Voice of a Threat Hunter

TEAM CYMRU™
THE POWER OF PURE SIGNAL™

REPORT

Introduction

The threats to organizations are only increasing, not only in number but in scope. A cyber attack isn't just an inconvenience; it can grind operations to a standstill, and cost an organization millions of dollars.

This is why it's key to have a threat hunting program in place to proactively identify and investigate potential threats to an organization. Threat hunting can help organizations identify and fix vulnerabilities not found by other security tools, and find malicious activity that has gone undetected despite their best efforts. It can also enable organizations to respond more quickly to attacks.

But how well are security teams utilizing their threat hunting program to keep their organization safe? Are they confident in their threat hunting tools, or are they concerned there are gaps that could be exploited?

In order to better understand how security professionals use threat hunting to protect organizations, we surveyed 218 security analysts to learn what works and what doesn't in their threat hunting program, how they measure success, and the biggest challenges they face each day.

We hope these findings will help you design an effective threat hunting program, benchmark your current processes, or help you improve your protection overall.

David Monnier
Chief Evangelist | Team Cymru

Here are seven insights our respondents gave us into their current threat hunting programs.

- **Most say their threat hunting program is not very, or is only somewhat, effective.** *Without effective threat hunting, these organizations blindly make security decisions, such as which assets to protect and which countermeasures to deploy.*

- **A lack of proper tools impacts threat hunting effectiveness — but good training can improve it.** *Going without the right threat hunting tools is the biggest challenge for practitioners, but having trained and experienced analysts improves effectiveness the most.*

- **Wish lists include network forensic detection, NetFlow telemetry, and full packet captures.** *The majority said these are the things they would most like to add to their threat hunting program in order to detect and respond to threats more effectively.*

- **Enterprise host forensic capability is the most valuable threat hunting product.** *Analysts are looking to quickly and easily identify malicious behavior by tracking all activity on their network. This capability allows them to respond quickly to any threats and keep their organization safe.*

- **More threat hunting outsourcing is on the horizon.** *Most respondents say their organization outsources threat hunting, and the top priority for security practitioners over the next year is adding more threat hunters or contracts for external support.*

- **Threat hunting budgets are going up.** *Nearly half of respondents have a budget of $350,000 or more for threat hunting, and 38% believe their annual budget for threat hunting will increase, indicating a growing emphasis on and recognition of the importance of proactively identifying and mitigating cyber threats.*

- **Security teams are concerned about measuring success.** *Respondents said they are most worried about their inability to measure the success of their threat hunting program, which can lead to difficulties in making informed decisions, allocating resources effectively, and justifying the value of the threat hunting program to stakeholders.*

Table of Contents

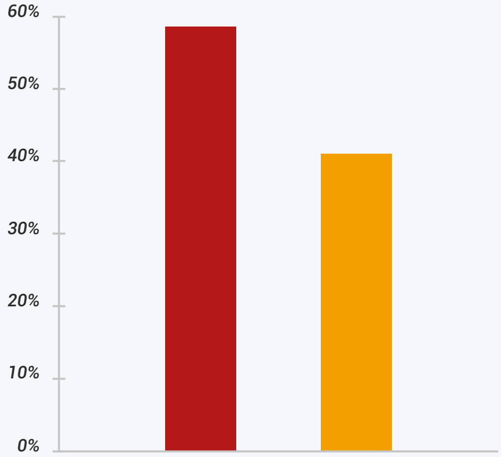
PART#1

Who We Surveyed

Methodology and Participant Demographics

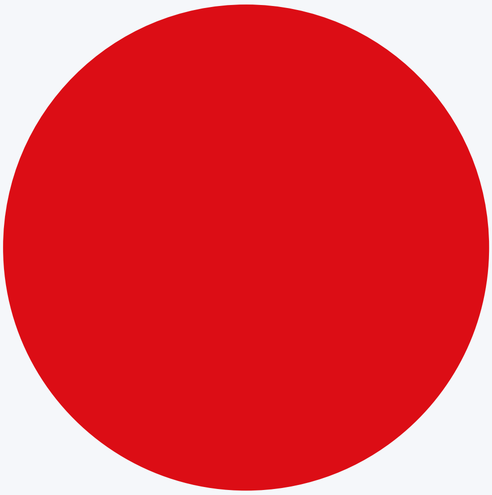
Starting on September 15, 2022, we surveyed 218 cybersecurity professionals that work in security analyst roles. The survey was performed online via Pollfish using organic sampling. To provide greater context around these findings, below are the details on who we surveyed and the methodology used. Learn more about the Pollfish methodology here.

