



# **Voice of a Threat Hunter Report 2024**

---

**EXECUTIVE SUMMARY**

# Introduction

As much as every security practitioner would love to see the tide of threat actors and malicious activity recede, it continues to rise – and security teams need to keep evolving their strategies to protect their organizations against that rising tide.

One of those key strategies is threat reconnaissance. Having a threat hunting program in place is a way to find and investigate potential threats inside the organization, yet our “Voice of a Threat Hunter 2024” survey informs us analysts feel that’s not enough – they want to be proactive in building defenses. Going beyond their borders to discover undetected malicious activity gives security teams the critical information to proactively and efficiently respond to attacks.

But security teams can’t achieve any of these successes without having the right tools, strategies, people, or budgets.

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. Overall, it shows where security teams are today in their threat hunting efforts, and – crucially for security leaders to take note of – where they want their ambitions to take them.

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.



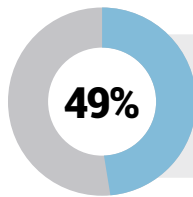
**David Monnier**

**Chief Evangelist | Team Cymru**

## Key Findings

Here are nine insights from respondents into their current threat hunting programs:

### Strategic Impact



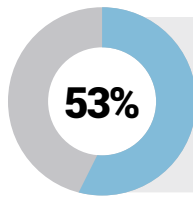
**49% have experienced a major security breach in the past 12 months.** Of those that did, 72% say their threat hunting program played a key role in preventing or mitigating the breach.

### Strategic Priorities

The top priority for the next year are:

- **Expanding third-party monitoring for signals of compromise**
- **Increasing host/network visibility**
- **Adding more threat hunters or contractors for external support**

### Processes

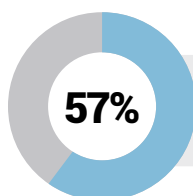


**53% believe their current threat hunting program is very effective.** Up from 41% in 2023, the increase in confidence relates to the tools in place trained and experienced threat hunters, and baseline data that shows what is 'normal'.

### Budget & ROI

Their biggest challenges to implementing an effective threat hunting program are:

- **Lack of appropriate funding**
- **Lack of historical data to threat hunt against**
- **Lack of trained threat hunters**



**57% see an ROI on their threat hunting activities.** However, only 44% expect their budget to increase over the next year.

## People

Their biggest worry are:

- Failing to retain qualified personnel
- Inability to accurately measure the success of the threat hunting program
- Failing to keep up with current trends and threat intelligence

To enhance their threat hunting program, respondents would:

- Add actionable threat intelligence
- Add additional staff with specific threat hunting experience
- Add network forensic detection, netflow telemetry, and/or full packet captures

## Technology

Their top objectives are:

- Proactive detection of previously unknown threats
- Monitoring third parties for indicators of compromise or risk
- Reducing the attack surface by discovering and removing weaknesses

The biggest ways to improve threat hunting are:

- Better threat intelligence tools
- More skilled personnel
- Increased funding

# Table of Contents

## SECTION #1

**Who We Surveyed**

## SECTION #2

**The State of Current Threat Hunting Program**

## SECTION #3

**Tools and Budget**

## SECTION #4

**Threat Hunting Priorities**

## SECTION #5

**Threat Hunting Performance and Measures**

## SECTION #6

**Outlook**

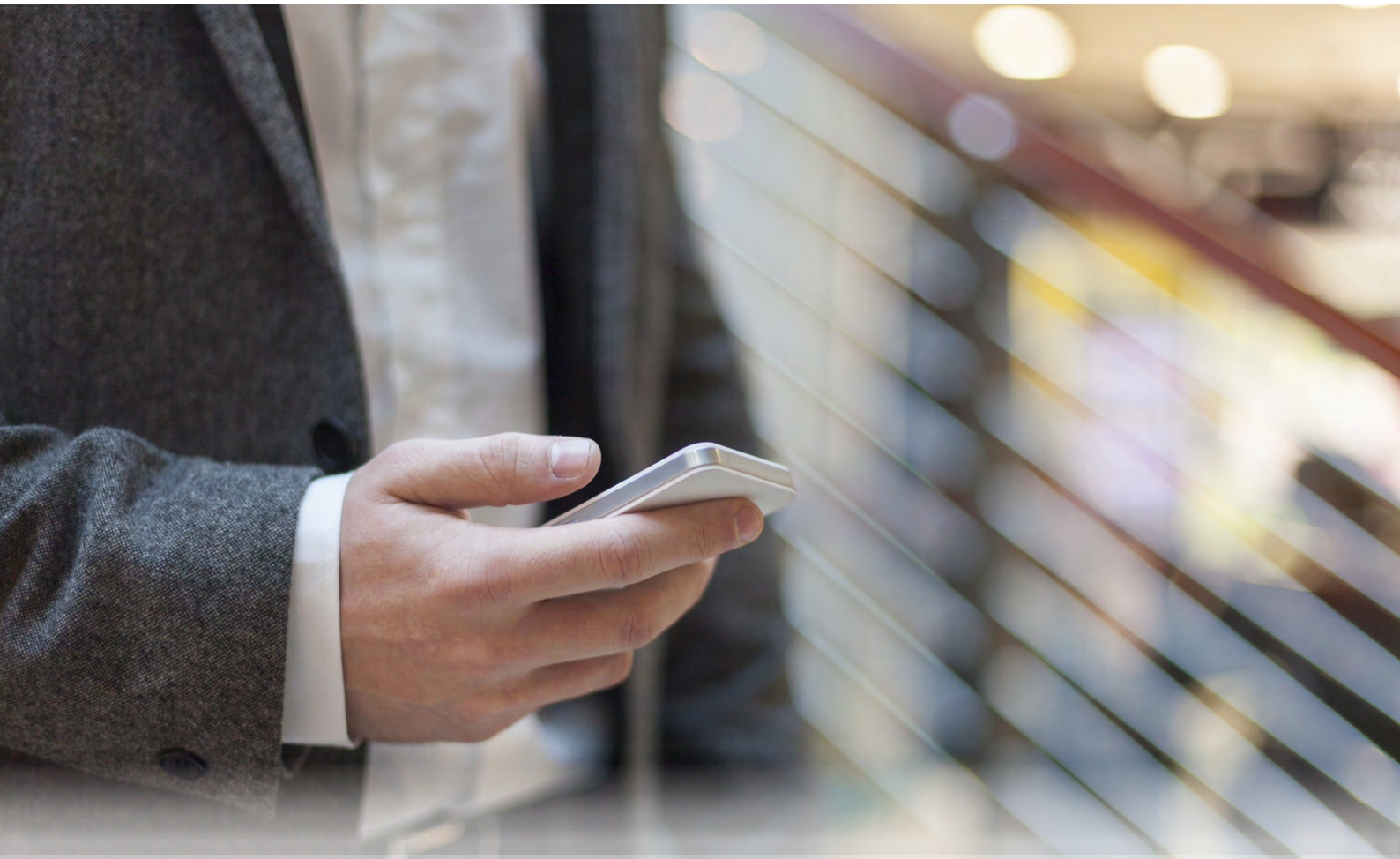
## SECTION #7

**Actionable Takeaways For Threat Hunting Team Leaders**

# **SECTION#1**

---

## **Who We Surveyed**



## Survey Methodology and Participant Demographics

Starting on April 24, 2024, we surveyed 293 cybersecurity professionals who work in security analyst roles. The survey was performed online via Pollfish using organic sampling. To provide greater context around these findings, below are the details on who we surveyed and the methodology used. Learn more about the Pollfish methodology [here](#). 100% of respondents

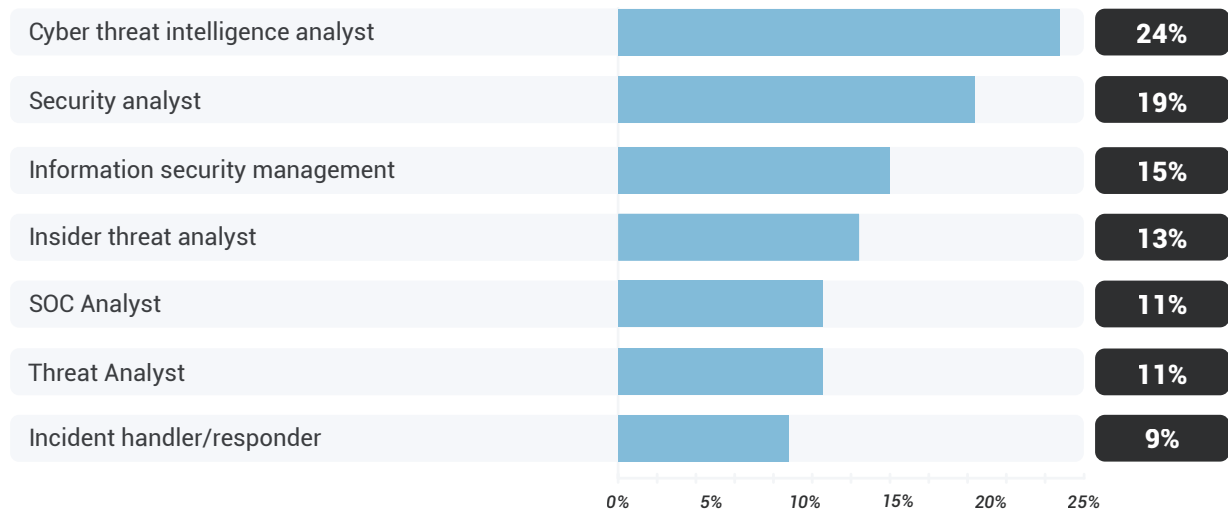
What best describes the department you work in?

