February 2023

# Wanted: A Few Good Threat Hunters

CRA | Business Intelligence
A CyberRisk Alliance Resource

ExtraHop

# Contents






ALSO IN THIS REPORT

FOREWORD

# A race against time

**At a glance, the threat hunting landscape in 2023 seems awash in contradictions.**

Human ingenuity and insight are essential to steering threat hunting investigations, yet technologies like advanced analytics and automation are integral to conducting these searches. When done right, threat hunting is proactive, methodical and unhurried, yet many security professionals see the activity as a "race against time" to process and act on every possible threat alert. Increasingly, organizations believe threat hunting is important in improving overall security posture, but do not have (or do not provide) sufficient funding to acquire the kind of skilled expertise, training, or improved tools that could make a significant difference. Meanwhile, organizations are hungry to add experienced threat hunters to their ranks but struggle to find such talent in an intensely competitive and specialized field.

Then there's the threats themselves, which are evolving to evade SIEMs and other defense tools that, in years past, would have been enough protection. As one respondent said, "we're growing, but we're not growing at the same rate as the bad guys." And despite growing recognition and interest in the value of threat hunting, security leaders we surveyed said there is still very low awareness of what processes, tools and policies are needed to maximize threat hunting potential.

Will it always be a "race against time", or can organizations find ways to defy the odds and integrate threat hunting capability in their ranks?

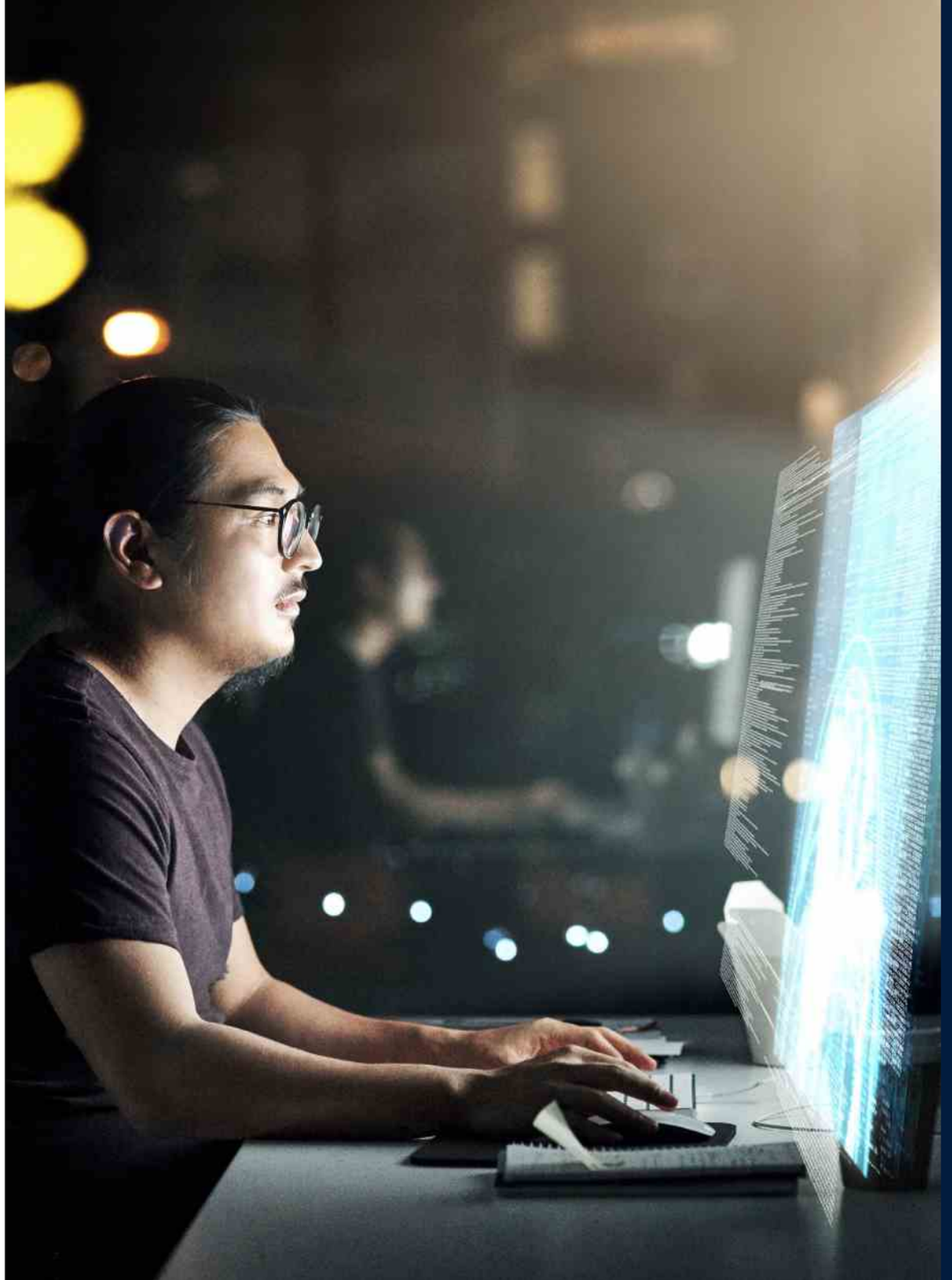
## Threat Hunting 101

**Threat hunting is proactive, not reactive.** Hunters construct hypotheses to test possible conditions under which an adversary might infiltrate the network. These hypotheses can either be lead-driven (i.e., prompted by abnormal network activity) or leadless (i.e., prompted by hypothetical intrusion scenarios).

**Threat hunting assumes the worst has happened.** Threat hunters carry out their hunts under the assumption that adversaries have already evaded existing defenses. Therefore, a hunt begins with the hypothesis that an attack was successful, then searches for evidence of conditions that would permit said hypothesis to come true.

**Threat hunting is a human-led activity but can benefit from appropriate technologies.** Organizations require trained human specialists to lead threat hunts. Hunters apply critical thinking, scripting knowledge, and manual search methods to identify threats that evade standard detection technologies. Emerging technologies like AI and machine learning can help hunters sift through massive volumes of data and make more informed search queries based on existing threat data.

Source: **https://www.scmagazine.com/resource/ransomware/threat-hunting-101**



"Detecting advanced threats through threat hunting can become incredibly complex. Simple attacks would be easier to uncover, but advanced attacks are extremely hard to detect as they occur over a longer period of time and are incredibly calculated and meticulous."

– SURVEY RESPONDENT

# Four key findings from the survey:

## 1.

### Still a pie in the sky...

An evolution in adversary attack patterns has cast a spotlight on the urgent need for threat hunters, highly trained individuals that can proactively investigate and eliminate cyber threats before they materialize.

However, while more organizations have announced intentions to introduce hunting capabilities in the next year, threat hunting overall remains out of reach to most businesses due to high costs of entry or limited understanding into what value it would bring.

## 2.

### Desperately seeking threat hunters

Organizations recognize the need for threat hunters and what they can bring to the table. The difficulty is finding the hunters themselves, a highly specialized subset of the infosec profession.

Respondents point to the difficulty in recruiting and retaining individuals who have such diverse skills and depth of expertise — a rare blend of technical knowledge, forensic talents and intellectual curiosity honed through years of experience battling adversaries on the cyber frontline. In addition to dealing with such a limited pool of candidates, respondents say threat hunters carry a price tag that many organizations simply lack the budget for.

## 3.

### Moving beyond reactive intelligence

The impression we get from respondents is that their organizations are straddling an iceberg of threat intelligence, but only a small portion is visible above the surface.

While rapid detection and response can fall under the threat hunter's portfolio, effective hunting should prioritize proactive investigations over reactive response.

Yet, within organizations that practice threat hunting, we find that response-oriented tools (such as SIEMs, EDRs, and IDS) are the most frequently used to support threat hunting activities. This results in addressing what is already found, versus discovering what could be critical vulnerabilities flying under the radar.

## 4.

### Threat hunters reap new rewards

Dedicated threat hunting programs that began in the last few years are already seeing a return in value.

We find that organizations that implemented threat hunting have observed improvements when it came to faster speed and accuracy in threat response, reduced attack surfaces and encounters with bad actors, as well as greater precision in discovering and detecting threats.