Gender



● Male	59.0%
● Female	41.0%

Country

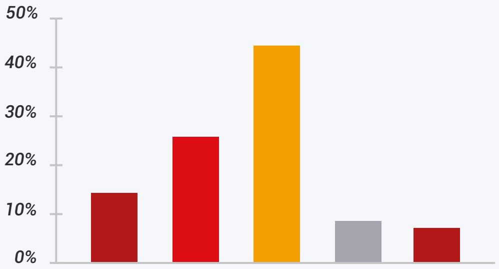


● United States	100.0%

Employment Status

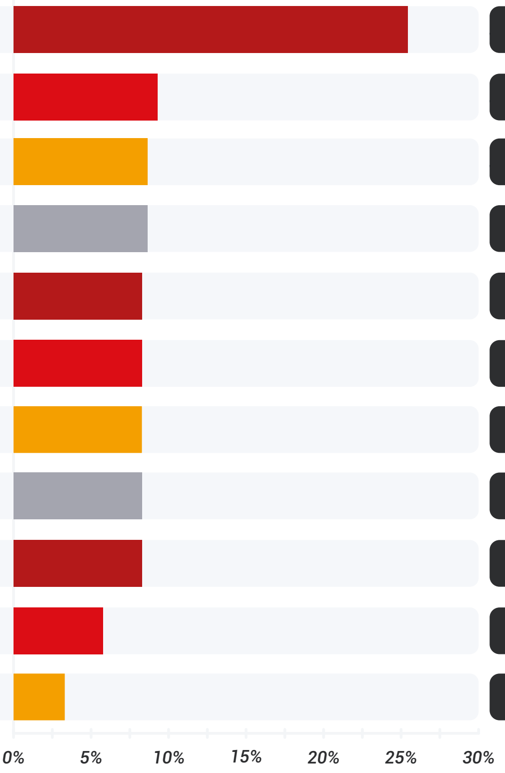
● Employed for Wages	100.0%

Age

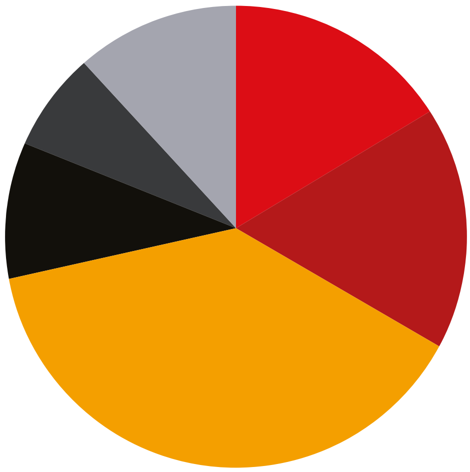


● 18 -24	13.2%
● 25 - 34	25.7%
● 35 - 44	43.5%
● 45 -54	9.3%
● >54	8.2%

What industry does your organization primarily operate in?



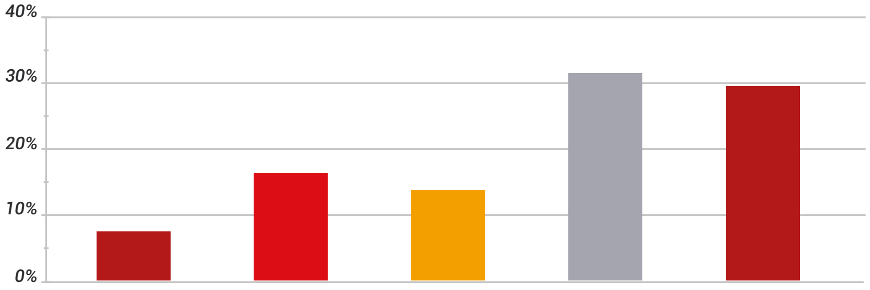
IT, technology, software	25.2%
Manufacturing	9.6%
Transportation/logistics	8.2%
State, local, federal government	8.2%
Financial services, insurance, real estate	7.8%
Higher education, K-12 education	7.8%
Healthcare, biotech, pharma, medical	7.8%
Marketing, advertising, media	7.8%
Retail	7.8%
Military/Defense	5.9%
Healthcare	3.6%



What best describes your job title?

● Cyber threat intelligence analyst	16.5%
● Incident handler/responder	17.4%
● Security analyst	38.5%
● Insider threat analyst	9.6%
● SOC analyst	7.3%
● Information security management	10.5%

On a scale of 1 - 5, how would you rate your organization's overall cybersecurity maturity? (1 least mature -- 5 extremely mature)



● 1	7.8%
● 2	16.0%
● 3	14.6%
● 4	31.6%
● 5	29.8%

PART#2

State of Threat Hunting

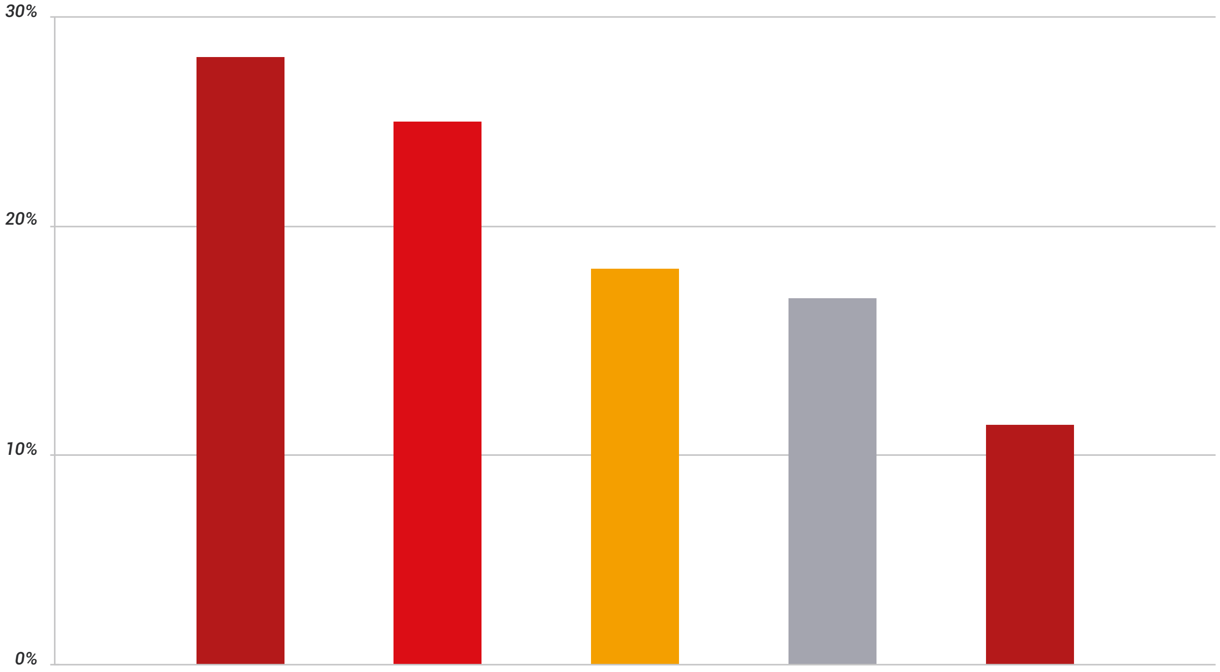
In cybersecurity, threat hunting has become critical for organizations of all sizes. By proactively searching for threats, security teams can mitigate and prevent costly data breaches. However, despite the importance of threat hunting, many organizations still struggle to implement an effective hunting program. This section will explore the current state of threat hunting and offer tips for making your organization's program more effective.