- **100% of respondents were in Cyber Security.**

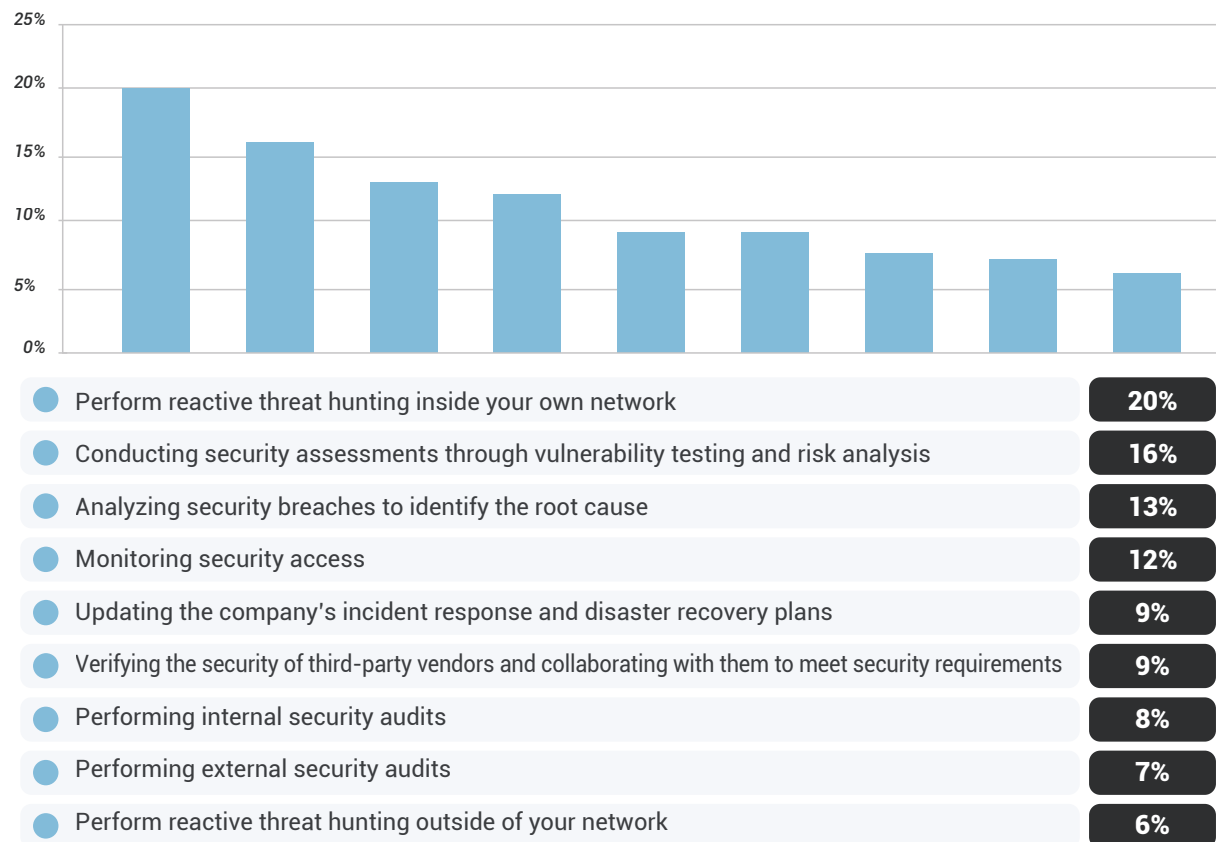
Does your organization currently have a threat hunting program?