THREAT HUNTING ADOPTION

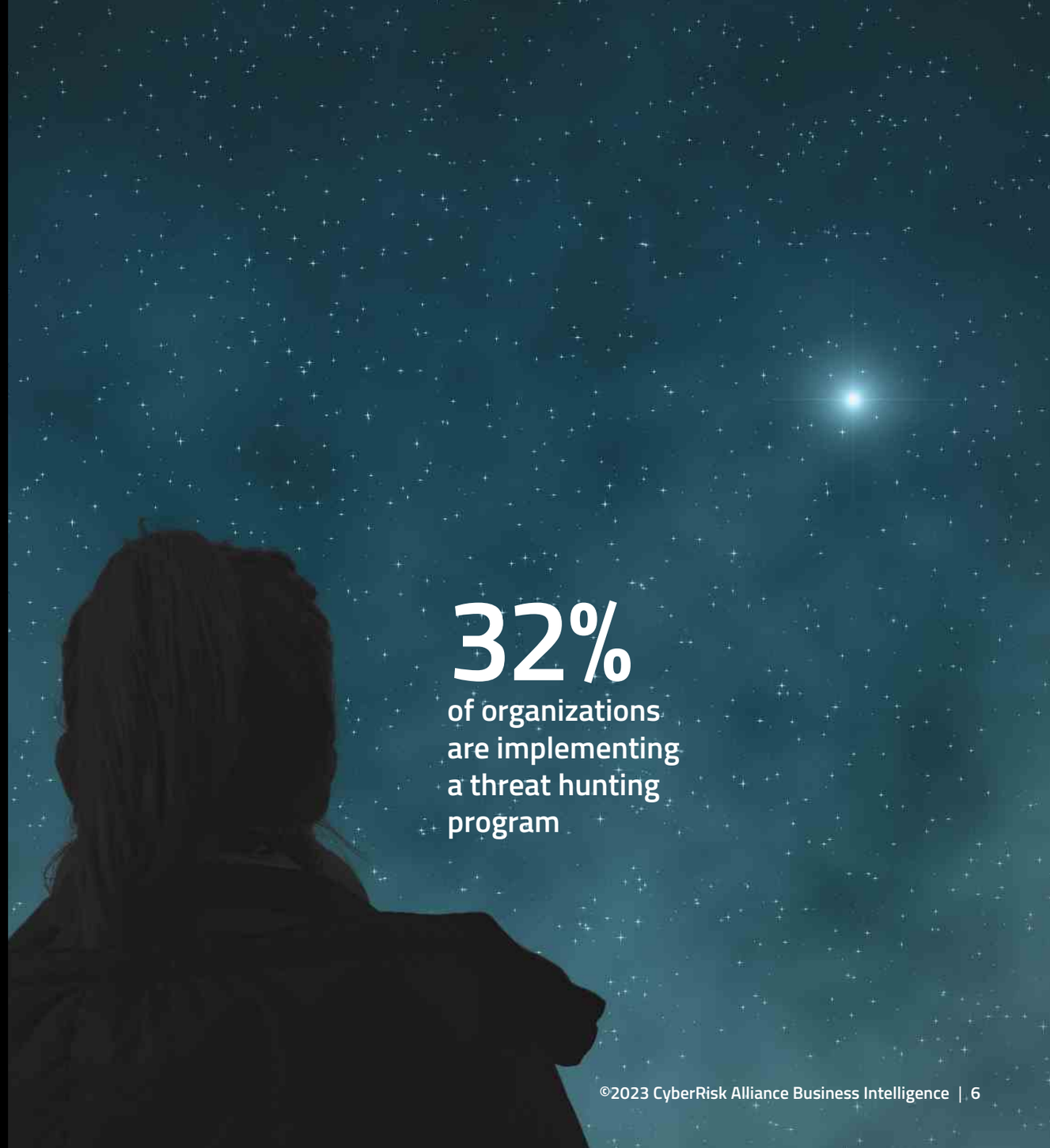
# 1 Still a pie in the sky…

For all the industry buzz and hype it's generated in the last 2 years, threat hunting in the SOC remains the exception rather than the norm. Why?

Well, there's still a high barrier to adoption and heavy cost in resources associated with threat hunting. You need time, money, and people — freakishly skilled people who know how to hunt. For this reason, threat hunting is more likely to be a staple in enterprise organizations that already employ higher numbers of IT security personnel.

It may be tempting for IT teams with minimal funding and personnel to see threat hunting as a pie in the sky project for the foreseeable future, about as realistic as summiting K2 without oxygen support.

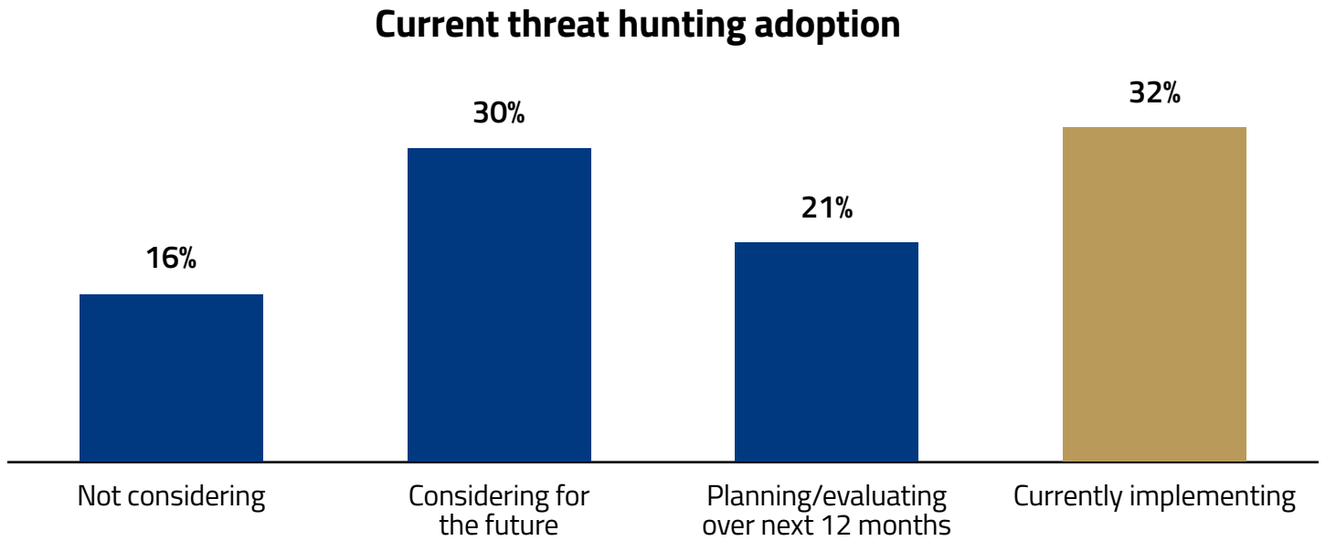
But hold your cyber horses. There's a sign that change may be on the way, as more organizations plan to adopt threat hunting capabilities this next year. In addition, more security pros testify that threat hunting would be a key ingredient to improving overall security posture — an enticing consideration for C-suite leaders sweating about the next data breach and PR crisis that might unfold.



**32%**

**of organizations are implementing a threat hunting program**

**Threat hunting is still not a reality for most organizations.** Although some may have it in their sights, it remains to be seen whether they can get this type of a program off the ground given the numerous obstacles they face.




## What is your organization's current status in implementing a threat hunting program?

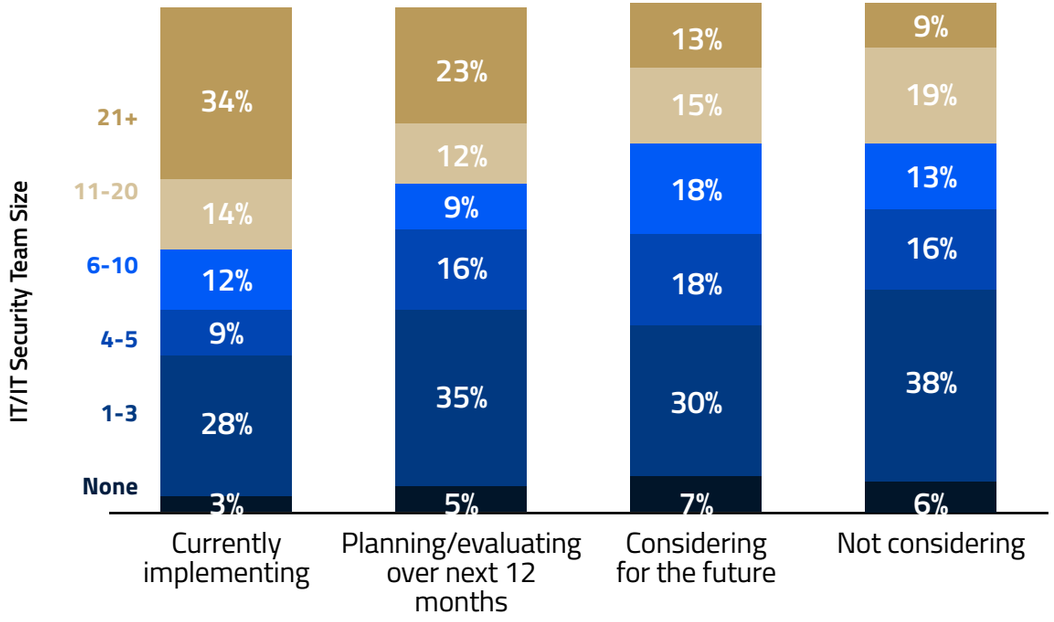
Less than one in three respondents said they are currently implementing a threat hunting program today; however, about half (51%) indicated they will be planning for it or evaluating it in the next 12 months or considering it for the future.

