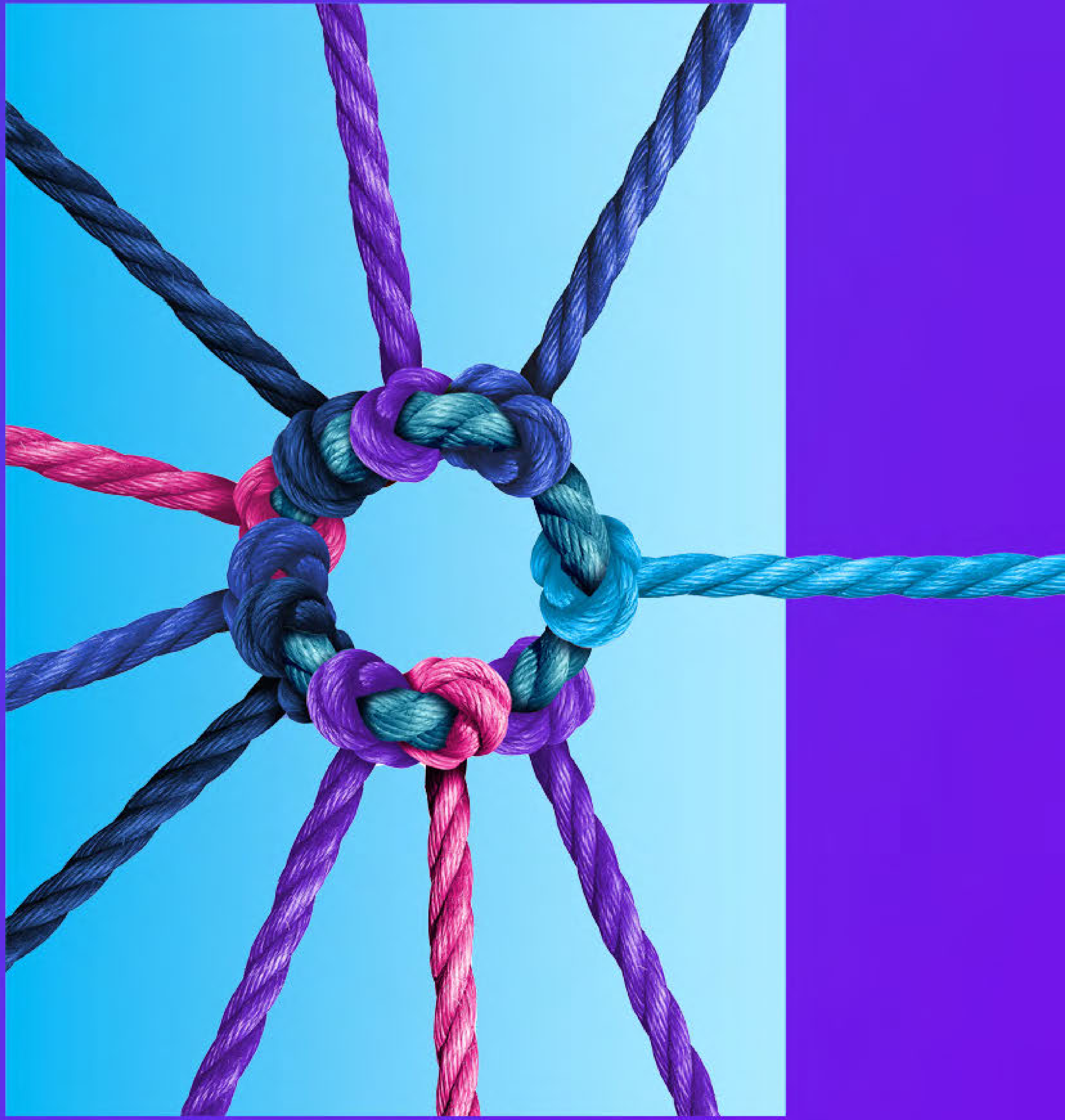
The Role of Trusted & Innovative MSSPs in Empowering Canada's Cybersecurity:

Strategic insights from the 2024 Canadian Cybersecurity Managed Services Survey

Read now ›



Contents

About the survey

KPMG in Canada surveyed 105 Canadian companies from January 2 to 10, 2024 on Sago's Methodify online research platform about their use and expectations of Managed Security Services Providers (MSSPs), with special focus on the managed detection and response (MDR) services they receive.