Top objectives to threat hunting include creating detection rules and identify threats before there's damage

To start, what is the top objective our respondents are hoping to achieve with their threat hunting program? The largest segment (28%) said they want to create detection rules based on threat hunt outputs. However, 24% say their top objective is to identify threats before an attacker causes damage.

Others say their top objective is to reduce the attack surface by discovering and removing weaknesses is the most critical (18.81%), proactive detection of previously unknown threats (18%), and to validate prevention and detection tools (11%).

What would you say are the top objective you are aiming to achieve with your Threat Hunting Program?

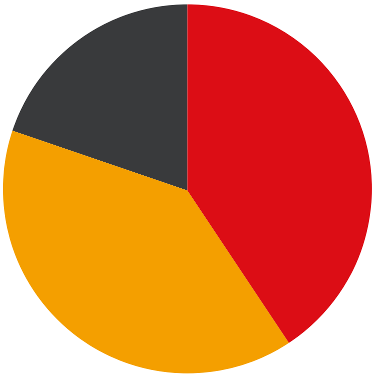


● Creating detection rules based on threat hunt outputs	28.0%
● Ability to identify threats before an attacker causes damage	24.0%
● Reducing attack surface by discovering and removing weaknesses	18.8%
● Proactive detection of previously unknown threats	18.0%
● Validate prevention and detection tools	11.0%

Only 41% think their threat hunting program is very effective.

Our survey revealed that many companies might not get the most out of their threat hunting efforts. 59% of respondents reported their program as either not very effective (21%) or only somewhat effective (38%) in mitigating threats.

This could be due to several factors, such as a lack of resources or inadequate training for hunters. Ultimately, without a properly functioning threat hunting program, organizations are unable to make informed decisions about their security, as they are unable to identify potential threats.

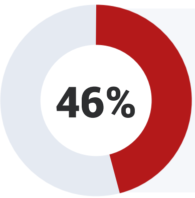


Overall, how effective would you say your current Threat Hunting Program is?

● Very effective	41.0%
● Somewhat effective	38.0%
● Not very effective	21.0%

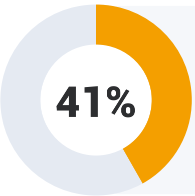
More than anything, trained and experienced analysts make threat hunting effective.

For those above who feel their threat hunting program is very effective, we asked them to select all the factors they felt made it so effective.



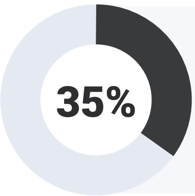
Trained and experienced threat hunting analysts

The number one reason why their threat hunting program is so effective is because of the analysts behind it.



Tools in place such as endpoint detection and response (EDR), security information and event management (SIEM)

The second most selected reason for an effective threat hunting program is the tools they have in place for detection, response, and overall visibility.

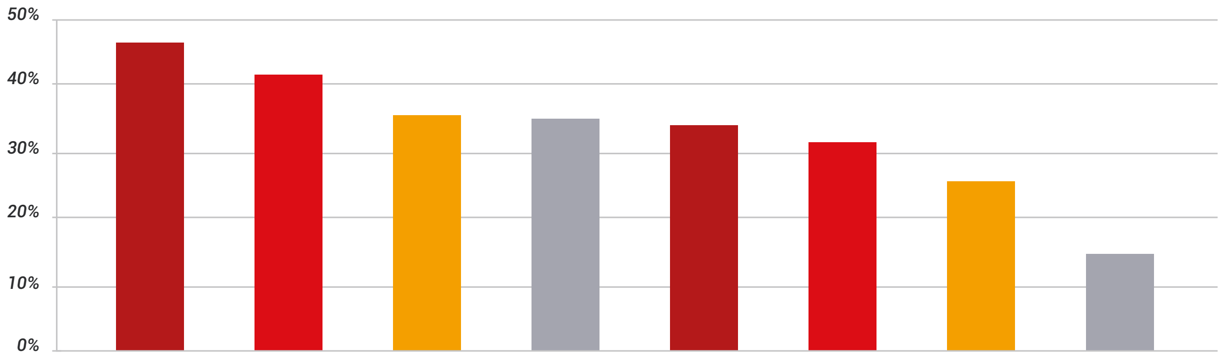


Formalized processes and procedures for conducting threat hunts

Respondents also said their threat hunting program is effective because of the structure they have in place to run it in a systemized manner.

Other reasons include threat intelligence tools (35%), forensic tools (33%), baseline data to identify what host and network "normal" looks like (31%), ease of use with tooling (26%), and appropriate levels of funding (15%).

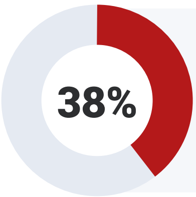
What would you say are the top factors that make your Threat Hunting Program so effective?



● Trained and experienced threat hunting analysts	46.0%
● Tools in place such as endpoint detection and response (EDR), security information and event management (SIEM)	41.0%
● Formalized processes and procedures for conducting threat hunts	35.0%
● Tools in place such as threat intelligence	35.0%
● Tools in place such as forensic tools	33.0%
● Baseline data available to threat hunters to identify what host and network “normal” looks like	31.0%
● Ease of use w/ tooling	26.0%
● Appropriate levels of funding	15.0%

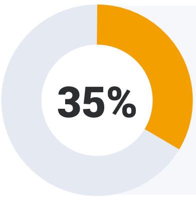
The lack of tools to perform threat hunting is the most challenging part of the respondents’ threat hunting program.