- **100% of respondents have a threat hunting program.**

### What best describes your title?

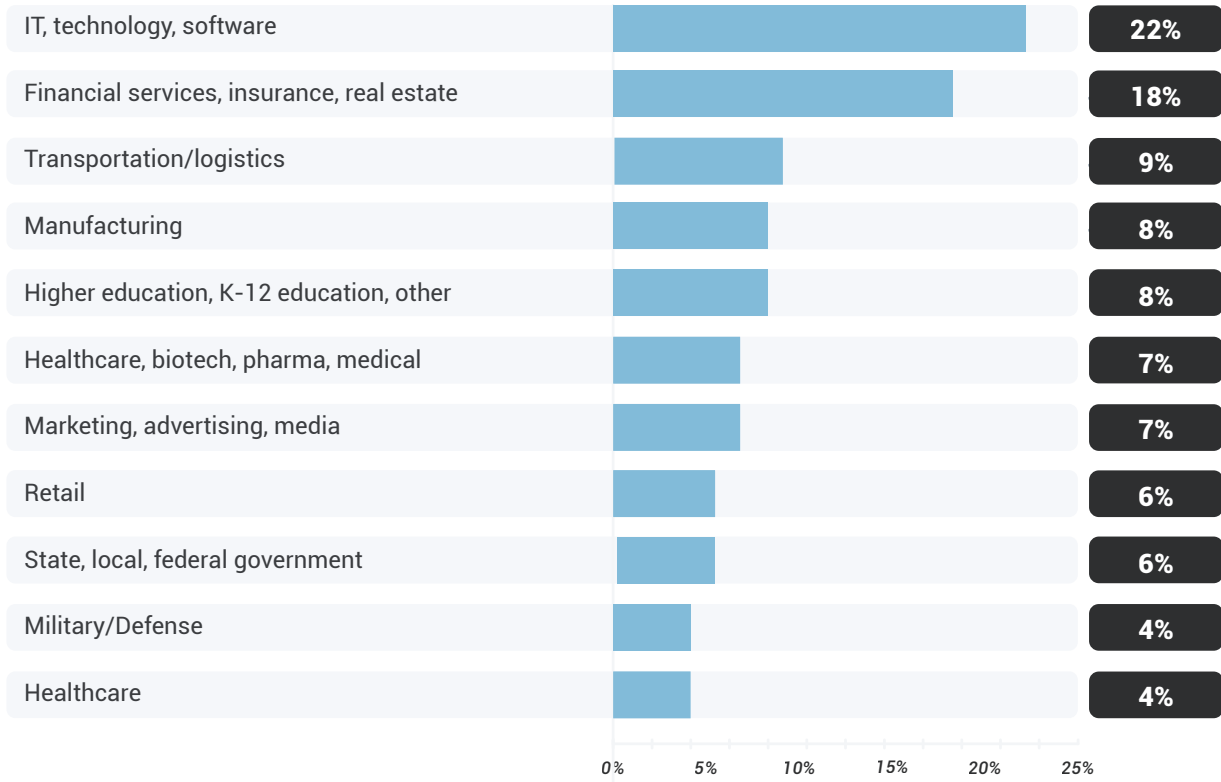


### What are your primary responsibilities?

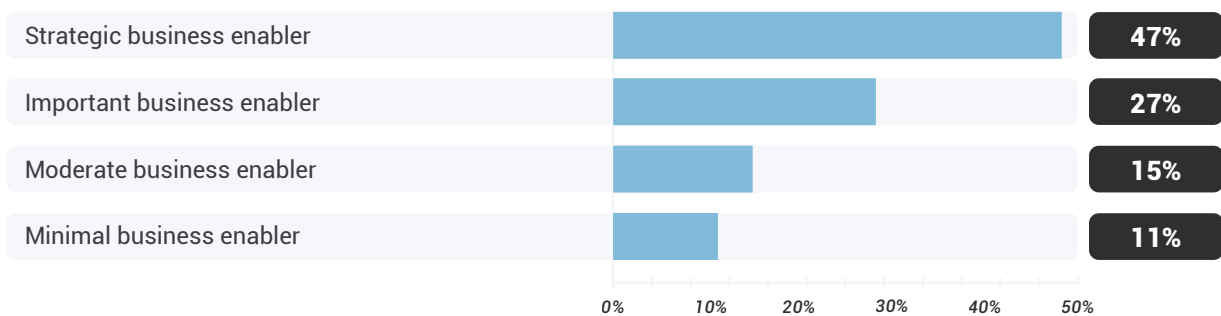




### What industry does your organization primarily operate in?



### On a scale of 1 - 5, how would you rate your organization's overall cybersecurity maturity?



# **SECTION #2**

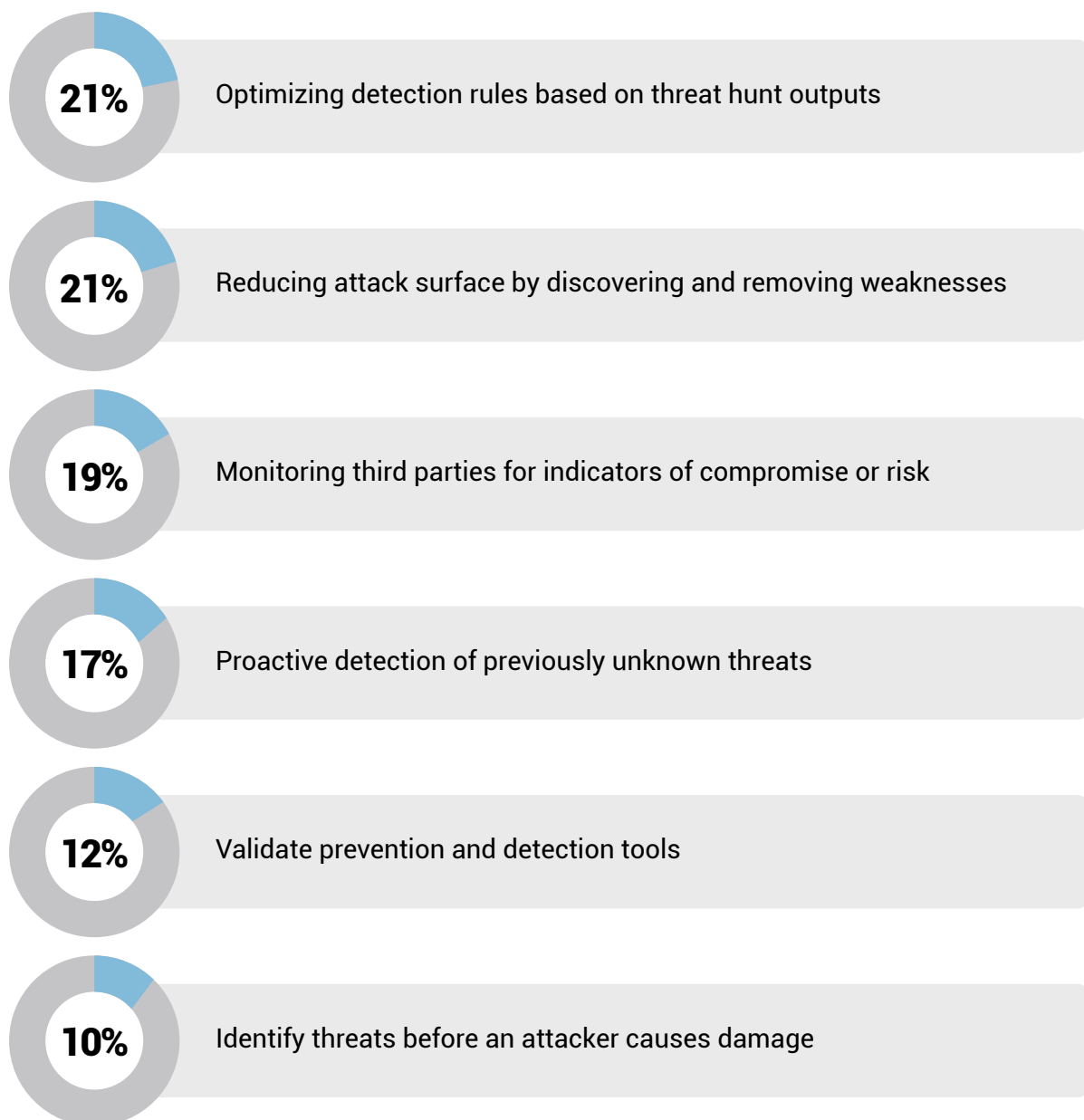
---

## **The State of Current Threat Hunting Program**

As attack surface risks remain dynamic, and as malicious actors evolve to become more sophisticated in their methods of discovering and exploiting security gaps, security teams are tasked with finding increasingly effective ways of protecting their organizations. One of those methods is external threat hunting, alternatively known as threat reconnaissance, which organizations can use to proactively search for active threats outside network borders before they evolve to costly cyberattacks. Here's where organizations stand with their threat hunting programs today.

## Top Three Objectives of a Threat Hunting Program

The top objectives respondents aim to achieve with their threat hunting program include:



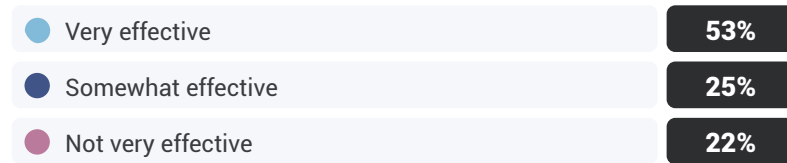
Validate prevention and detection tools 12.50%Other objectives include optimizing detection rules based on threat hunt outputs (17%), identifying threats before an attacker causes damage (15%), and validating prevention and detection tools (10%).

## Half believe their threat hunting program is very effective

53% believe their current threat hunting program is very effective. 25% believe it's somewhat effective, and 23% believe it's not very effective.

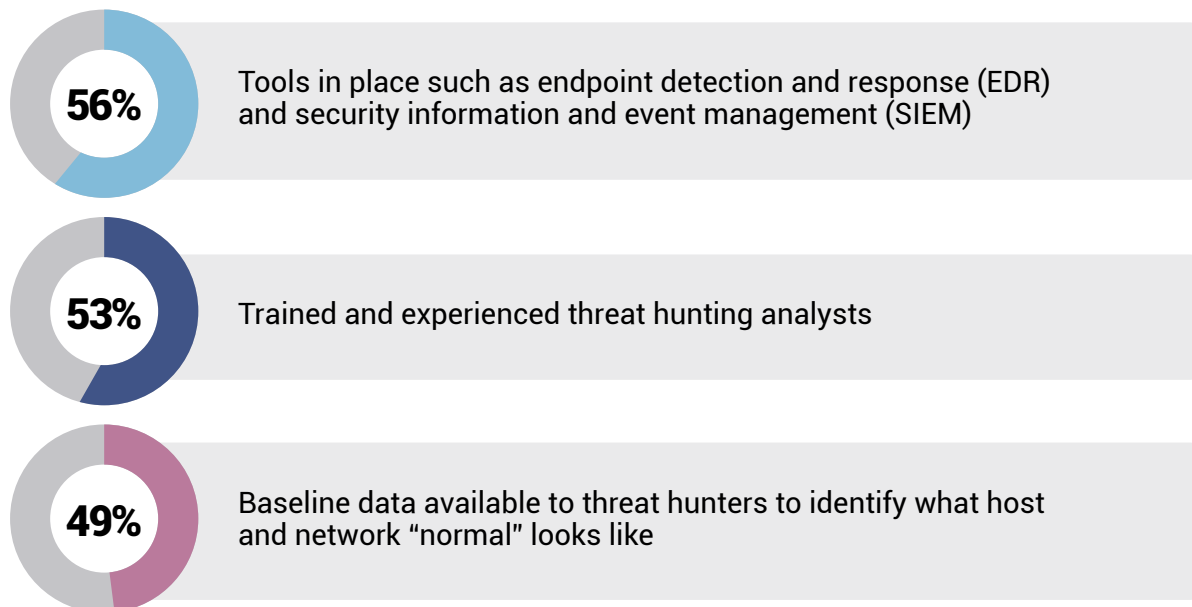


Overall, how would you rate the effectiveness of your current threat hunting program?



## Top Three Factors of a Successful Threat Hunting Program

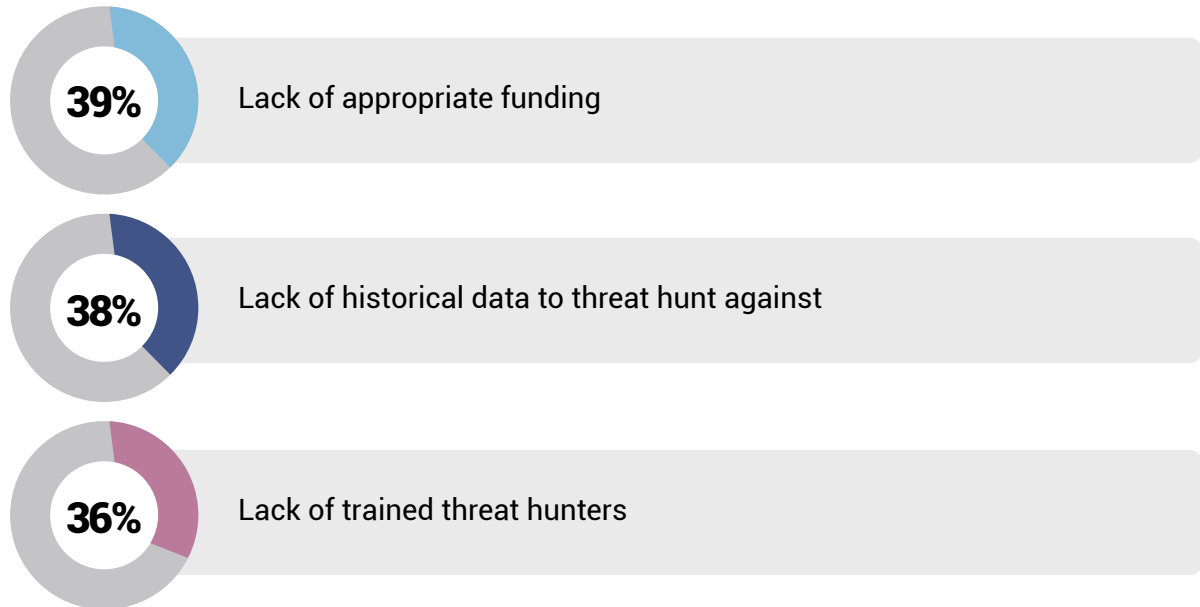
For those who answered "very effective," the top factors that make their threat hunting program successful are:



Other factors include tools in place such as threat intelligence (45%), ease of use with tooling (44%), formalized processes and procedures for conducting threat hunts (42%), tools in place such as forensic tools (40%), and appropriate levels of funding (34%).