22% of the respondents are Chief Technology Officers

20% SVP or VP of Information Technology

17% are Chief Information Officers

17% are in Cybersecurity (Director Level and Above)

28% of respondents have between 10-20 FTE employees dedicated to cybersecurity

19% have 20-30 employees

16% have 30-40 employees

14% have 40-50 employees

60% of the companies have between $50MM and $499MM in annual revenue

13% have $500MM to $699MM

19% have $700MM to $1bn

9% have more than $1bn

The Role of Trusted & Innovative MSSPs in empowering Canada's Cybersecurity

Strategic insights from the 2024 Canadian Cybersecurity Managed Services Survey

Organizations have significantly increased their cybersecurity investments over the last five years due to immediate and constant cyber threats. Internet-facing systems are subject to automated vulnerability scans on a 24/7 basis – and common cyber threats including ransomware, data breaches, and fraud are becoming increasingly complex with the advent of disruptive technologies, like the cloud or generative AI, and the new hybrid way of working. In this rapidly evolving threat landscape, organizations face new challenges and expanded attack surfaces, necessitating innovative, robust, and wide-reaching defensive strategies.

At the same time, many Canadian organizations face a shortage of skilled cybersecurity talent, resources, and budget, leading them to outsource to MSSPs. Our January 2024 survey shows small- to mid-sized Canadian organizations often rely on external service providers for cybersecurity. And while outsourcing often boosts their confidence in handling cyberattacks, organizations are also uncertain about their MSSPs' security practices, have doubts about their choice of provider, and face challenges in finding a vendor that meets their exact needs.

That's because organizations' expectations of MSSPs are high – and for good reason. Organizations don't just want the basics; they want knowledge, training and insights, advanced technology capabilities, and exceptional skills and expertise to help them stay ahead of continually evolving and ever advancing cyber threats. To meet these needs, organizations must articulate their issues clearly to their service providers. However, they often lack the internal expertise to effectively communicate their needs and support their MSSPs in addressing their unique cybersecurity challenges. Without dedicated internal support, MSSPs can struggle to meaningfully understand their clients' challenges, and fall short in providing effective solutions.

So, while Canadian organizations want and are willing to pay for cybersecurity innovation and expertise to protect themselves and respond to threats, they often face a high degree of uncertainty about whether their vendors are actually doing what they say they're doing, as many of these services aren't "visible" to them.

This report examines Canadian organizations' current cybersecurity postures – and offers insights to help take a more strategic approach to decision making, address budget and performance challenges, and get the support needed to move forward with confidence and trust.

Click here to discover how KPMG can help empower your cybersecurity posture.

Weighing the costs of cybersecurity programs

Internal SOC or external MSSP?