Now that we know about their threat hunting program’s effectiveness, or lack thereof, we wanted to know the top challenges they face in executing their program (they selected all that applied, and selections were pretty evenly chosen)?



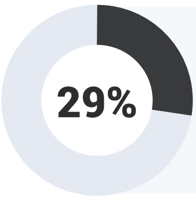
Lack of tools to perform threat hunting with

Their biggest challenge is that they lack the proper tools with which to perform success and thorough threat hunting. This can be compared to above, where effective threat hunters had the right tools to detect and mitigate threats.



Poorly understood and/or undocumented baseline activity

The second biggest challenge was a lack of adequately documented baseline activity with which to compare “normal” against.

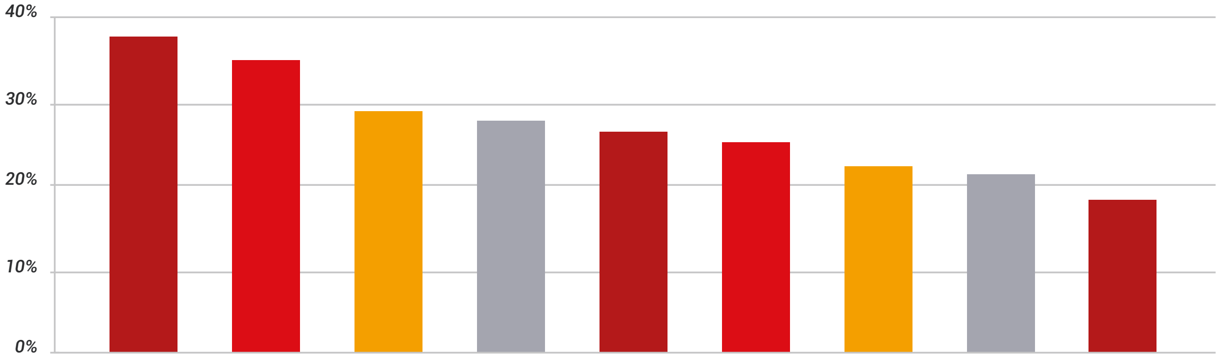


No executive-level support of threat hunt program

Unfortunately, no executive-level support, buy-in, and likely funding is their biggest challenge.

They also chose a lack of trained threat hunters (28%), lack of host/network visibility (27%), lack of historical data to threat hunt against (26%), lack of appropriate funding (23%), too many tools and/or too many alerts (22%), and a lack of visibility outside the internal network and/or lack of Internet telemetry (18%).

What factors make your Threat Hunting Program most challenging



●	Lack of tools to perform threat hunting with	38.0%
●	Poorly understood and/or undocumented baseline activity	35.0%
●	No executive-level support of threat hunt program	29.0%
●	Lack of trained threat hunters	28.0%
●	Lack of host/network visibility	27.0%
●	Lack of historical data to threat hunt against	26.0%
●	Lack of appropriate funding	23.0%
●	Too many tools and/or too many alerts (alert fatigue)	22.0%
●	Lack of visibility outside the internal network / lack of Internet telemetry	18.0%

More network data is what most would like to add to their program.

We asked respondents what they would like to add to their existing threat hunting program to make it more effective.

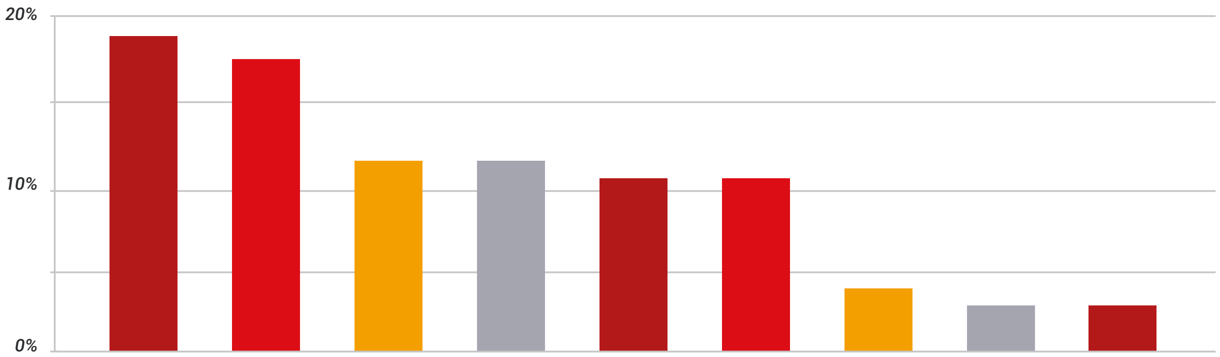
The largest segment (17%) said network forensic detection, NetFlow telemetry, and/or full packet captures was their number one choice, as by having access to this data, they would be able to detect and respond to threats more effectively.

Additional staff with specific threat hunting experience was chosen by 15% — especially since those with effective threat hunting programs cited well-trained staff as the reason for their success.

The need for endpoint detection and response tools (13%) and SIEM/SOAR platforms (13%) came in tied at third.

They also want automation across workflows and actions (11%), enterprise host forensic capability (11%), actionable threat intelligence (8%), access to internet telemetry (6%), and visibility across all assets that need to be protected (6%).

Of the following, what would you like to add to your existing threat hunting program?



●	Network forensic detection, netflow telemetry, and/or full packet captures	17.0%
●	Additional staff with specific threat hunting experience	15.0%
●	Endpoint detection and response tool	13.0%
●	SIEM/SOAR	13.0%
●	Automation (workflows and actions)	11.0%
●	Enterprise host forensic capability	11.0%
●	Actionable threat intelligence	8.0%
●	Access to internet telemetry	6.0%
●	Visibility across all assets that need to be protected	6.0%

Summary

What's the state of threat hunting at our respondents' organizations? In need of better tools and approaches, it seems. Less than half see their threat hunting program as very effective, though they say their success lies in having trained analysts at the helm, the right tools in place, and a formalized process for their procedures.