## Top Three Most Challenging Factors of a Threat Hunting Program

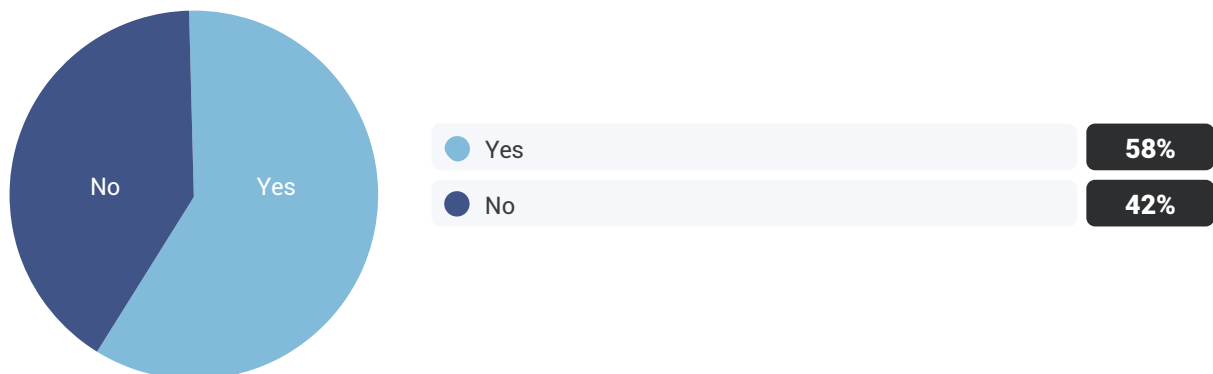
What makes their threat hunting program challenging include:



Other factors include a lack of tools to perform threat hunting with (34%), lack of host or network visibility (32% tie), poorly understood and/or undocumented baseline activity (32% tie), too many tools and/or too many alerts (alert fatigue) (32% tie), no executive-level support of threat hunt program (28% tie), and lack of visibility outside the internal network or lack of internet telemetry (28% tie).

## 58% outsource their threat hunting

58% of respondents outsource their threat hunting-related work, while 42% do not.

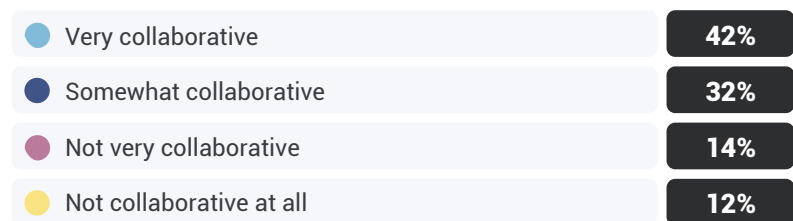


## 74% say threat hunting and other security functions are “very” or “somewhat” collaborative

When assessing the level of collaboration between their threat hunting team and other cybersecurity functions within their organization, 42% say they're very collaborative. 32% say they're somewhat collaborative, while 14% say they're not very collaborative. 12% say they're not collaborative at all.

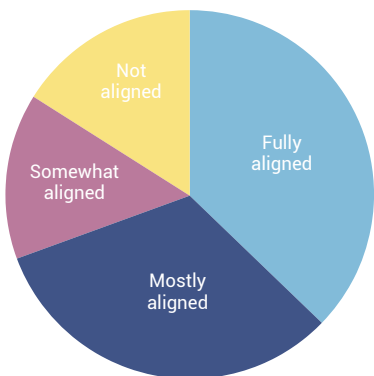


How do you assess the level of collaboration between your threat hunting team and other cybersecurity functions within your organization?

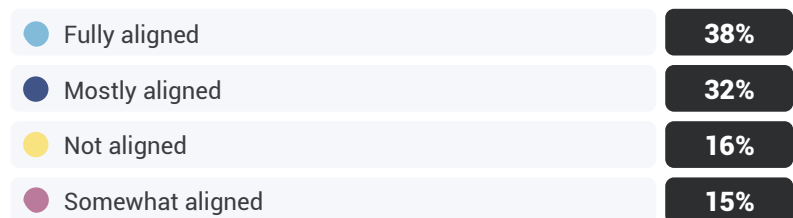


## 70% say threat hunting is “fully” or “mostly” aligned with overall security objectives

38% say their threat hunting activities are fully strategically aligned with their organization's overall cybersecurity objectives. 32% say they're mostly aligned, while 15% say they're somewhat aligned. 16% say they're not aligned at all.



How strategically aligned do you believe your threat hunting activities are with your organization's overall cybersecurity objectives?



## Summary

The current state of threat hunting is only half of those who responded feel it's effective.

*53% believe the effectiveness of their current threat hunting program is very effective.*

*25% believe it's somewhat effective, leaving 23% who believe it's not very effective.*

The top objective for their threat hunting program is the proactive detection of previously unknown threats, which demonstrates a focus more on threat reconnaissance and preventing attacks before they begin by learning which outside threats are most relevant.

Those who find their threat hunting program very effective attribute their success to detection tools like EDRs and SIEMs and having baseline data to identify what "normal" looks like so those detection tools can alert to what's not normal. They also attribute their success to having experienced threat hunting analysts who know how to use these tools and what to look for.

However, the biggest challenge to realizing that objective is a lack of funding, which can deprive security teams of those tools and experienced team members. Other obstacles include a lack of historical data to threat hunt against and a lack of trained threat hunters – two elements of a successful program.

Given the importance of integrating threat hunting and reconnaissance into their overall security approach, 74% say the level of collaboration between their threat hunting team and other cybersecurity functions is 'very' or 'somewhat' high. 70% say threat hunting activities are "fully" or "mostly" aligned with their overall security objectives.

# **SECTION#3**

---

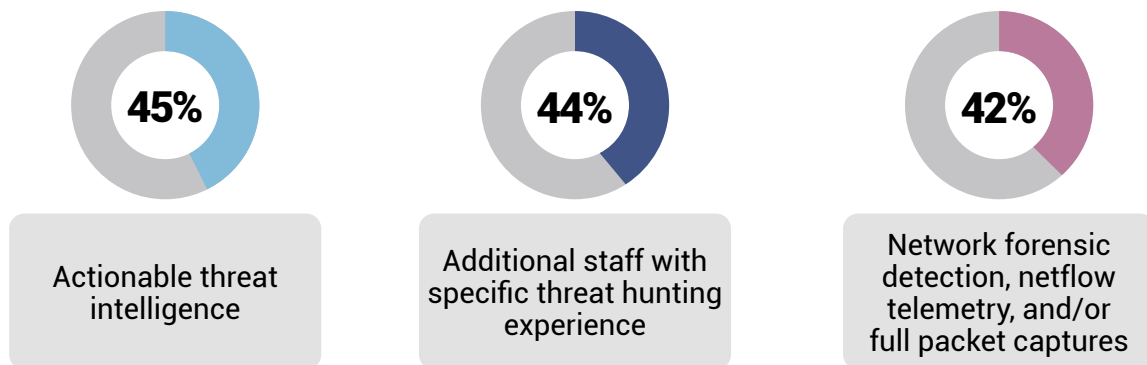
## **Tools and Budget**



Not all threat hunting programs are the same, as each industry and organization size will dictate much of the size, scale, and requirements for the team involved. To effectively protect against attack, organizations need both advanced tools with features that will successfully produce results and the budgets to acquire those tools. This section examines what threat hunting tools security teams use and how they're paying for them.

### Top Three Threat Hunting Program Enhancements

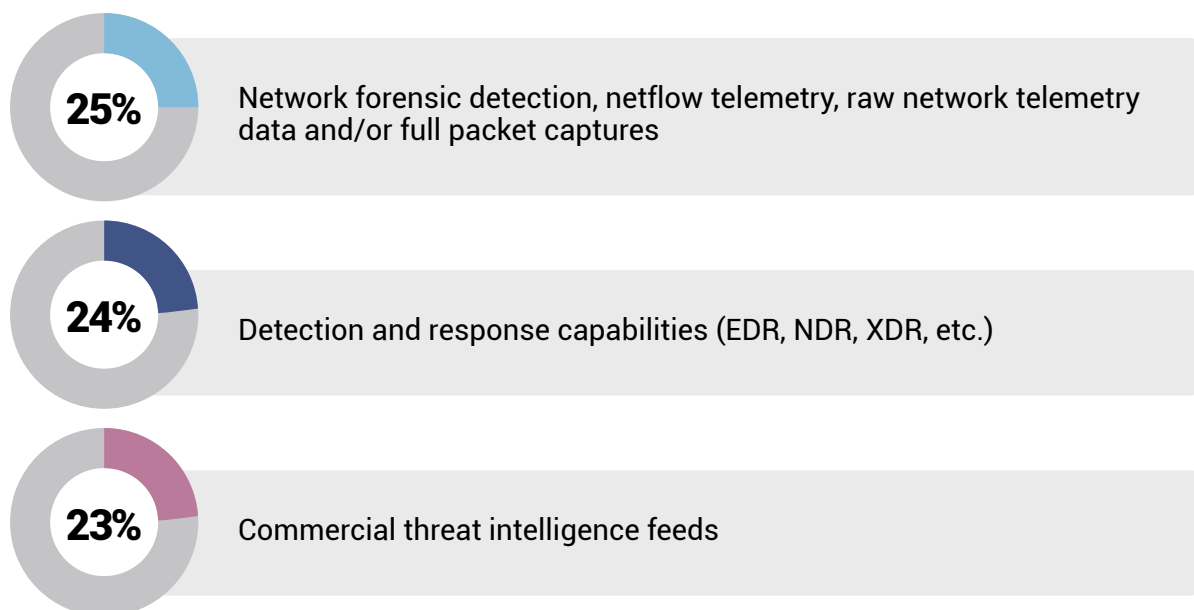
The enhancements respondents would like to add to their existing threat hunting program include:



Other enhancements include visibility across all assets that need to be protected (31%), an EDR tool (30%), automation (including workflows and actions) (29%), a SIEM/SOAR (27% tie), access to internet telemetry (27% tie), and enterprise host forensic capability (25%).