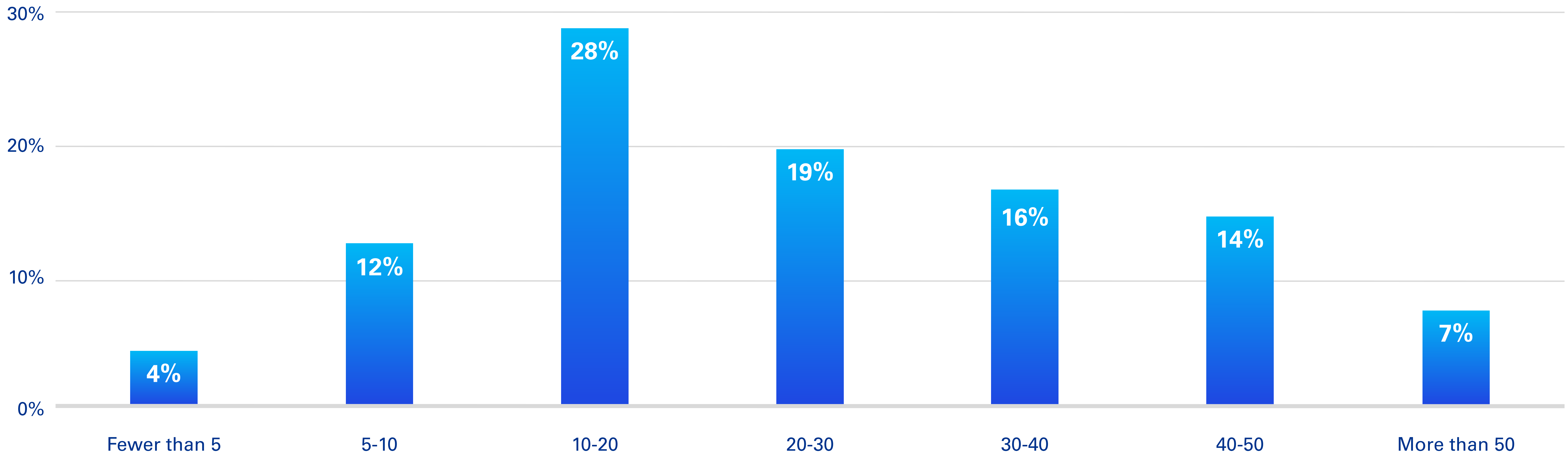
Modern Security Operation Centers (SOCs) are often responsible for preventing, detecting, and responding to cyber threats. The cost is very different, however, if a SOC is operated internally or managed via an MSSP. To better understand trends in MSSP engagement against this known discrepancy, we've correlated survey respondents' annual revenues with the sizes of their security teams and stated MSSP spend.

The largest group of respondents indicate they have between $50MM and $499MM in annual revenue, and among those, one third have between 10 and 20 FTEs dedicated to cybersecurity. Many factors influence the size of security teams, in particular the SOC. And while as a rule of thumb, 24/7/365 monitoring calls for 3 FTEs per shift (six people for two 12-hour shifts, nine for three 8-hour shifts), this is a starting point and increases with volume, assets monitored, etc.

How many full time employees are in your cybersecurity department or dedicated to cybersecurity?

Your SOC monitors your company's network and assets for threats, but it's not the only thing they're accountable for. Leveraging an MSSP to deliver certain services, such as MDR (Managed Detection and Response), frees your SOC from the need to overly specialize, letting internal talent focus on higher value security work. It's also important to consider the distribution of skills among members of your SOC. Asking too much from one person can lead to employee dissatisfaction (at a minimum), and threats going undetected, as fewer personnel will gravitate to higher-value activities, by default.

Although roles in a SOC are often tiered and differentiated, the most effective SOCs operate with fluid integration between people, processes, and technology at all levels. With these integrated processes in mind, it's important to evaluate your internal needs based on the load and volume that each of these operational pillars receives.



Total number of respondents = 105

Cybersecurity table stakes

The high cost of maintaining an internal SOC

Some organizations continue to run whole SOCs internally, rather than outsourcing key functions, such as MDR for example, to MSSPs. Smaller companies often try to do it all, without enough resources to do it effectively. However, the SOC performs many other functions – and not focusing enough on any one of these other areas exposes your organization to vulnerabilities. Companies need their internal SOCs to do the things they are best equipped to do and transfer the rest to MSSPs.

Maintaining focus with a fully enabled internal SOC team is becoming more and more rare, achievable by only the largest organizations. Because of the scarcity of cybersecurity talent and the increasing challenges of keeping pace with the rapidly changing landscape, the cost of establishing and maintaining an internal cybersecurity team continues to rise:

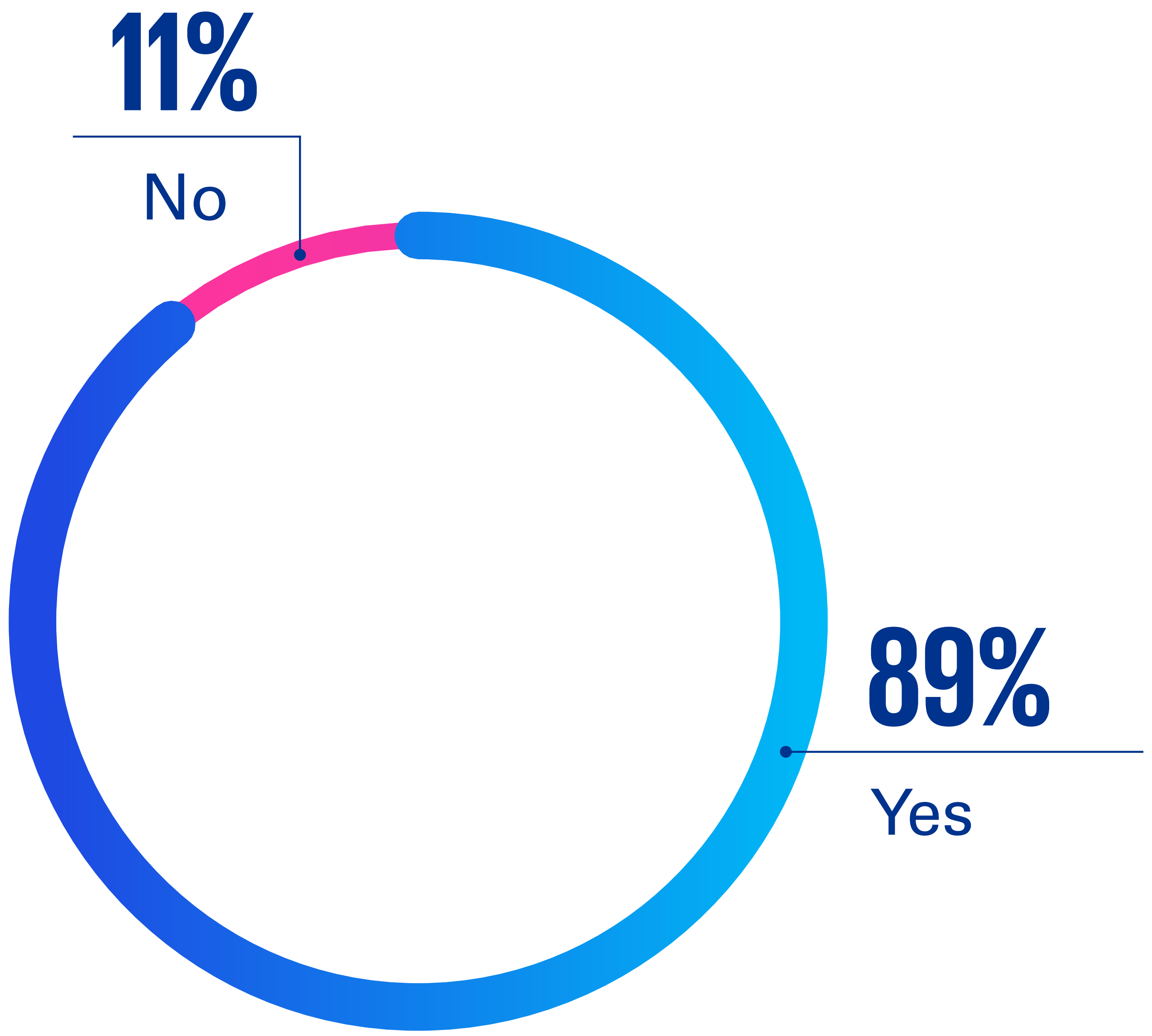
Industry average costs associated with establishing and maintaining internal cybersecurity teams:

Minimum 8 to 10 cybersecurity professionals	$100K to $150K each annually
Technology infrastructure	$1MM
Annual maintenance fees	25% to 30%
Total	**$1MM to $3MM annually**

It's no secret that owning and operating a SOC doesn't come cheap. Many organizations cite the eye-watering cost of establishing in-house SOC capabilities as a primary driver for outsourcing them to an MSSP. In this survey, 89% of respondents indicate they have already outsourced some or all aspects of their program to an MSSP, and the remaining 11% indicate they plan to engage an MSSP in the next 6 months.