However, in order to improve their threat hunting programs, respondents say they need access to better data, as the lack of it is likely limiting their ability to make informed security decisions and take effective countermeasures to protect their assets. They also want to add more trained staff to their team, and better detection and management tools as well.

Overall, their challenges echo what they wish they could add to and improve with their approach. They're challenged by a lack of tools to perform threat hunting, a lack of awareness around their baseline, and a lack of support — buy-in, confidence, and budget — from above.

In this section, the survey respondents have illuminated where the threat hunting field stands today. Next, we'll probe the respondents for information about what they want to see in the future.

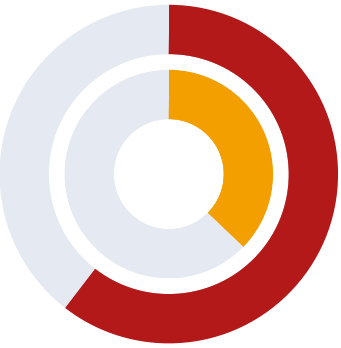
PART#3

Threat Hunting Priorities and Plans

In our last section, our survey respondents gave us a clear picture of the current state of threat hunting, and their need for better tools and more training. However, it's just as informative to consider where teams want it to go in the future. What are their priorities, and how will they help security teams achieve success in their threat hunting programs?

62% of respondents say their organization outsources threat hunting related work.

Only 38% approach their threat hunting in-house. The remaining 62% say their organization outsources it. Many organizations rely on outside vendors for their threat hunting needs, as it often requires specialized skills and resources. Considering that one of their concerns above is having people that are highly trained, then outsourcing would be a solution.

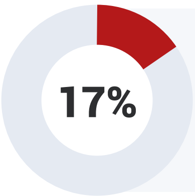


Does your organization outsource threat hunting related work?

● Yes	62.0%
● No	38.0%

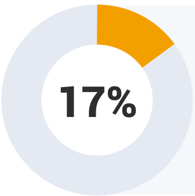
The top priority for security practitioners is to add more threat hunters and increase visibility.

With the increasing sophistication of cyber attacks, it is no longer enough for a security team to rely solely on traditional prevention and detection solutions. What are they prioritizing for their threat hunting program for the coming year?



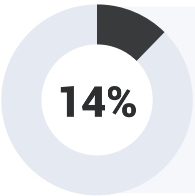
Add more threat hunters or contract for external support

Their top priority is related to the challenge they stated above: needing more analysts trained and experienced in threat hunting.



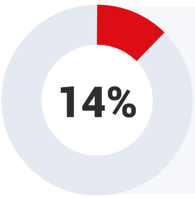
Increase host/network visibility

Their other top priority is to increase visibility into their network so that they have better insight into the weakness and vulnerabilities in their environment.



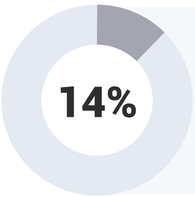
Establish baseline activity for hosts and networks

Considering that one of the challenges security teams face is not having a clear baseline, a secondary priority is to better establish "normal."



Increase storage and retention of logs for use by threat hunters

Another secondary priority is to better manage audit logs so that analysts can track access and movement.

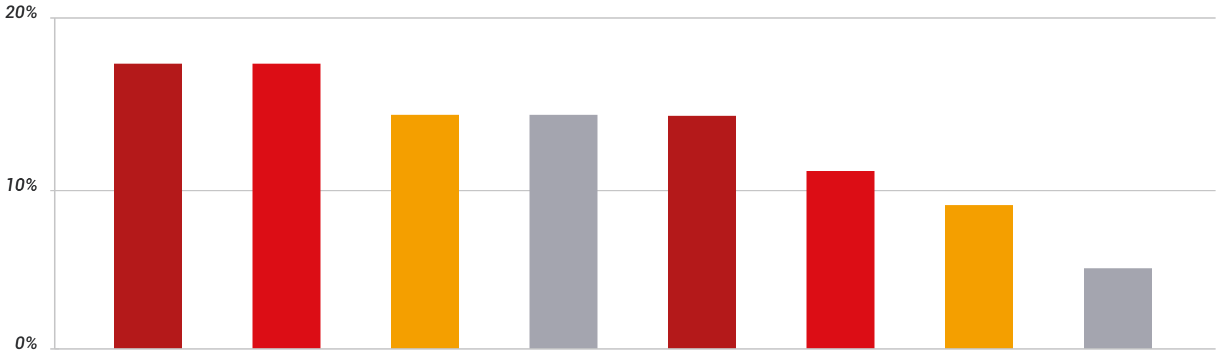


Investment in new tooling to perform threat hunting with

Another priority relates back to one of the elements they would add to their program: better tools for detection, response, and management.

They also want to expand third party monitoring for signals of compromise (11%), reduce the mean time to detect and remediate threats (9%), and train new hires (5%).

What would you say is your #1 priority of your Threat Hunting program over the next 12 months?