### Top Three Most Valuable Threat Hunting Products

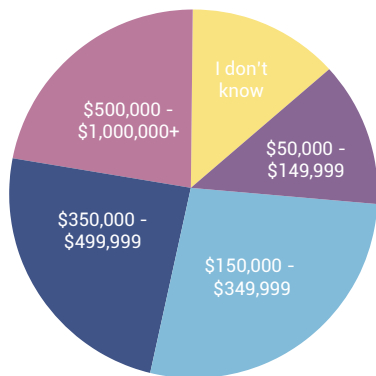
These threat hunting products are the most valuable to respondents:



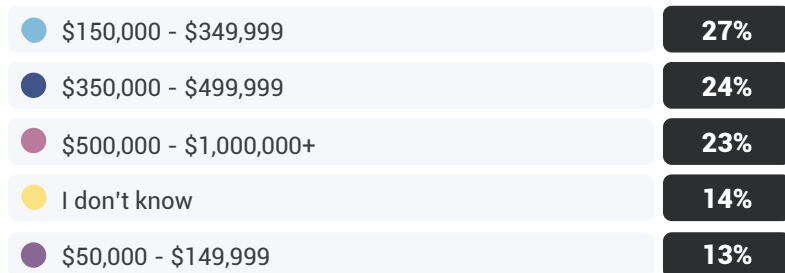
Other products include enterprise host forensic capability (14% tie) and a SIEM/SOAR (14% tie).

## 51% have threat hunting budgets between \$150,000 and \$499,999

13% have a threat hunting budget, including labor, tools, and any contracts, between \$50,000 and \$149,999. 27% have a budget between \$150,000 and \$349,999. 24% have a budget between \$350,000 and \$499,999. 23% have a budget between \$500,000 and \$1,000,000+. Finally, 14% don't know their threat hunting budget.

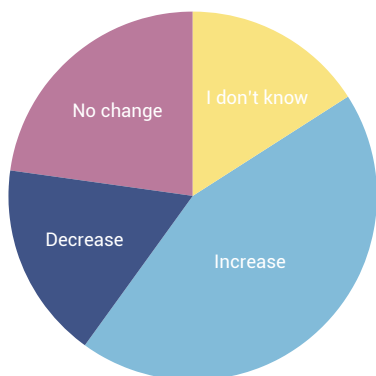


What is your annual budget specific to threat hunting (including labor, tools, and any contracts)?

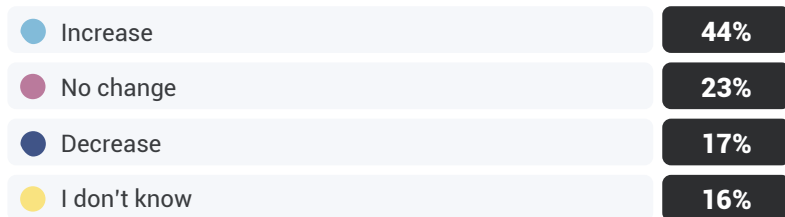


## 44% will see increased threat hunting budgets

44% say their budget for threat hunting will increase over the next year. 23% say there will be no change while 17% say their budget will decrease. 16% don't know.

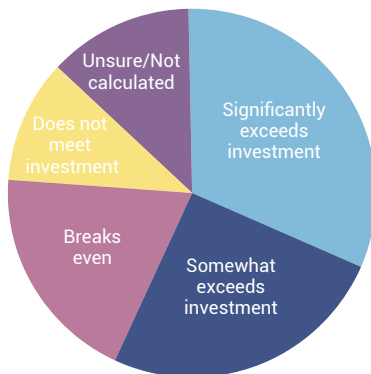


How is your budget for threat hunting going to change over the next 12 months?



## 57% see an ROI on their threat hunting activities

32% say the return on investment (ROI) from their threat hunting activities significantly exceeds investment. 25% say it somewhat exceeds investment. 19% break even on their ROI, while 11% say it does not meet investment. 13% were unsure how to calculate it or don't calculate it.



### How do you rate the return on investment (ROI) from your threat hunting activities?



## Summary

In the previous section, the top contributor to an effective threat hunting program was the tools the security team had in place. When it comes to the most valuable tools or products, security teams are turning to network forensic detection, netflow telemetry, raw network telemetry data and/or full packet captures, commercial threat intelligence feeds, and detection and response capabilities like EDR, NDR, or XDR.

To improve and enhance their threat hunting program, respondents would like to add actionable threat intelligence, additional staff with specific threat hunting experience, and network forensic detection, netflow telemetry, and/or full packet captures.

But effective tools need the budgets to purchase them. 51% of respondents say their threat hunting budget is between \$150,000 and \$499,999, while 23% have a budget between \$500,000 and \$1,000,000+. 44% say their budget for threat hunting will increase over the next year – however, for 66%, it will not.

# **SECTION #4**

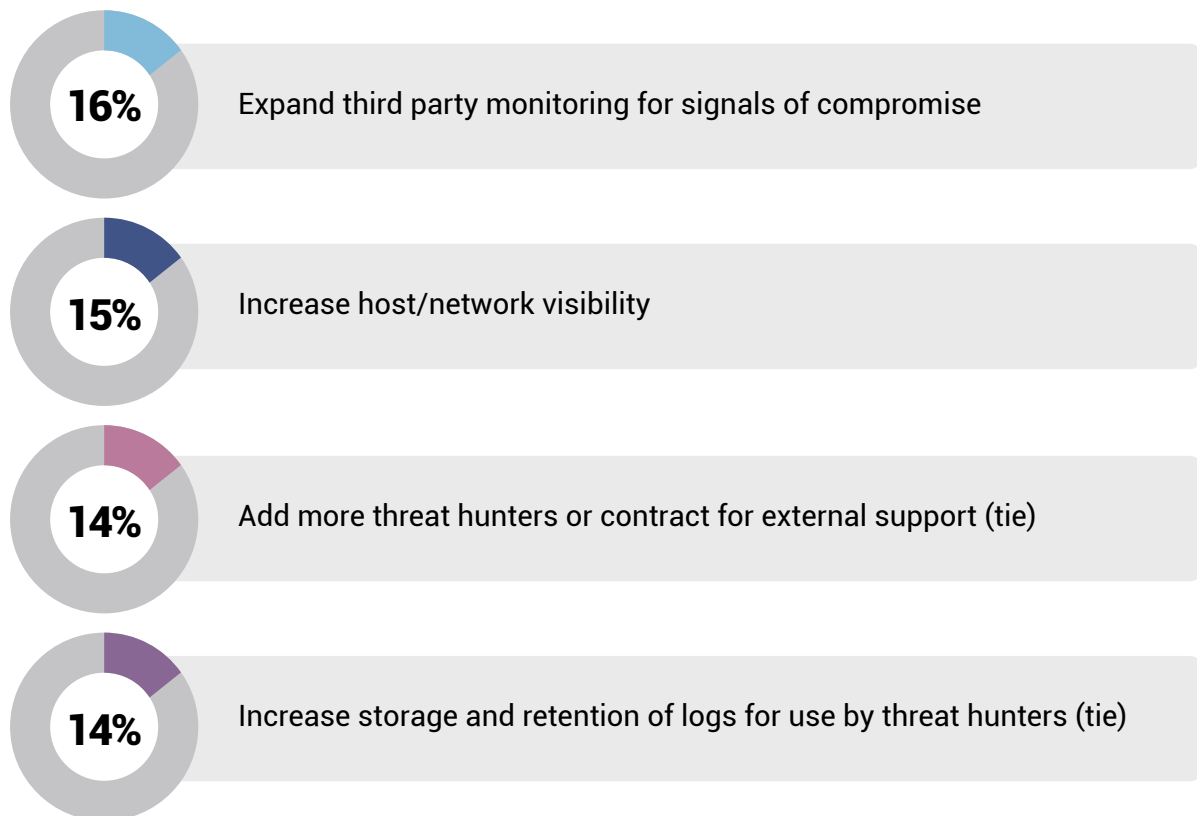
---

## **Threat Hunting Priorities**

Is their threat hunting program successful? What could they do to improve their impact, increase knowledge of threat actors to raise awareness, and reduce risk? Here, security teams give their feedback on future priorities for strengthening their threat hunting program, their greatest worries, and what they wish they could improve.