Inevitably, organizations expect to face numerous obstacles in launching and implementing an effective threat hunting program.

Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: All respondents; "Don't know" excluded (n=201).

# **An effective threat hunting program requires resources.**
Organizations with large IT/IT security teams are more likely to be conducting threat hunting or planning for it in the coming year.

## Current threat hunting adoption, by IT security team size




Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: All respondents; "Don't know" excluded (n=201).

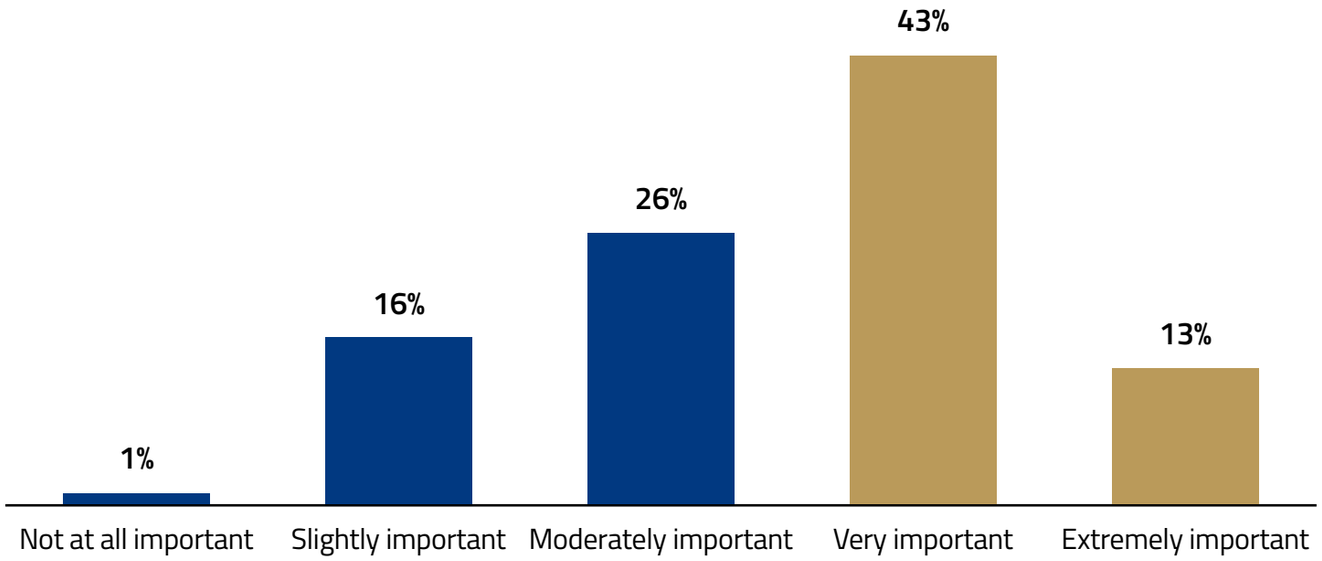
## What is your organization's current status in implementing a threat hunting program?

Nearly half (48%) of organizations implementing threat hunting programs have large IT/IT security teams (11 or more team members).

Additionally, organizations with large IT teams are more likely to be planning or evaluating a threat hunting program (35%).

**Security pros mostly believe threat hunting is important in improving their organizations' security posture.** As a more proactive approach to advanced threat detection and response, threat hunting is gaining popularity.

## Importance of threat hunting in improving security posture




### How important do you think threat hunting is/would be in improving the overall security posture of your organization?

More than half (56%) of respondents believe threat hunting is very/extremely important in improving the overall security posture of their organization.

Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: All respondents (n=212).

For all the vigilance and peace of mind that threat hunting can provide, there's no denying it carries a steep cost of entry — in more ways than one. According to the security professionals we surveyed, five challenges stood out from the rest:

### 1. Time is always in short supply.

There's never enough time, respondents voiced again and again. Some cited the time it takes to train analysts in threat hunting skills. Others pointed out not having enough time to conduct manual threat hunts in the first place. A few bemoaned the time it takes to deploy new technologies, while others singled out the length of time needed just to replace skilled personnel. Wherever you look in the SOC, it seems that time is in universally short supply.

### 2. Skills and staffing fall short of the requirements.

There's no sugarcoating it; threat hunting is a human-led endeavor. While technologies like automation can enhance threat hunts, it can't be the driver. Across all organizations and sectors we surveyed, participants repeatedly expressed dismay at insufficient staffing and skill sets they had to carry out threat hunts. "No one on my team has any experience, so it's learning as we go and trial-by-fire," said one respondent. "Threat hunting is hard to hire for and difficult to train and teach," voiced another.

### 3. It's an uphill battle to get leadership support.

Respondents would like to see greater support for threat hunting from their leadership. Part of the difficulty is justifying threat hunting from a business perspective. "[My] management won't be interested in paying for such a service until a major client mandates that we have it," said one respondent. Another individual anticipated difficulties in convincing leadership of threat hunting's value in cases where hunts revealed nothing notable: "Things aren't always happening, but that doesn't mean threat hunting isn't working."

### 4. It's just not in the budget this year.

*Money / it's a crime / share it fairly, but don't take a slice of my pie*, sings Roger Waters on Pink Floyd's 1973 hit track "Money". Respondents think it's a crime too, as many express dissatisfaction with how their organization has failed to budget for threat hunting. Whether it's building up hunting operations from within or getting outside help from a provider, there was general agreement that the cost was prohibitively high. "We would like to have more internal staff, but it's just not in the budget this year," shared one individual. "The overall cost for third party managed threat hunting programs can be unrealistic for small to medium businesses," voiced another.

### 5. Threat hunting is rife with technology challenges.

Even though humans – not machines – are responsible for engineering threat hunts, emerging technologies like AI and machine learning can greatly enhance the insights their hunts yield. But respondents say such tools are few and far between. "We need more behavior data that is not collected by our SIEM," said one. Another said their organization was struggling to establish a comprehensive hunt program due to "limits on endpoint and encrypted traffic visibility." Respondents also pointed to the difficulty of conducting hunts at scale: "We have a complex, global ecosystem and establishing the same controls at all of our international locations proves a challenge when it comes to data congruence and capability in disparate networks."

> "No one on my team has any experience, so it's learning as we go and trial-by-fire. There isn't a big enough buy-in from executive management to get additional training or hiring an experienced threat hunter."
>
> – SURVEY RESPONDENT