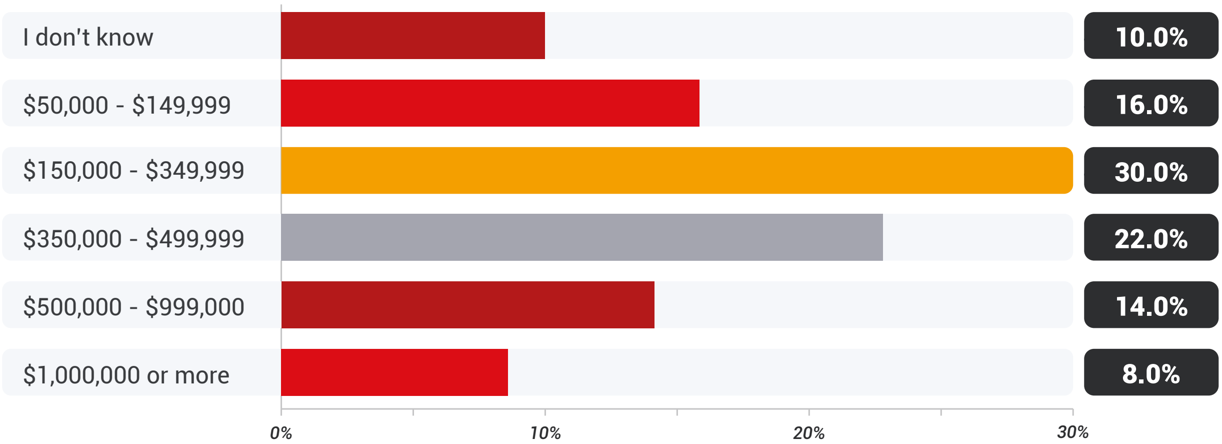
● Add more threat hunters or contract for external support	17.0%
● Increase host/network visibility	17.0%
● Establish baseline activity for hosts and networks	14.0%
● Increase storage and retention of logs for use by threat hunters	14.0%
● Investment in new tooling to perform threat hunting with	14.0%
● Expand third party monitoring for signals of compromise	11.0%
● Reduce the mean time to detect and remediate threats	9.0%
● Training new hires	5.0%

Nearly half have budgets of $350,000 or more for threat hunting.

What is their annual budget specific to threat hunting, including labor, tools, and any contracts? 44% have an annual budget of $350,000 or more, while 46% have an annual budget of $349,999 or less. (10% didn't know their budget.)

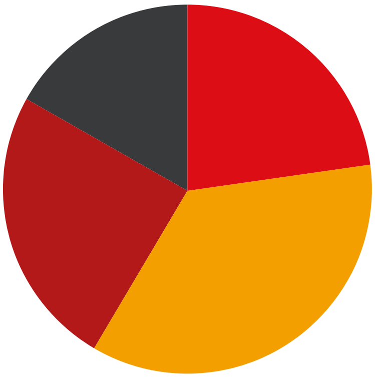
Broken down, 16% have a budget between $50,000 and $149,999, 30% have a budget between $150,000 and $349,999, 22% have a budget between $350,000 and $499,999, 14% have a budget between $500,000 and $999,000, and 8% have a budget of $1,000,000 or more.

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



38% believe their annual budget for threat hunting will increase over the next 12 months.

While 23% didn't know how their budget would change, 38% are expecting that their budget for threat hunting will increase over the next year. 22%, however, expect it to decrease. 17% say they don't anticipate any change.



How is your budget for Threat Hunting going to change over the next 12 months?

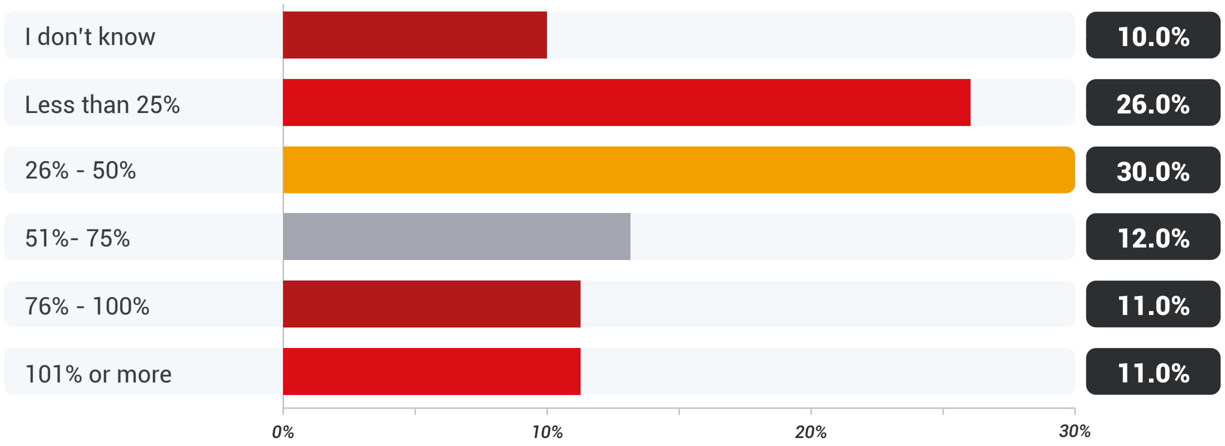
● I don't know	23.0%
● Increase	38.0%
● Decrease	22.0%
● No change	17.0%

Some respondents predict their budget for threat hunting will increase by 26% to 50%.

How much will budgets increase? The largest segment (30%) anticipates it changing by 26% to 50%, while the second largest segment (26%) sees it only changing by 25% or less. These numbers suggest that projected budgets may not keep up with the demand for additional threat hunting resources.

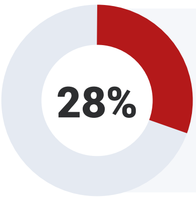
Additionally, 12% of respondents see it changing by 51% to 75%, 11% see it change by 76% to 100%, and 11% see it changing by 101% or more.

By what percentage will it change?

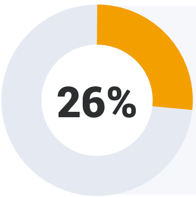


Enterprise host forensic capabilities are what respondents find most valuable.

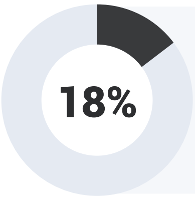
What threat hunting products are most interesting and would be the most valuable to our respondents? Here's what they said.



Enterprise host forensic capability
They're most interested in products that can help with host forensic, helping them better investigate threats in their system.



