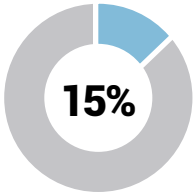


Reducing attack surface by discovering and removing weaknesses

Additional objectives include:



Optimizing Detection Rules Based on Threat Hunt Outputs

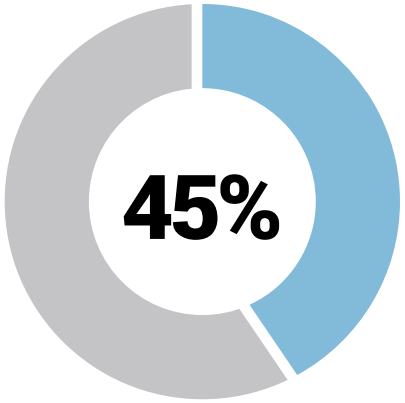


Identifying Threats Before an Attacker Causes Damage

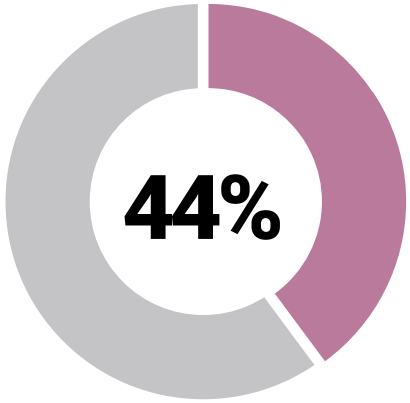
Validating Prevention and Detection Tools

Program Enhancements

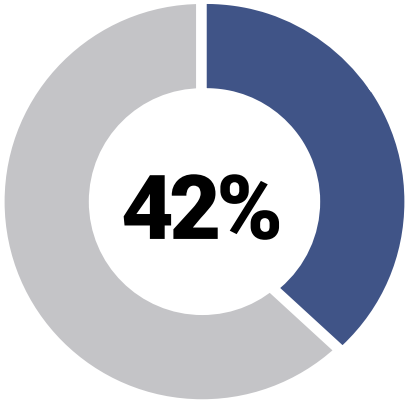
To improve threat hunting efforts, respondents have identified several key enhancements:



Actionable threat intelligence

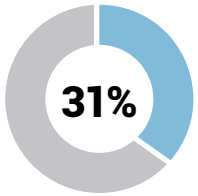


Additional staff with specific threat hunting experience

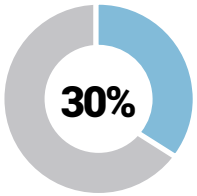


Network forensic detection, netflow telemetry, and/or full packet captures

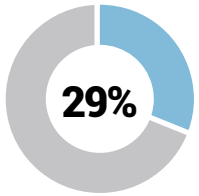
Other enhancements include:



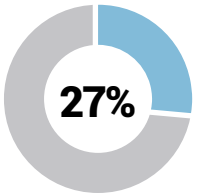
Visibility Across All Assets That Need To Be Protected



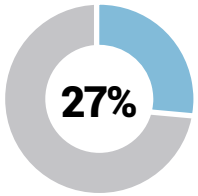
EDR Tool



Automation (Including Workflows and Actions)



SIEM/SOAR



Access To Internet Telemetry

Key Takeaways

The following key takeaways provide actionable insights to help organizations enhance their threat hunting capabilities, strengthen defenses, and navigate the complexities of cybersecurity.

TOOLS

Invest in tools like EDRs, SIEMs, and network forensic tools that enhance visibility and map your organization's attack surface, which are crucial for identifying vulnerabilities and proactive threat hunting. These tools should also provide actionable threat intelligence that is tailored to your organization's needs, helping to streamline responses and reduce analysis time.

TRAINING

Address the cybersecurity talent shortage by equipping your team with the necessary tools and training to become skilled threat hunters. Leveraging automation and AI can alleviate manual tasks, allowing your team to focus on strategic threat hunting activities.

FUNDING

To overcome funding challenges, optimize your current budget by investing in technologies that offer high returns on investment, such as automation and AI. Additionally, demonstrate the value of your security initiatives to leadership to secure increased budget allocations.

BASELINE DATA

Ensure you have comprehensive baseline data to define what is “normal” for your network, which is vital for effective threat hunting. Increase your data storage capabilities to improve historical data analysis, aiding in future threat detection and response.

PRIORITIZE THIRD-PARTY MONITORING

Expand third-party monitoring to detect compromises more effectively, as third-party breaches are a significant risk. Implement thorough security assessments for all third-party vendors to enhance your overall security posture.

Conclusion

The survey findings underscore the evolving landscape of threat hunting in cybersecurity, revealing both the progress made and the challenges that persist. As organizations navigate the complexities of cybersecurity, it is crucial to invest in the right tools, people, and strategies to fortify defenses beyond their network borders. The insights gleaned from this survey can inform strategic decisions and guide organizations in implementing a robust threat hunting program to keep malicious actors at bay.

Download the full report here for complete insights on The Voice of a Threat Hunter 2024.

Team Cymru's mission to Save and Improve Human Lives is fulfilled by empowering security teams around the world to track and disrupt the most sophisticated bad actors and malevolent infrastructures. Powered by the Pure Signal™ platform, the largest source of context-enriched external threat intelligence, our Enterprise and Government customers gain real-time visibility of vulnerabilities and malicious internet activity beyond network borders to proactively close security gaps and accelerate incident response across organizations and third-party ecosystems. Its Community Services provides no-cost threat detection, alerting, DDoS mitigation, and threat intelligence to more than 140 CSIRT teams across 86+ countries.

Learn more at **team-cymru.com**

Try Scout Insight Free