## Top Priorities of a Threat Hunting Program

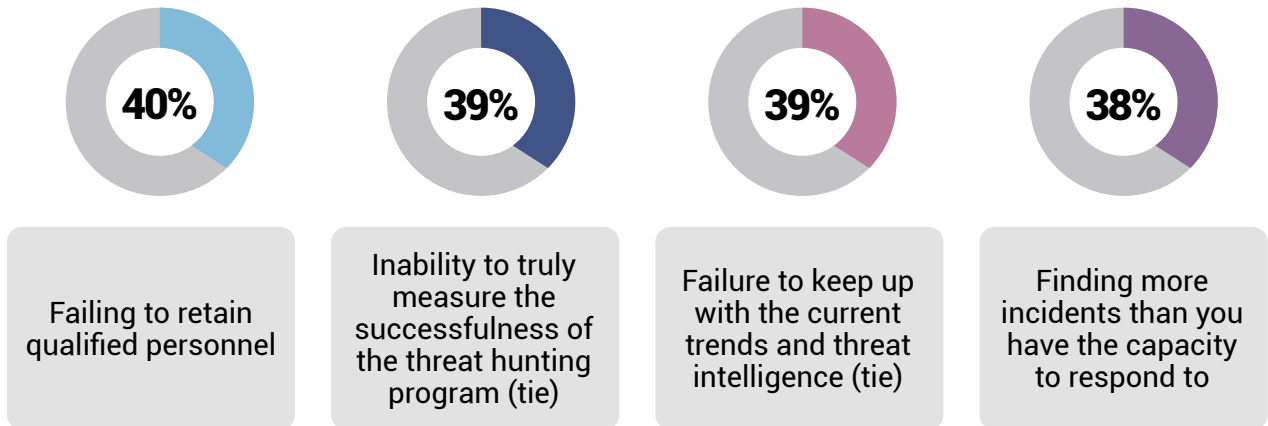
Respondents say the priorities for their threat hunting program over the next 12 months are:



Other priorities include reducing the mean time to detect and remediate threats (13%), investing in new tooling to perform threat hunting with (12%), establishing baseline activity for hosts and networks (9%), and training new hires (8%).

## Top Worries About Threat Hunting Activities

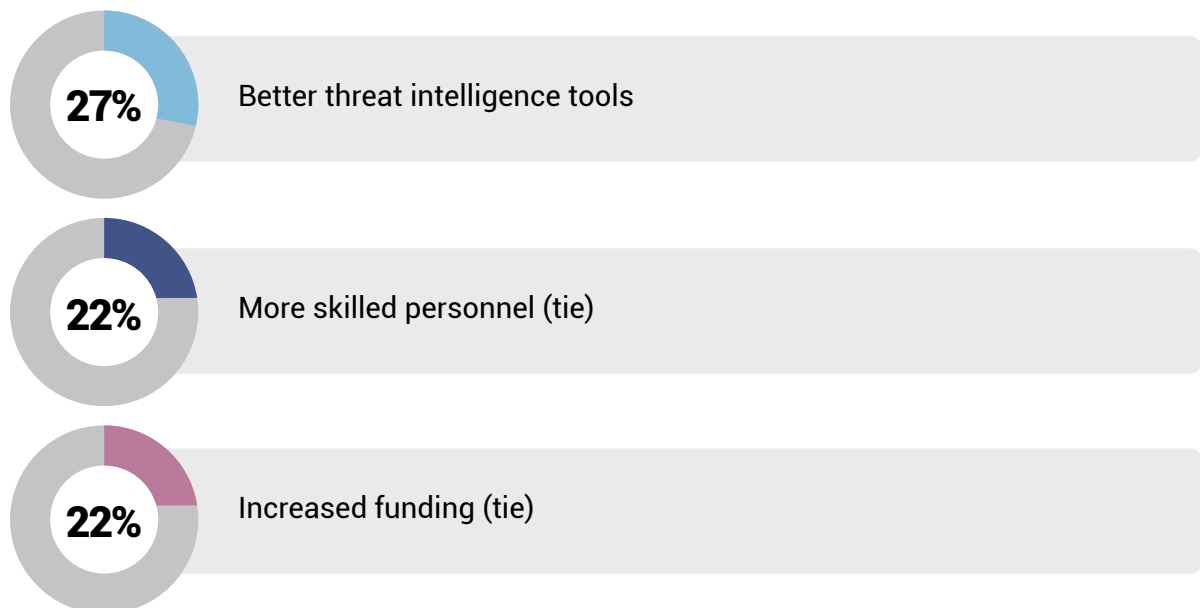
The pitfalls respondents most worry about with their threat hunting activities include:



Other pitfalls includes senior management lacking understanding of value (34% tie), tool effectiveness (34% tie), ease of use for tools and processes (31%), management adopting new technologies like AI (29%), cognitive bias and fatigue of threat hunters (28%), and attribution (21%).

## Top Three Ways to Improve Threat Hunting

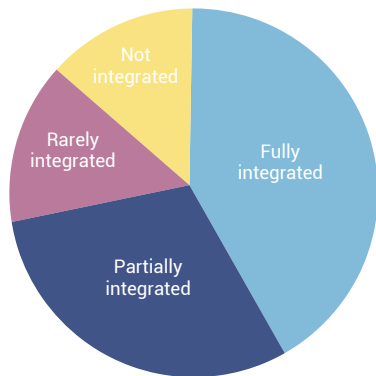
If respondents could have one wish granted to improve their threat hunting program, it would be:



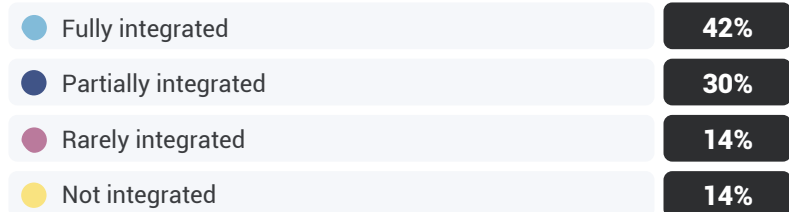
Other wishes include better integration with other security functions (17%) and more training opportunities (12%).

## 42% have fully integrated threat intelligence into their threat hunting activities

42% say threat intelligence is fully integrated in their day-to-day threat hunting activities. 30% say it's partially integrated, while 14% say it's rarely integrated. 14% say it's not integrated at all.



### How integrated is threat intelligence in your day-to-day threat hunting activities?



## Summary

To improve their threat hunting program over the next year, respondents intend to prioritize their efforts on expanding third party monitoring for signals of compromise, and increasing host or network visibility. They also intend to add more threat hunters or contractors for external support and increase storage and retention of logs for use by threat hunters.

But despite those intentions, respondents are also worried about failing to retain qualified personnel and that they'll be unable to truly measure the successfulness of the threat hunting program. They're also worried about failing to keep up with the current threat intelligence trends and finding more incidents than they have the capacity to respond to.

Ultimately, if respondents could have one wish granted to improve their threat hunting program, the majority asked for better threat intelligence tools, with the next most wished for being more skilled personnel, and increased funding.

# **SECTION #5**

---

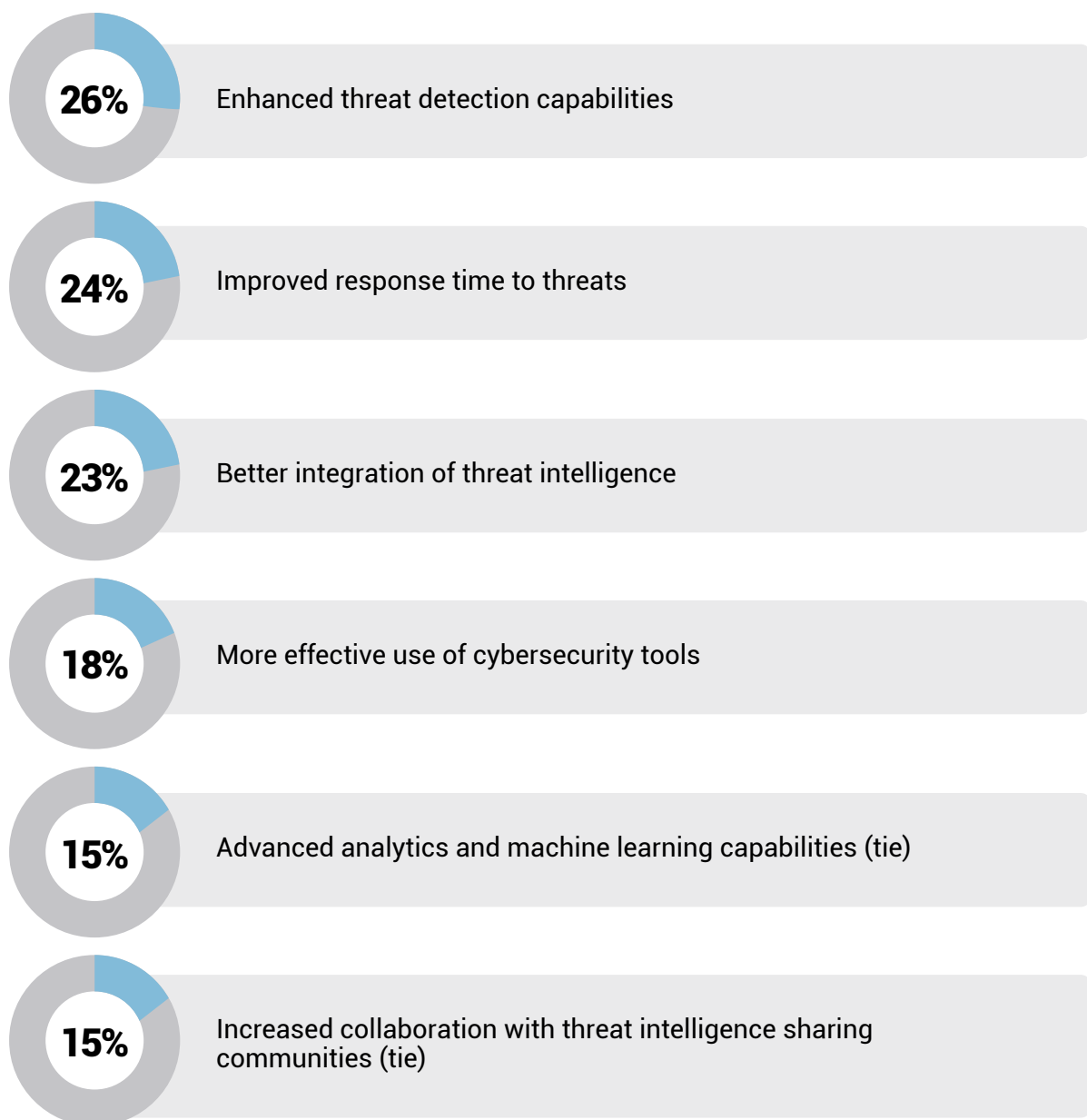
## **Threat Hunting Performance and Measures**



In this section, respondents tell us how their threat hunting program is performing and how effective it is at mitigating threats or breaches. The adage says that “You can’t manage what you don’t measure,” and to have an effective, always-evolving threat program, respondents share what they’re measuring and how they’re making improvements.