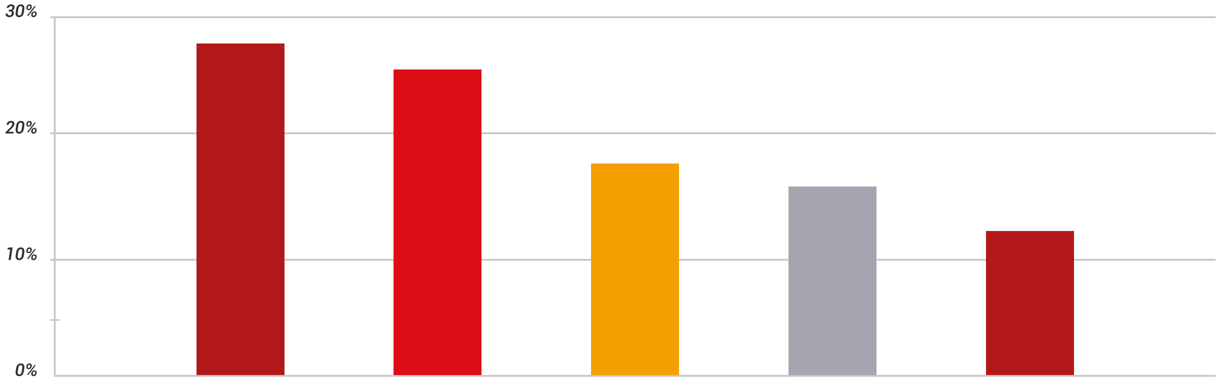
Network forensic detection, netflow telemetry, raw network telemetry data and/or full packet captures
Mirroring their wish list from above for better data sources, they also want products that can record and provide the data they need to better visualize their environments and analyze attacks.



Detection and response capabilities like EDR, NDR, XDR, etc.
They're also interested in products that can help them better understand and mitigate the threats to their environment.

They're also interested in commercial threat intelligence feeds (16%) and SIEM/SOAR platforms (12%).

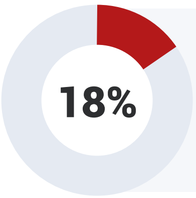
What threat hunting products are most interesting to you/most valuable?



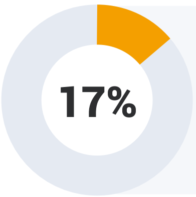
●	Enterprise host forensic capability	28.0%
●	Network forensic detection, netflow telemetry, raw network telemetry data and/or full packet captures	26.0%
●	Detection and Response Capabilities (EDR, NDR, XDR, etc)	18.0%
●	Commercial threat intelligence feeds	16.0%
●	SIEM/SOAR	12.0%

Respondents are most worried about the inability to measure their threat hunting program's success accurately.

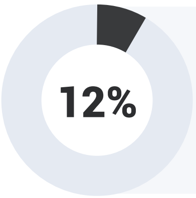
Finally, when asked about the pitfalls they worry about most with their threat hunting activities, respondents said they're concerned about the following.



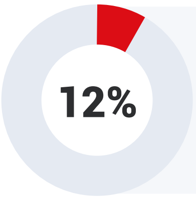
Inability to truly measure the successfulness of the threat hunting program
They're most worried that they won't be able to truly measure their success, meaning they doubt they have full visibility into the impact their efforts are making and are missing blindspots.



Finding more incidents than they have the capacity to respond to
Another worry is that their team will be easily overwhelmed by incidents, and won't have the ability to catch up.



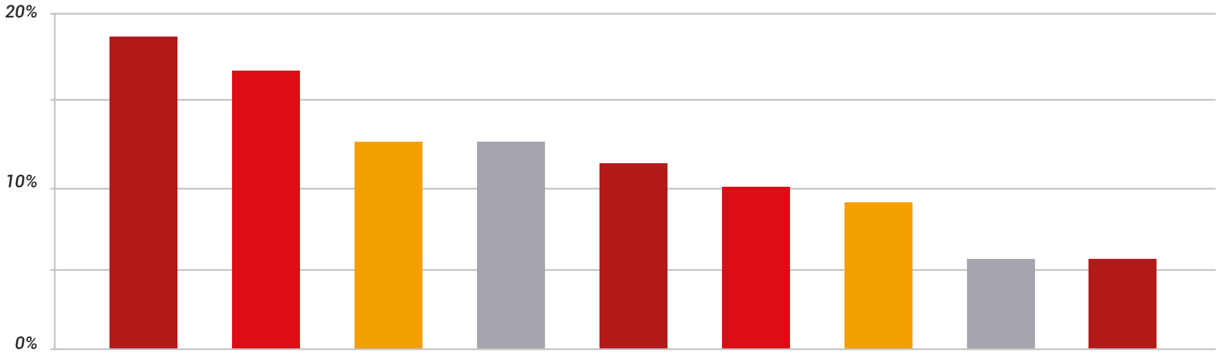
Failure to keep up with the current trends and threat intelligence
They're also concerned that they'll fall behind in being aware of the latest security threats, leaving themselves vulnerable through a lack of knowledge.



Tool effectiveness
As we've seen above, they worry they don't have adequate tools to help them protect their organization.

They're also concerned that senior management lacks the understanding of the value of threat hunting (11%), cognitive bias and fatigue of threat hunters (10%), failing to retain qualified personnel (9%), attribution (6%), and ease of use for tools and processes (6%).

What pitfalls do you worry about most with your Threat Hunting activities?



●	Inability to truly measure the successfulness of the threat hunting program	18.0%
●	Finding more incidents than you have the capacity to respond to	17.0%
●	Failure to keep up with the current trends and threat intelligence	12.0%
●	Tool effectiveness	12.0%
●	Senior management lacks understanding of value	11.0%
●	Cognitive bias and fatigue of threat hunters	10.0%
●	Failing to retain qualified personnel	9.0%
●	Attribution	6.0%
●	Ease of use (tools, process)	6.0%

Summary

In this section, respondents gave us more insight into their priorities, trends, budgets, and worries, and we're starting to get a better picture of their desire for more talent and better tools in order to improve their threat detection.