ORGANIZATIONAL REQUIREMENTS

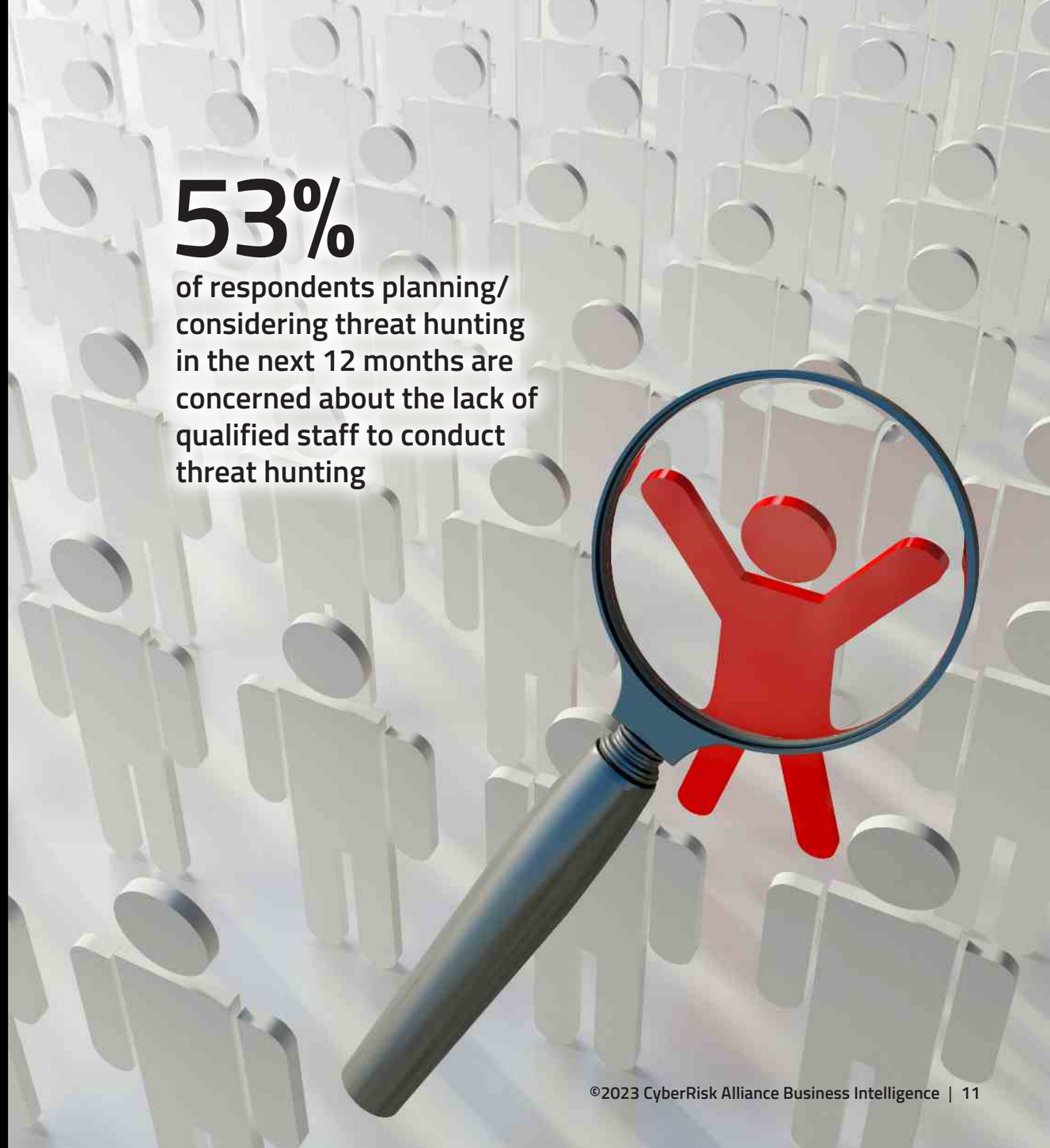
# 2 Desperately seeking threat hunters

There's a well-documented shortage of information security professionals in the job market today. Among this limited pool, threat hunters are the rarest kind.

That's because threat hunters bring years of experience and interdisciplinary skills to their craft. A hunter is expected to be competent in a range of subjects, as fluent in data forensics and analytics as they are in being able to translate technical findings into non-technical recommendations for business leadership.

Funding is a major impediment to launching threat hunting programs, which has a cascade effect on organizations' ability to budget for skilled personnel and training.

"Hiring and retaining qualified threat hunting analysts will be a challenge at least for the foreseeable future," voiced one respondent, a sentiment shared by many of their colleagues.

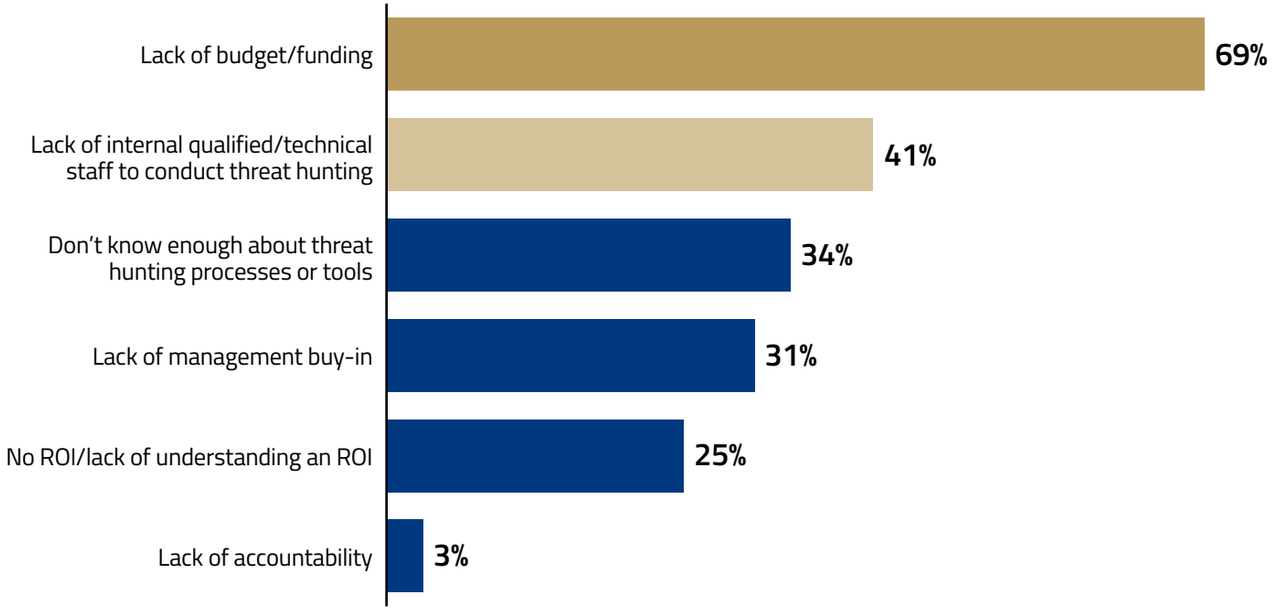


**53%**

**of respondents planning/ considering threat hunting in the next 12 months are concerned about the lack of qualified staff to conduct threat hunting**

**The barriers for adopting a threat hunting program are mainly about limited resources.** Respondents whose organizations are not considering threat hunting say their limited budgets and lack of qualified threat hunting staff are keeping them from adopting it.

## Top barriers in adopting threat hunting



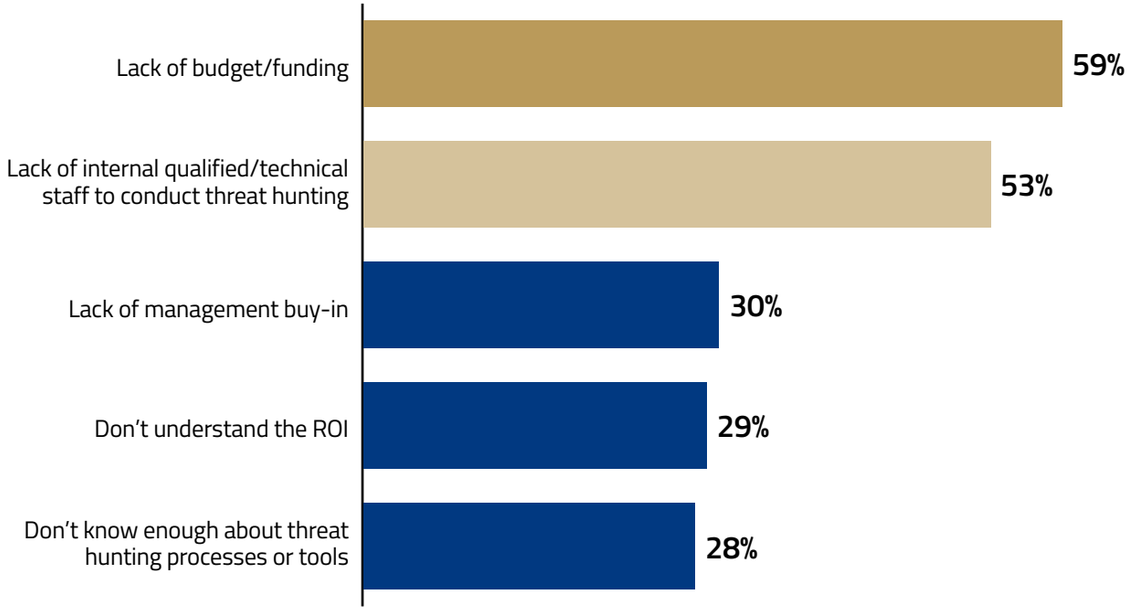

Note: Respondents were asked to select all that apply.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: Respondents not considering threat hunting (n=32).