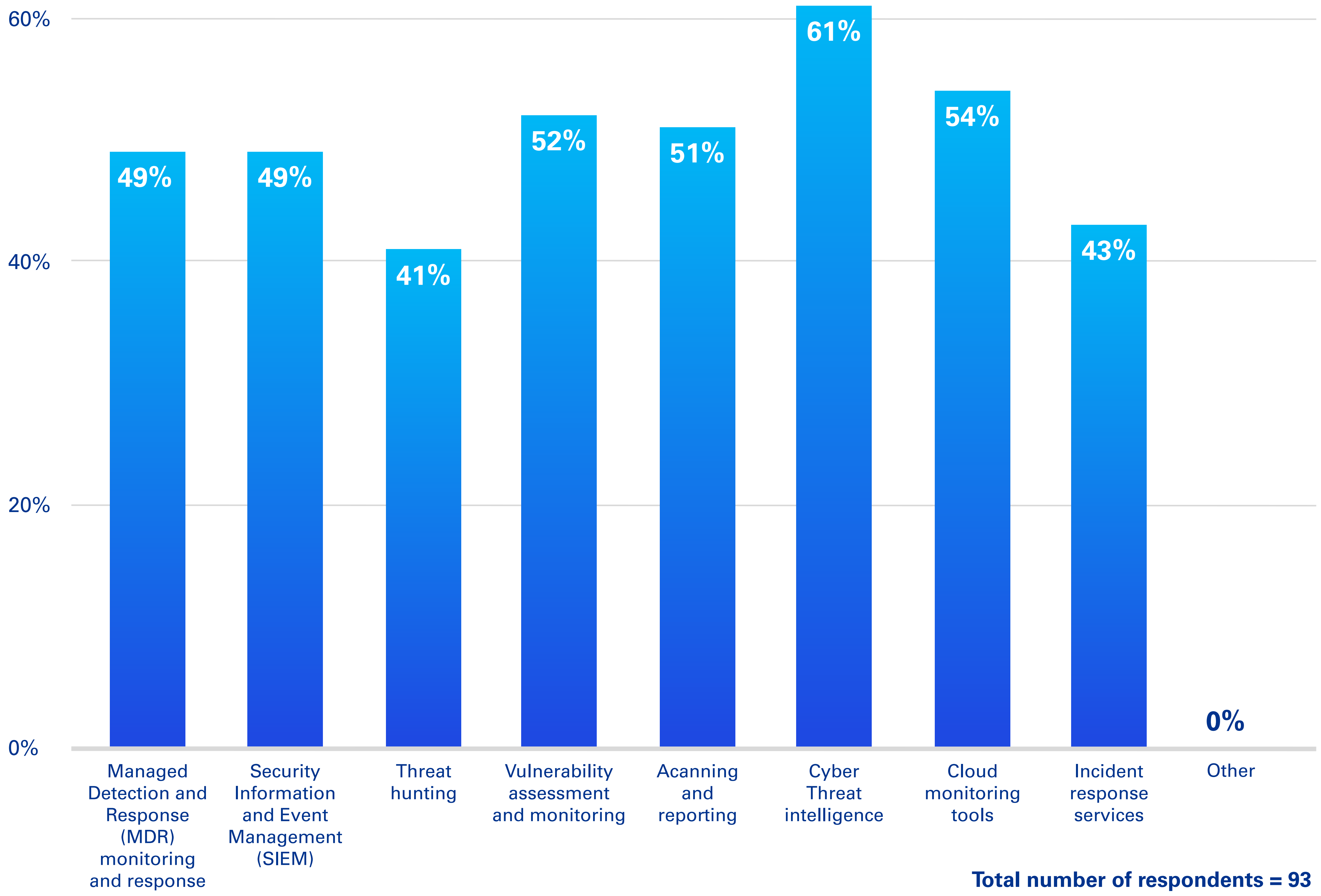
A managed security services provider (MSSP) is a third party that protects an organization against cyberthreats. An MSSP takes on some or all aspects of a customer's cybersecurity program, such as detection and response, vulnerability management, or application security.

Does your company use an MSSP?