## Top Threat Hunting Improvements

The following improvements have been most significant in respondents’ threat hunting programs over the last year:



Other improvements include increased budget and resources (13%), enhanced network behavior analysis (11%), strengthened incident response and disaster recovery protocols (10% tie), expanded digital footprint coverage through external monitoring (10% tie), customized threat intelligence feeds (9%), enhanced training programs for threat hunting staff (8% tie), implementation of proactive threat hunting methodologies (8% tie), and access to comprehensive global threat intelligence data (8% tie).

### Half experienced a security breach in the past year

49% have experienced a major security breach in the past 12 months. 32% have not and 19% don't know if they have.



### 72% say threat hunting prevented or mitigated the breach

For those who experienced a breach, 72% say their threat hunting program played a key role in preventing or mitigating the breach. 28% say the program had no significant impact on the breach's outcome.



## Top Three Threat Hunting KPIs

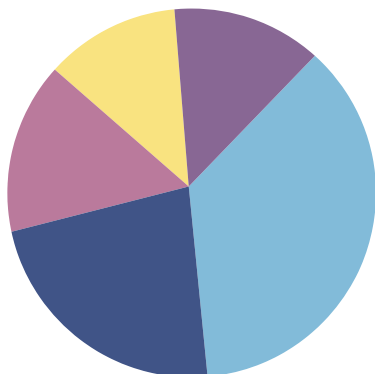
Respondents use the following Key Performance Indicators (KPIs) to measure the success of their threat hunting program:



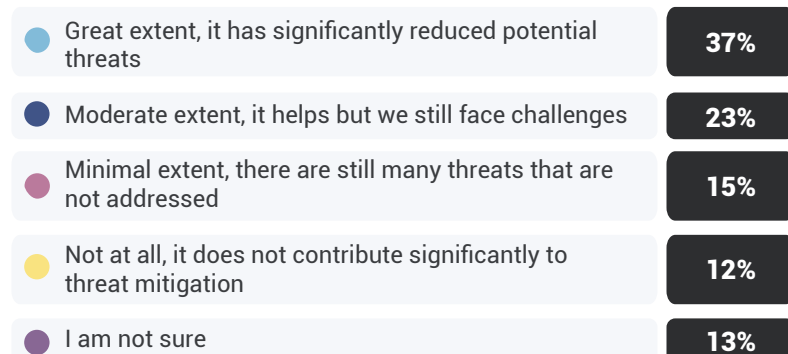
Other KPIs include cost savings due to proactive threat mitigation (13% tie), feedback from employees and management (13% tie), number of false positives and negatives (11%), and time taken to detect threats (10%).

## 60% say threat hunting helps significantly and moderately mitigate potential threats

37% say their program has helped mitigate potential threats to a great extent by significantly reduced potential threats. 23% say it has mitigated threats to a moderate extent, but they still face challenges. 15% say it has to a minimal extent, but there are still many threats that are not addressed. 12% say it hasn't helped at all and does not contribute significantly to threat mitigation. 13% are not sure of its impact.



### To what extent do you think your threat hunting program helps in mitigating the potential threats?



## Top Three Identified Threats

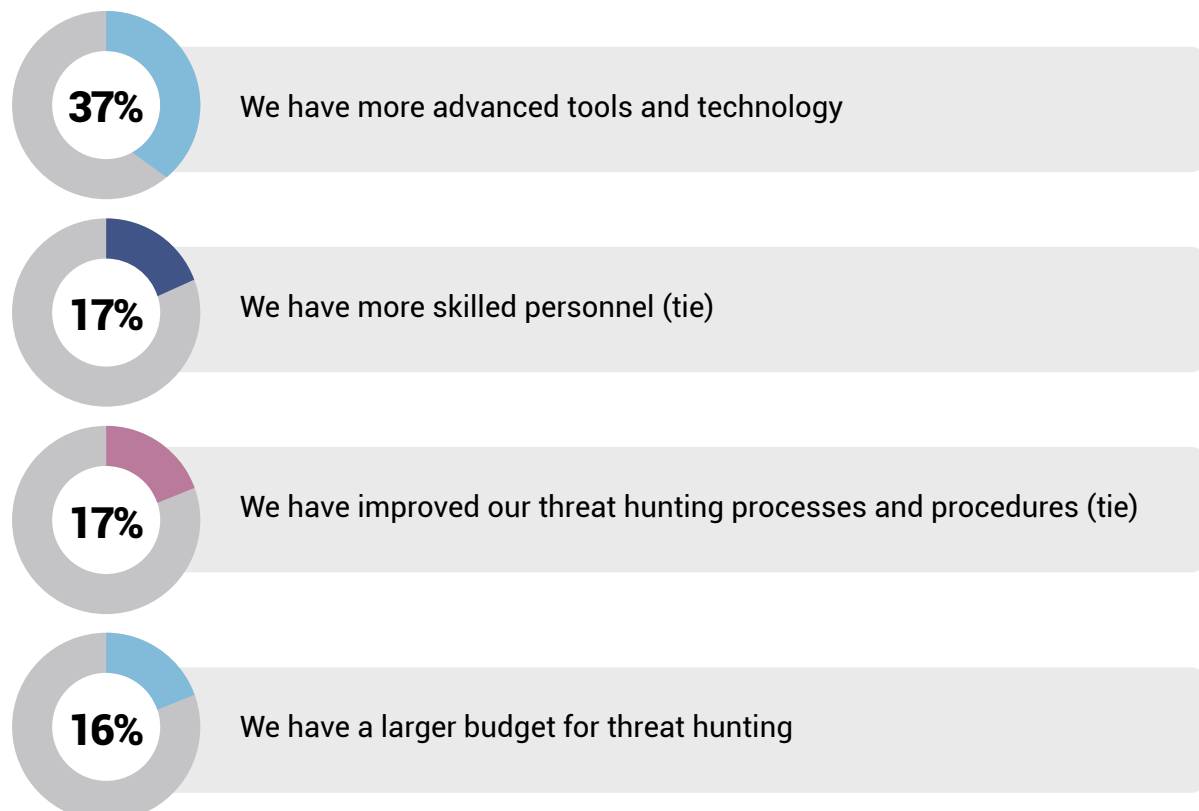
The following types of threats are what their threat hunting program has been most successful at identifying:



Other threats include malware infections (13% tie), unauthorized access attempts (13% tie), distributed denial-of-service (DDoS) attacks (10%), and insider threats (9%).

## Top Threat Hunting Program Evolutions

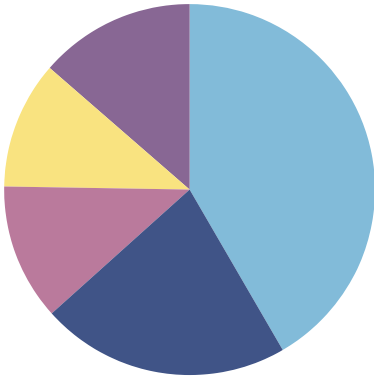
Respondents' threat hunting programs have evolved over the past year in the following ways:








## Only 42% say threat hunting is “very” integrated with other security functions

42% say their threat hunting program is very integrated, and that their threat hunting program works closely with all other security functions, this level of integration is optimal and gives security teams a speed advantage over those who aren't as integrated.

The remaining 58% have less integration, showing that many teams lag behind in fulfilling their true value and potential, putting further investment at risk. 22% say it's somewhat integrated, and that there is some collaboration but also room for improvement. 12% say it's not very integrated and that the threat hunting program operates largely independently. 11% say it's not at all integrated and that there is little to no collaboration with other security functions. Finally, 14% are unsure how well it's integrated.



### How well integrated is your threat hunting program with other security functions in your organization?

 Very integrated, our threat hunting program works closely with all other security functions	<b>42%</b>
 Somewhat integrated, there is some collaboration but also room for improvement	<b>22%</b>
 Not very integrated, the threat hunting program operates largely independently	<b>12%</b>
 Not at all integrated, there is little to no collaboration with other security functions	<b>11%</b>
 I am not sure	<b>14%</b>

## Summary

49% of respondents said their organization experienced a major security breach in the past 12 months. Of those that did, however, 72% say their threat hunting program played a key role in preventing or reducing the effect of the breach. 60% also say threat hunting helps significantly and moderately mitigate potential threats.

The top threat hunting improvements they've made over the past year which likely helped mitigate those compromises include enhanced threat detection capabilities, improved response time to threats, and better integration of threat intelligence. Over the past year, they've also evolved their threat hunting program by having more advanced tools and technology, more skilled personnel, improving their threat hunting processes and procedures, and increasing their budget for threat hunting.