### Which of the following best describes the reasons why your organization is not considering a threat hunting program?

Respondents not considering a threat hunting program are mostly hampered by a lack of budget and qualified technical staff.

# **Future adopters of threat hunting have similar concerns.** Their top issues are the same as those for non-adopters: lack of funding and an internal qualified staff to conduct threat hunting.

## Concerns about threat hunting among future adopters




Note: Respondents were asked to select all that apply.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: Respondents considering or planning/evaluating threat hunting (n=104).

### Which of the following best describe your organization's issues or concerns in considering, planning, or evaluating a threat hunting program?

Similar to the group of respondents whose organizations are not considering a future threat hunting program, those considering or planning for threat hunting are mainly concerned about a lack of budget or funding and the qualified technical staff required to conduct threat hunting.

TECH CHALLENGES

# 3 Moving beyond reactive intelligence

Even among organizations that have threat hunting programs, the most common technologies tend to be reactive and response-oriented rather than proactive in nature.

SIEMs and EDR solutions are commonplace, attested to by at least 7 out of every 10 respondents. These tools are useful for detecting and rapidly responding to anomalous behavior on the network but are not a threat hunter's main weapons when conducting a search.

Conversely, less than half of respondents use dark web monitoring or manual search to gather hunt intelligence. Roughly two-thirds say their hunting does not allow for collection of a high number of data types, and nearly as many (61%) indicate that data analytics and machine learning are not yet being used to refine and automate hunting methods.

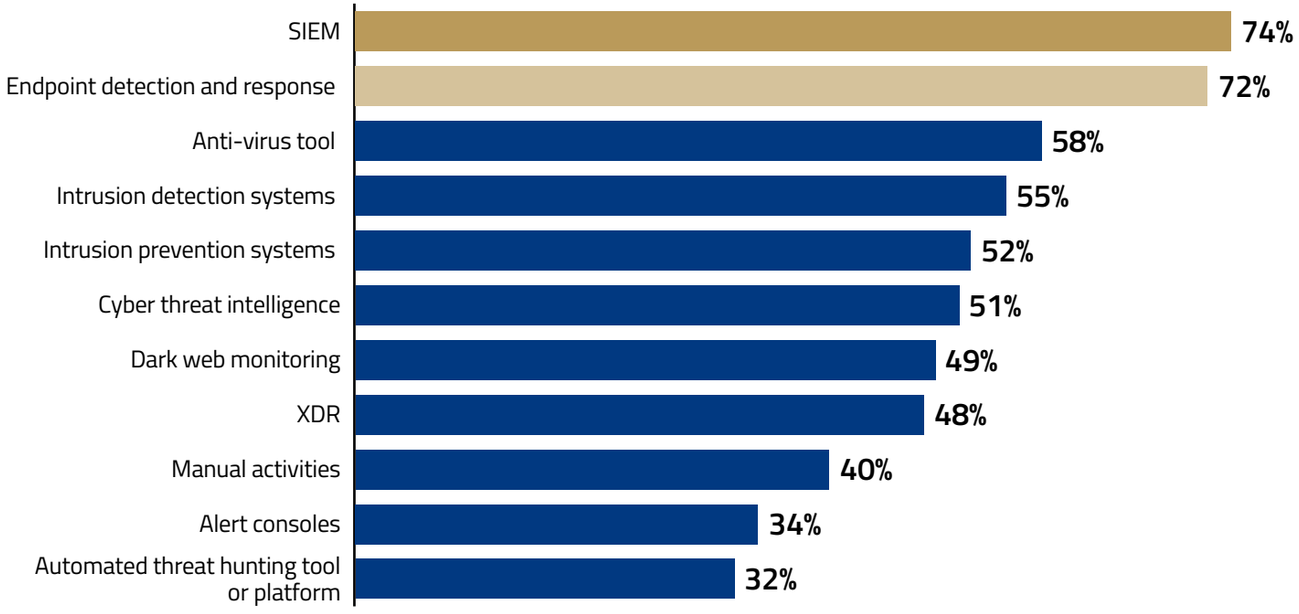
What this results in is a culture of "catch-up", where the SOC is in constant response mode instead of being empowered to build threat hypotheses and make new discoveries.

**35%**

**of respondents said they implement a high level of data collection (with many data types) to drive their threat hunting programs**

**SIEM and EDR are the most common tools used in threat hunting.** However, they are not a threat hunter's only weapons: threat intelligence, dark web monitoring, and manual activities should be a primary focus for threat hunting initiatives.

## Threat hunting methods

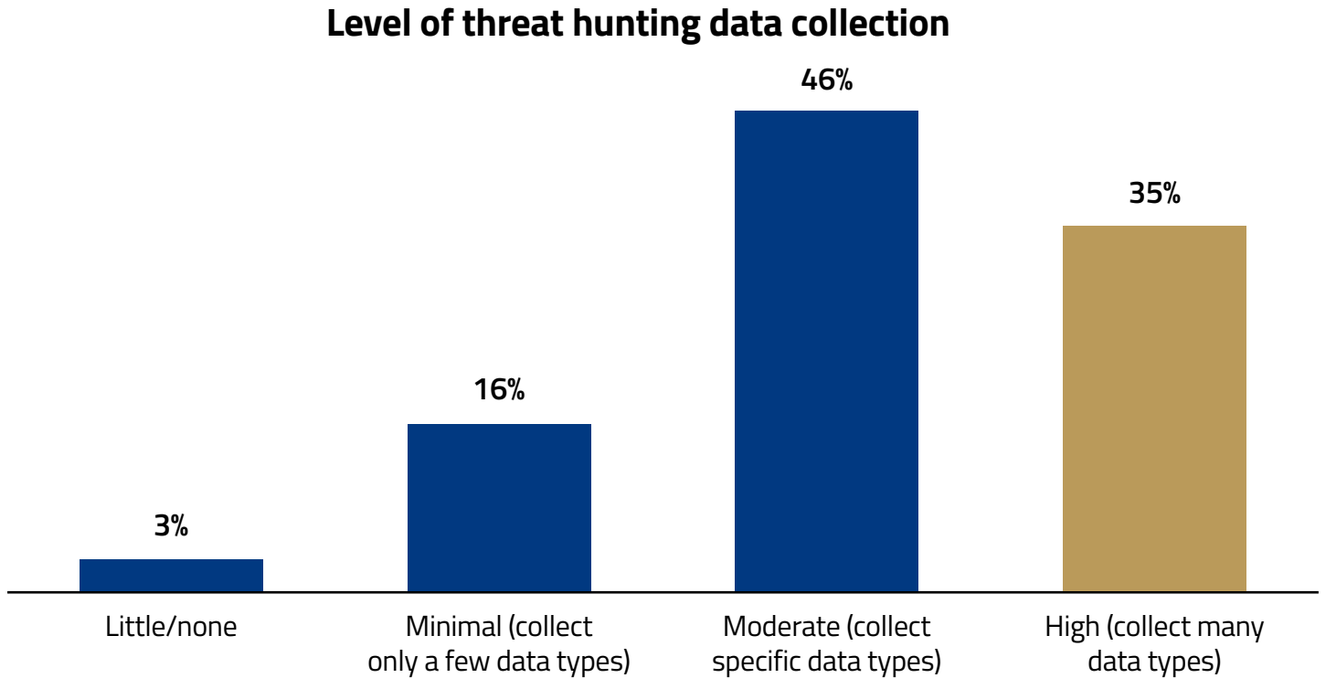



Note: Respondents were asked to select all that apply.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: Respondents implementing a threat hunting program (n=65).

### What methods or tools are used in your threat hunting program?

Roughly 3 out of 4 respondents use SIEM and/or endpoint detection and response tools (EDR) in their threat hunting programs while cyber threat intelligence is only used by about half of these organizations.

**One in three respondents say they collect many data types for their threat hunting program.** This data is key for the proactive detection of irregularities that may suggest potential threats.