When it comes to budgets, it's encouraging to see 38% anticipate that their budget for threat detection will increase in the coming year. This increase in budget could be a result of organizations wanting to enhance their overall security posture, increase their ability to detect and respond to threats, and stay ahead of the ever-evolving cyber threat landscape. But not all budgets are going up, and 22% expect it to decrease over the coming year. One reason for this could be tied to the third most selected challenge from above and one of their worries here: no executive-level support, or a lack of understanding the value of threat hunting from senior management.

Security teams are also concerned about being able to measure success. While there may be indicators that a program is successful, such as a decrease in alerts or incidents, it can be challenging to quantify the link between the program and these outcomes. Evaluating the success of a threat hunting program is important for determining whether their efforts are effectively reducing the risk of cyber attacks, identifying and mitigating threats, and improving the overall security posture of the organization. The inability to measure success can lead to difficulties in making informed decisions, allocating resources effectively, and justifying the value of the threat hunting program to stakeholders.

Finally, their top priorities for 2023 include adding more threat hunters to their team or contracting out for support, increasing host and network visibility, establishing better baselines, better log storage and retention, and investing in new tools.

PART#4

Actionable Takeaways For Threat Hunting Team Leaders

Threat hunting is a vital part of an organization’s security posture, involving knowledge of current threat trends, proactive monitoring of your environment, and having the data to make informed decisions before deploying countermeasures. Yet as our respondents told us above, security teams are looking for better tools, more data, and more training in order to effectively succeed at threat hunting.

Based on their responses, here are five action items that security leaders can implement to strengthen their threat hunting program.

1: Selecting better tools.

Budget increases — which 38% of respondents are expecting — can give security teams options when it comes to bringing new tools into their organization. When evaluating new threat hunting tools, consider aspects of the tool like its functionality and how it aligns with your team's needs, how well it will integrate with your existing systems, and how it will scale, both in terms of data volume and the number of users.

As you evaluate vendors, consider not just upfront costs, but total costs that include licensing, maintenance, and support. Consider the vendor's reputation as well, and what level of support they can give you going forward.

Finally, as you look to bring new tools into your organization, consider your maturity. Every team we encounter overestimates their maturity, leading to disappointment when it comes to using more advanced tools. It's important to find tools that align with your maturity, and that can grow with you and your team over time.

2: Sharing threat intelligence.

The more information and insights into threats, the better — one of the things security practitioners wanted more of, as stated above. When collaborating and sharing threat intelligence internally, think about what information will be most relevant, actionable, and timely for other teams.

Don't just consider what you're sharing, but how you're sharing it, too. Abide by your organization's confidentiality and privacy protocols around intelligence sharing, as well as any relevant laws and regulations. Make sure it's in the format and medium that's most appropriate, and that it's classified based on its level of sensitivity.

As you share intelligence, build relationships with the teams you're sharing with as well, and solicit feedback about your intelligence sharing initiatives. This will help to encourage open and effective communication and to promote mutual understanding and trust.

3. Becoming a more effective team.

More data. Better tools. More training. These are just some of the things that respondents said could help them be more proactive in their threat hunting and make a bigger impact. Start by investing in employee development to help close the skills gap and to attract and retain top talent. This can include training programs, certification courses, and professional development opportunities.

If you're unable to train internally or attract experienced threat hunters, look outside your organization. Teams should consider partnering with third-party providers who specialize in threat hunting services to help supplement their in-house capabilities and to access additional expertise and resources as needed.

Additionally, leverage automation and artificial intelligence (AI) to help augment the skills and capabilities of your threat hunting program, reducing the reliance on manual processes and freeing up time for more strategic activities.

Finally, use metrics to evaluate the success of your threat hunting program, including the number of threats detected, the time to detect and respond to threats, and the impact of threat hunting activities on the overall security posture of the organization. By measuring success, teams can identify areas for improvement and make changes to their threat hunting program as needed.

4: Monitor third-party risks.

Proactively protecting your organization also means becoming experts at monitoring third parties for signals of threats and strong evidence of risks by taking action. First, develop and implement policies and procedures to assess and manage the risks posed by third-party relationships, including the regular monitoring of third-party activities and data. Then, conduct regular threat assessments and implement continuous monitoring for real-time visibility into third-party activities and data.

Additionally, foster collaboration with third-party partners and service providers to promote open and effective communication and to facilitate the sharing of information and intelligence related to potential threats. Regularly update policies and procedures to reflect changes in the threat landscape and to ensure that your third-party monitoring program remains effective and relevant.

5: Better data for better protection.

Having your hands on the right data will make or break your threat hunting activities. Start by evaluating your current infrastructure and identifying gaps in your data sources. Then assess the data collection needs of your threat hunting program, including the types and volumes of data required, and the sources from which this data will be collected.

Once you know what you need, invest in the right data collection tools and technologies that can help give you more visibility and insights into your organization's environments. As you increase your data collection, be sure that data is integrated into your SOC, and that you create retention policies around it, like how long to store your data.

Finally, regularly monitor and evaluate the data collection process to identify and address any issues or challenges, and to ensure that the data collected is accurate and relevant to the threat hunting program.

CONCLUSION

With today's rising cyber attacks, keeping a proactive stance against threats is key — but teams will only be as successful in protecting their data and assets if they have robust tools to help, the data and visibility into their environments, and experienced analysts to track and stop malicious activity.

Need Any Assistance?

We are here to help. Get in touch to discuss or learn more – we'll be happy to explain.

LET'S CONNECT

TEAM CYMRU™
THE POWER OF PURE SIGNAL™