The top KPIs they're using to measure the performance of their threat hunting program include number of threats detected and mitigated, time taken to respond to and mitigate threats, and the reduction in the number of successful breaches over time. Additionally, the top threats they've identified with their threat hunting program are ransomware related activity, phishing attacks, and advanced persistent threats (APTs).

Finally, 64% say threat hunting is "very" or "somewhat" integrated and that their threat hunting program works closely with all other security functions, but there's also room for improvement.



# **SECTION #6**

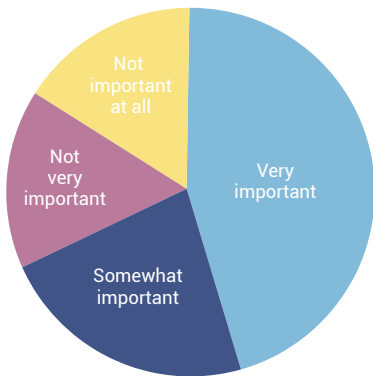
---

## **Outlook**

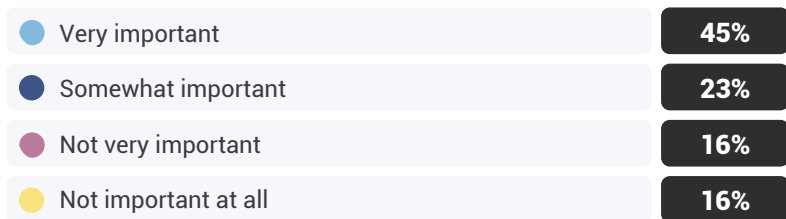
Cyber attacks are only going to continue to increase and security teams will always be racing to stay one step ahead of malicious actors. How will security practitioners continue to evolve their training and knowledge to face those increasing challenges? Respondents here share their career preferences and outlook.

### 68% say the availability of career opportunities are “very” or “somewhat” important

45% say the availability of career development and advancement opportunities within their threat hunting role is very important. 23% say it's somewhat important while 16% say it's not very important. 16% say it's not important at all.

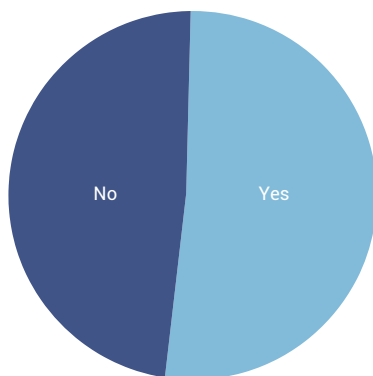


How important is the availability of career development and advancement opportunities within your threat hunting role?

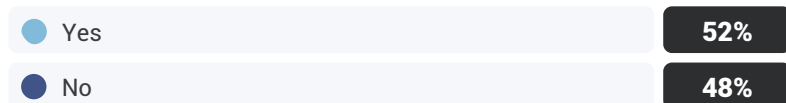


### Half would go to another organization for more training opportunities

52% say they would quit their job today to go work at an organization that offered more advanced cybersecurity training and certification opportunities if it paid 10% less, while 48% say they would not.



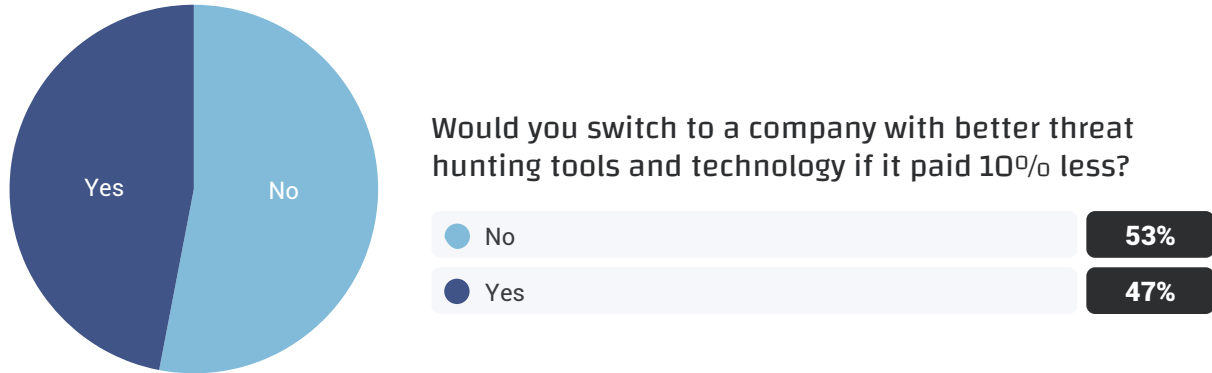
Would you quit your job today to go work at an organization that offered more advanced cybersecurity training and certification opportunities if it paid 10% less?





## Half would go to another organization with better threat hunting tools

53% say they would quit their job today to go work at an organization that offered better threat hunting tools and technology if it paid 10% less, while 47% say they would not.



### Summary

When it comes to the future outlook of their career, 68% say the availability of career development and advancement opportunities within their threat hunting role are “very” or “somewhat” important to them. About half would quit their job today to go work at an organization that offered more advanced cybersecurity training and certification opportunities if it paid 10% less. Additionally, about half would quit their job today to go work at an organization that offered better threat hunting tools and technology if it paid 10% less.

# **SECTION#7**

---

**Actionable Takeaways  
For Threat Hunting  
Team Leaders**

An organization needs a threat hunting program for better security, and as seen above, three out of four security practitioners said that their threat hunting program played a key role in preventing or mitigating the breach. Based on the responses above, here are some ways you can improve your threat hunting program today.

## Tools

A common theme throughout was having the right tools for threat hunting: it's a key factor in their success and a place where they've evolved their threat hunting program in the past year.

Look for tools that can give you increased visibility into your networks and environments, and that can map your attack surface, alerting to vulnerabilities and areas waiting for compromise. This can include EDRs and SIEMs, or tools for network forensic detection, netflow telemetry, raw network telemetry data and/or full packet captures, or commercial threat intelligence feeds.

Invest in tools that provide you with actionable threat intelligence that's specific and relevant to your organization as well. This will not only help you be more proactive in your threat hunting because you'll be able to narrow down which threats are targeting your organization. With tools that provide streamlined intelligence, you'll reduce the time and effort it takes to sift through outdated reports so you can respond faster.

## Training

It's no surprise that when there's a cybersecurity talent shortage, and when teams are being stretched thin, respondents say that one of their biggest challenges is a lack of trained threat hunters. They also wish for more skilled personnel and to improve their threat hunting, they would add additional staff with specific threat hunting experience.

It doesn't necessarily have to be a wish. With the right tools and training, your team can become skilled threat hunters and add that capability to your portfolio of strategies. Implementing other tools like automation and AI that can handle manual, repetitive tasks frees up your security team to focus on proactive threat hunting as well.

## Funding

Their biggest challenge is a lack of appropriate funding for their threat hunting program. They also wish for increased funding, and while 44% say their budget for threat hunting will increase over the next year, 66% said it won't.

Increasing an already tight budget can be done in two ways. First, optimize your budget by investing in tools and technology that will save time for your security team, like automation and AI. Investing in more advanced tools now will allow you to be more effective and have a higher ROI than investing in affordable tools that may not be as effective or may need upgrading in a year. Second, increase your budget with increased buy-in from leadership by recording and demonstrating how your security actions are saving the organization everyday from attack.

## Baseline data

Respondents attribute their successes to having baseline data available to threat hunters to identify what host and network “normal” looks like. Related to this, one of their worries is the inability to truly measure the successfulness of the threat hunting program, and one of their biggest challenges is a lack of historical data to threat hunt against. This signals a lack of tracking and visibility into an organization's assets and security actions.

Address this need by first making sure you have a comprehensive inventory of the assets, systems, and environments that need to be protected, and map your attack surface so you know your perimeter. Have a plan for increasing the storage and retention of your log data so that you can use it for future threat hunting, and document your past processes and procedures as well.

## Prioritize third-party monitoring

If security teams wish to demonstrate value, they need to recommend expanding third party monitoring for signals of compromise – which is not surprising considering the rise in third-parties being the largest source of a breach. Invest in threat intelligence tools that can help you proactively monitor not just your systems but third-party systems as well to scan for threats that may be targeting them. Additionally, just as you inventory your assets and map your attack surface, know exactly which vendors or suppliers have access to your systems. Consider implementing security questionnaires or assessments before onboarding new third parties as well.



## Recommendations:

### Focus on Proactive Threat Detection

Given the high importance placed on proactive detection, investments in advanced threat detection tools and training should be prioritized.

### Cross-Industry Collaboration

With significant representation from diverse industries, cross-industry collaborations can enhance threat intelligence and resilience.

### Enhance Maturity

For organizations not yet at a strategic level of cybersecurity maturity, targeted improvements in processes and tools can help elevate their status.

### Continuous Improvement

Regular assessment of the effectiveness of threat hunting programs and addressing challenges such as lack of visibility and trained personnel are crucial for maintaining high effectiveness.

## 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, investing in the right tools, people and strategies are critical to success.

Moreover, the insights gleaned from this survey can inform strategic decisions and guide organizations in implementing a robust threat hunting program to fortify their cybersecurity defenses beyond their network borders.

[Try Scout Insight Free](#)



**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](https://team-cymru.com)**