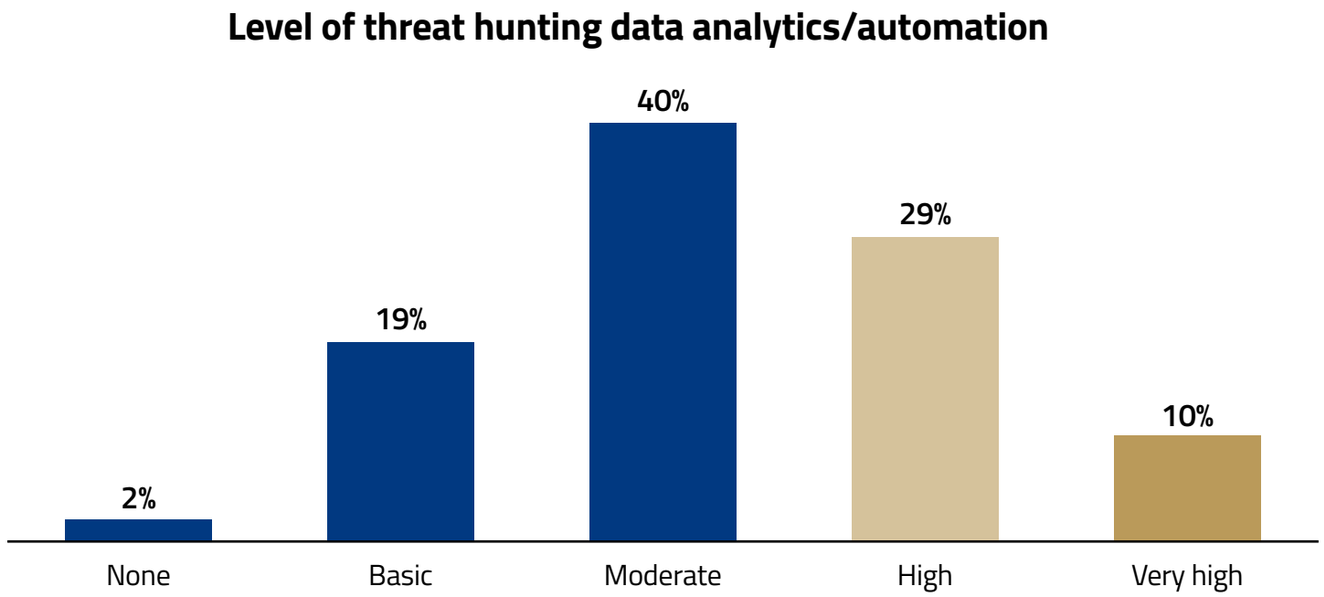



Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: Respondents implementing a threat hunting program; "Don't know" responses excluded (n=63).

## Which of the following describes the level of data collection for your organization's threat hunting program?

About 8 in 10 respondents collect at least a moderate level of data that provide the analytics that power their threat hunting programs. Data collected for threat hunting can include endpoint data, network data, and various types of security data (e.g., alerts, threat intelligence, etc.).

**Most threat hunting organizations lack automation and machine learning capabilities.** This technology gap indicates most organizations have not reached fully mature threat hunting programs.




## Which of the following describes the level of data analytics/automation for your organization's threat hunting program?

Only 10% have automated/machine learning capabilities driving their threat hunting programs

Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: Respondents implementing a threat hunting program; "Don't know" responses excluded (n=62).
Note: Levels of data analytics are as follows: 1) Basic (integrated with automated alerts); 2) Moderate (built a library of hunting procedures for regular use); 3) High (built a library of hunting procedures for frequent use; provide basic data analytics); 4) Very high (automated with continuous improvements to alerts; machine learning capabilities).

# 4

**ORGANIZATIONS ON TRACK**

# Threat hunters reap new rewards

Hunts may reveal proof of a vulnerability, or they may reveal network activity that is completely unrelated to the target of the investigation. Regardless of what is found, hunting exercises expand the organization's security awareness and visibility of the network.

And this visibility — the capacity to identify threats and get out ahead of them — is a top driver for threat hunting investments. Improved detection capability also reduces the attack surface for adversaries to target.

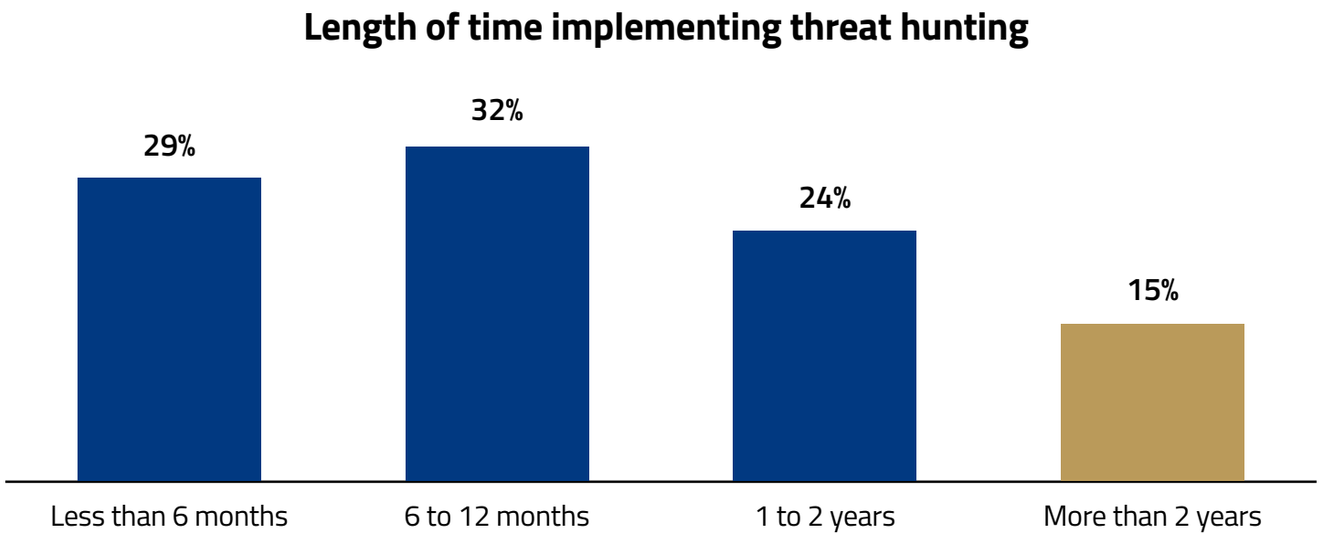
Even though threat hunting operations are still fairly new — most having their origin in the last 2 years — those that have launched programs say their work is already paying off.

Among areas of improvement, respondents note the biggest gains since instituting threat hunt programs have been in speed and accuracy of threat response.

**72%**

**have achieved at least a 50% improvement in the speed and/or accuracy of threat response from their threat hunting programs**

**Threat hunting is a relatively new approach for most organizations.** The vast majority have been implementing threat hunting for less than two years.




## How long have you been implementing threat hunting?

A large majority of respondents (85%) have been implementing threat hunting for less than two years.

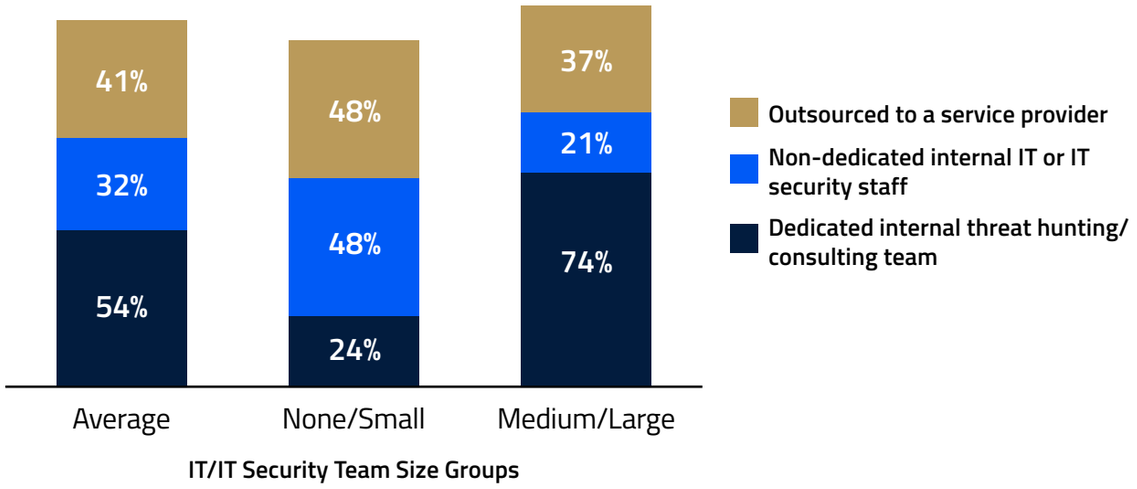
"The new threat hunting has allowed us to have better visibility and better reporting on where an incident is taking place, allowing us to more quickly shut down a threat actor."

– SURVEY RESPONDENT

Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: Respondents implementing a threat hunting program; "Don't know" responses excluded (n=62).

# **Threat hunting relies on dedicated technical support.**
Organizations with small or no IT/IT security staff are more likely to outsource threat hunting or have non-dedicated IT/IT security staff running these programs.

## Threat hunting capabilities, by IT team size groups



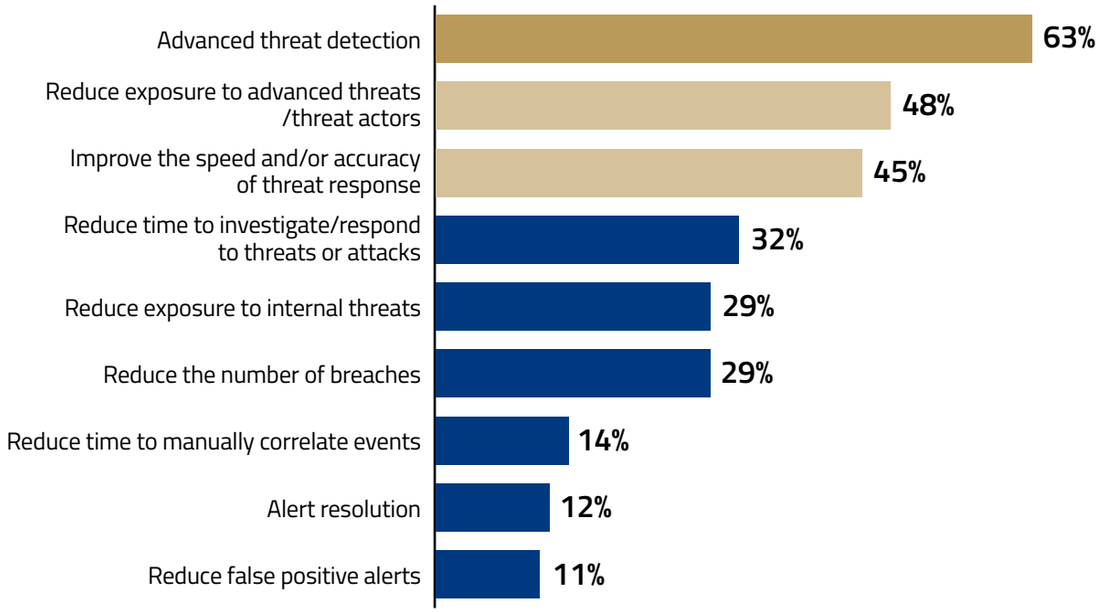

## How do you conduct threat hunting?

Nearly three in four respondents with medium/large IT/IT security teams have a dedicated internal threat hunting team. Organizations with smaller teams are more likely to use non-dedicated staff or outsource threat hunting to a third-party.

Note: Respondents were asked to select all that apply. Multiple responses allowed.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: Respondents implementing a threat hunting program; 'Don't know' responses excluded (n=63).
Notes: IT/IT Security Groupings: None/Small=5 or less team members; Medium/Large=6 or more team members.

**Threat hunting organizations are driven by advanced threat detection and response.** Key objectives for threat hunting organizations are detecting, reducing exposure to, and improving the speed and accuracy of threat response.

## Key objectives for implementing threat hunting




Note: Survey respondents were asked to select their top three objectives.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: Respondents implementing a threat hunting program (n=65).

### Which of the following best describe your organization's primary objective(s) for implementing a threat hunting program?

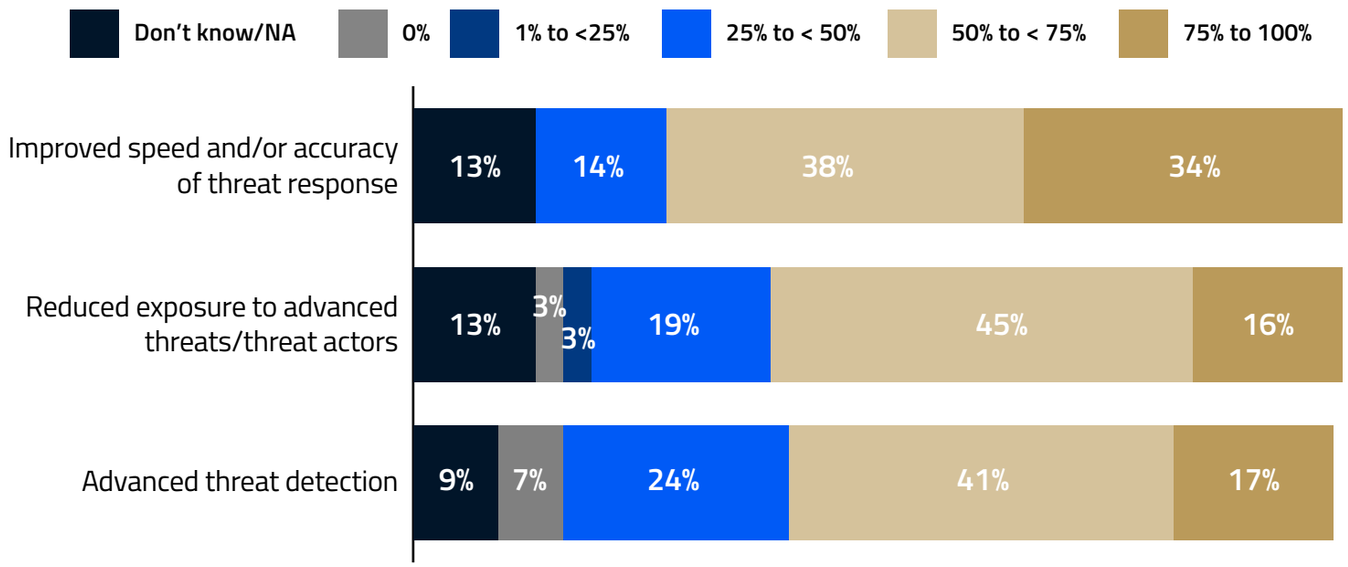
At the top of respondents' list of objectives for conducting threat hunting are advanced threat detection, reduced exposure to advanced threats, and improving the speed and accuracy of the threat responses.

"We are still in the early stages of implementing our threat hunting program but have already reaped significant rewards. We expect to continue to learn about best practices for threat hunting and to continuously improve our program over the coming months."

– SURVEY RESPONDENT

# **Organizations are seeing moderate to high levels of improvement in their main objectives as a result of their threat hunting programs.** The highest levels of improvement are seen in the speed and accuracy of threat response.

## Improvements in most common objectives




Source: CyberRisk Alliance Business Intelligence (CRA BI), Threat Hunting Survey, November 2022.
Base: Threat hunting organizations indicating their top three objectives are: advanced threat detection (n=41); improved speed/accuracy of threat response (n=29); reduced exposure to advanced threats/threat actors (n=31).

### For each of your top three objectives, what level of improvement have you achieved with each?

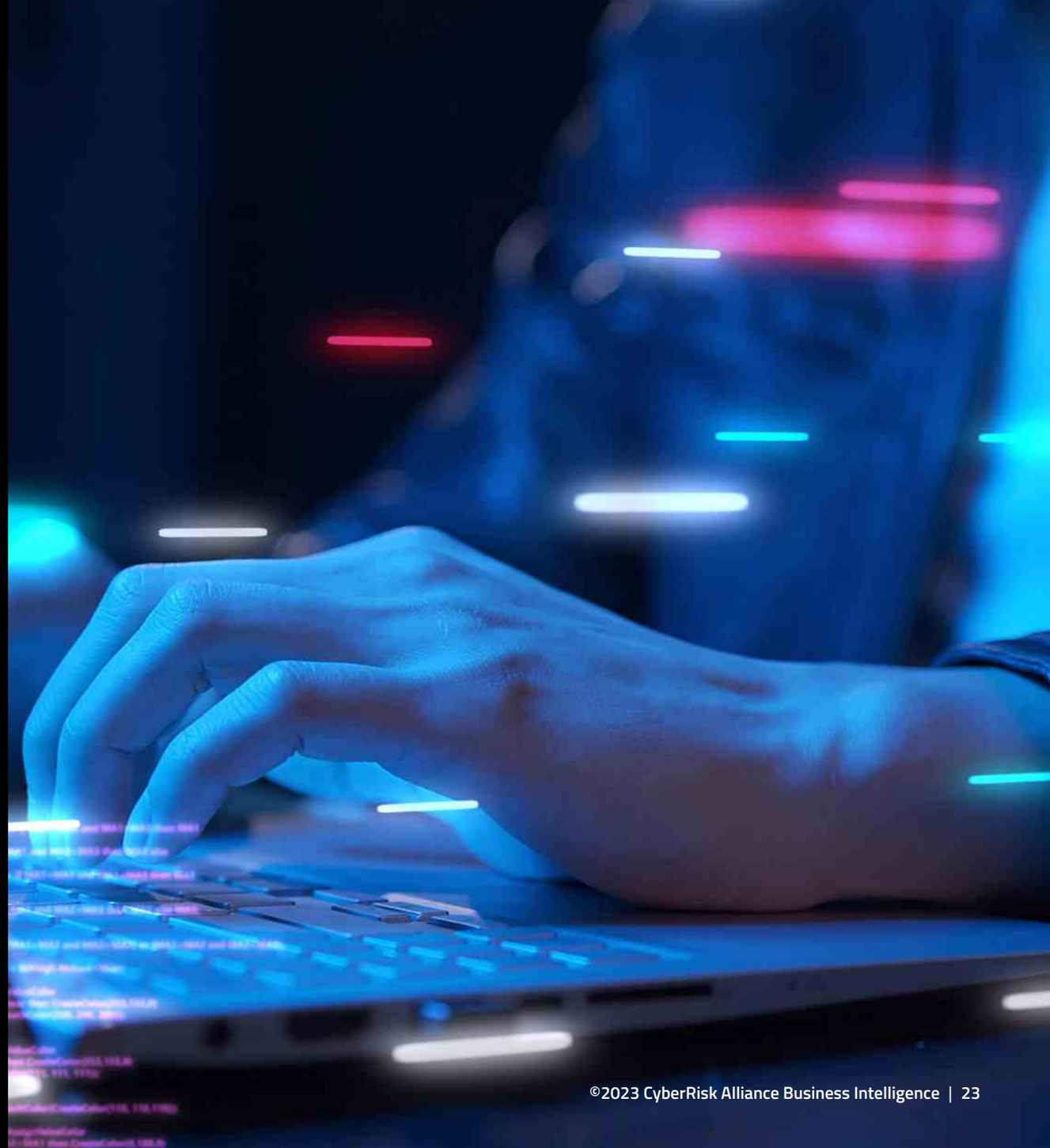
Nearly 3 in 4 respondents (72%) say they have achieved at least a 50% improvement in the speed and/or accuracy of threat response from their threat hunting programs.

MOVING FORWARD

# 5 Making threat hunting a reality

One of the most striking findings from the survey was the shared consensus by all respondents when it came to the top challenges to threat hunting. For organizations that already practice threat hunting, a lack of internal staff with the knowledge to conduct threat hunts were a major liability. And for organizations with no organized threat hunting operation, difficulty in finding skilled specialists was a major reason for why such efforts failed to gain ground in the first place.

At the same time, organizations need not assemble the greatest team of threat hunters alive to begin making a substantial difference. As the wise Mr. Miyagi says in The Karate Kid, "first learn stand, then learn fly." Before they can fly, there are a few basic measures organizations can take to move the threat hunting needle forward.



With funding and expertise in such short supply, here are a few steps organizations might consider as they put their threat hunting ambitions to the test.

**1. Measure existing threat hunt maturity.** Conducting an audit of one's security posture is a good first step to understanding if the organization is ready for threat hunting. Organizations can evaluate their readiness by using a cybersecurity maturity model and collecting insight from various frameworks and threat databases. The **MITRE ATT&CK** framework, **CIS Top 18**, and **NIST 800-171** are excellent resources

**2. Address the tech gap.** For threat hunters to be effective, they need full visibility of the network and the tools to search it. Organizations might consider using an **eXtended threat and response (XDR)** platform that natively integrates threat hunting tools into one package, along with providing a dashboard interface to explore threat signals and other vulnerable assets.

**3. Develop and implement an incident response plan.** As threat hunting operations grow, security managers must develop a **living incident response plan** that can accommodate any changes in protocols as it relates to detection, reporting, triage and analysis, containment, and post-incident cleanup.

**4. Decide on the right threat hunting approach.** Once organizations have a better reading on their threat hunting needs and goals, they can begin looking for an arrangement that's right for them. Part of that is deciding whether to cultivate threat hunters from within, outsource threat hunting to a third party, or set up a hybrid arrangement of in-house and out-of-house expertise.

**5. Address the skills gap.** Threat hunting is a chiefly human exercise, and organizations need to budget accordingly to attract skilled professionals. But if the budget to hire trained threat hunters just isn't there, consider carving out time in your current teams' workloads to integrate threat hunting exercises in small doses (like building and testing hypotheses). In addition, some MDR providers encourage their veteran threat hunters to share hunting disciplines and knowledge with their clients over time. Wherever they exist, seize moments that give your teams the breathing room and license to think creatively and critically about potential threats.

> "As attacks become more sophisticated, there should be a skilled person at the helm to maintain order and resolve issues."
>
> – SURVEY RESPONDENT

# Survey Methodology

The data and insights in this report are based on an online survey conducted in November 2022 among 212 security and IT leaders and executives, practitioners, administrators, and compliance professionals in the U.S. from CRA's Business Intelligence research panel.

The objective of this study was to explore organizations' experience with threat hunting, including their adoption and plans for future programs, tools and methods used, and the issues and challenges in implementing these programs.

**Notes:**

- Not all figures add up to 100%, as a result of rounding percentages
- The respondent base for charts is 212 (all respondents) unless otherwise noted in the chart. In some cases, 'don't know' responses have been excluded, which reduce the base size.

The respondent profile is as follows:

**IT or IT Security Roles/Titles:**

- CISOs/CROs/CIOs/CTOs (9%)
- VPs/SVPs/EVPs (8%)
- Directors (28%)
- Managers (31%)
- IT/security admins (17%)
- Analysts/consultants (8%)

**Organization sizes:**

- Small (1 to 99 employees) (8%)
- Medium (100 to 999 employees) (28%)
- Large (1,000 to 9,999) (36%)
- Enterprise (10,000 or more) (27%)

**Industries:**

- Education (14%)
- High-tech, IT software and telecom (14%)
- Financial services (11%)
- Manufacturing (10%)
- Healthcare (10%)
- Professional services (consulting, legal, etc.) (8%)
- Retail, trade, and eCommerce (8%)
- Government (6%)
- Other (media/communications/advertising, transportation/warehousing, non-profit, energy, utilities, construction, hospitality, and real estate) (19%)

# Other CRA Business Intelligence Reports

1. Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations (January 2023)
2. Threat Intelligence: Critical in the Fight Against Cyber Attacks, But Tough to Master (December 2022)
3. Ransomware Ready: Organizations Fight Back with More Aggressive Strategies and Technology (November 2022)
4. Harsh Realities of Cloud Security: Misconfigurations, Lack of Oversight and Little Visibility (October 2022)
5. Zero Trust Adoption Faces Ongoing Headwinds (October 2022)
6. Endpoint Security: Security Pros Concerned About the Proliferation of Non-Traditional Devices and Endpoints (September 2022)
7. Organizations Adopt Aggressive, More Proactive Vulnerability Management Strategies in 2022 (August 2022)
8. Threat Intelligence: The Lifeblood of Threat Prevention (July 2022)
9. CRA Study: Attackers on High Ground as Organizations Struggle with Email Security (July 2022)
10. Security Teams Struggle Amid Rapid Shift to Cloud-Based Operations (June 2022)
11. CRA Study: XDR Poised to Become a Force Multiplier for Threat Detection (May 2022)
12. CRA Study: Zero trust Interest Surges, But Adoption Lags as Organizations Struggle with Concepts (April 2022)
13. CRA Study: Managing Third-Party Risk in the Era of Zero Trust (March 2022)
14. CRA Ransomware Study: Invest Now or Pay Later (February 2022)
15. CRA Research: A Turbulent Outlook on Third-Party Risk (January 2022)

## CRA Business Intelligence Contacts

**Bill Brenner**
VP of Content Strategy and Research
bill.brenner@cyberriskalliance.com

**Dana Jackson**
VP of Research
dana.jackson@cyberriskalliance.com

**Daniel Thomas**
Custom Content Producer
daniel.thomas@cyberriskalliance.com

# About CyberRisk Alliance

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now, the Official Cyber Security Summit and TECHEXPO Top Secret. **Click here to learn more**.

# About ExtraHop

ExtraHop is on a mission to stop advanced threats. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to threats—before they compromise your business. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised. **Click here to learn more**.