Total number of respondents = 105

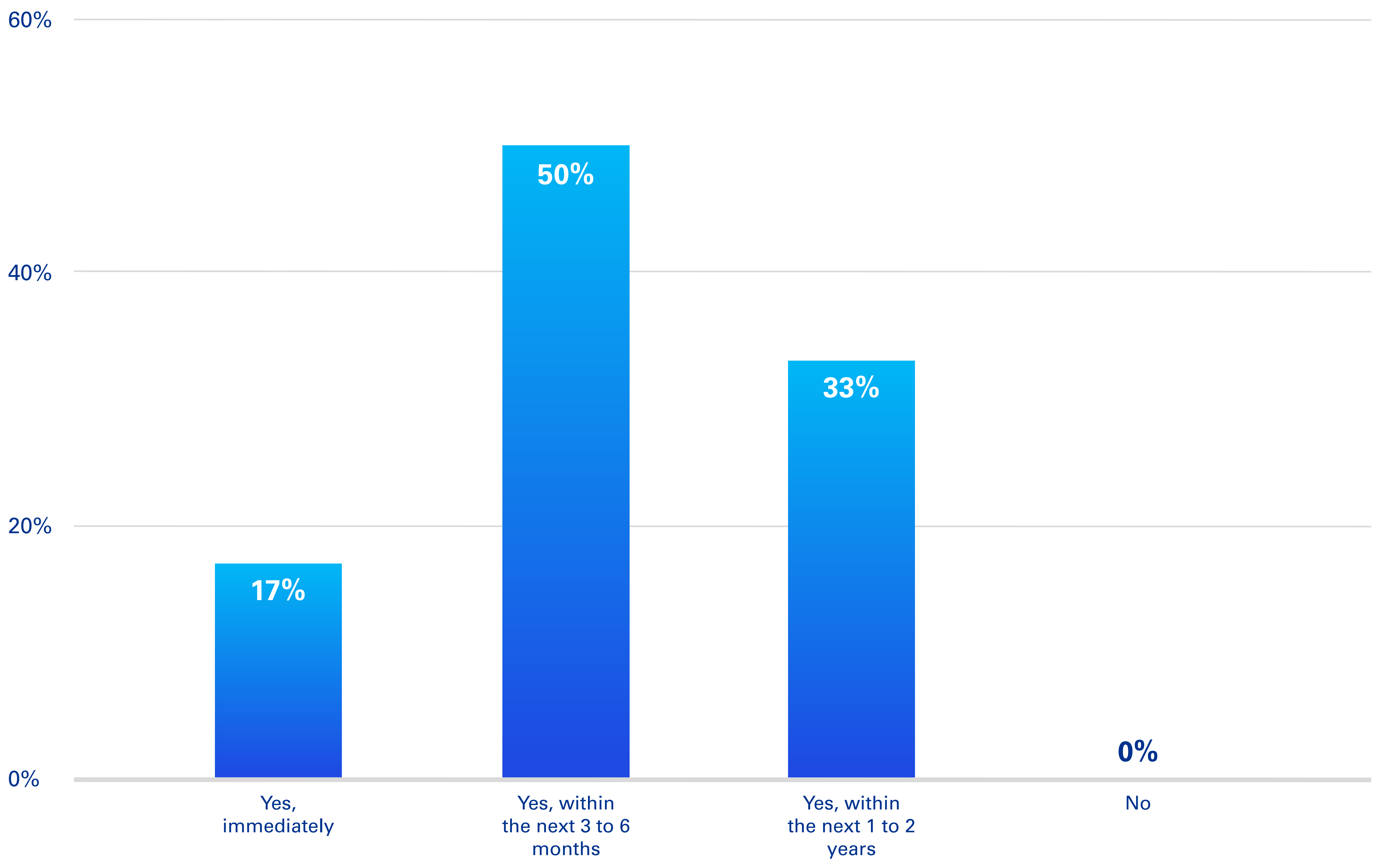
If you responded "yes" to using an MSSP, what types of services does your MSSP provide?



Total number of respondents = 93

If you responded "no" to using an MSSP, is your company looking to engage or renew with an MSSP?

Opting for an MSSP can be a strategic choice. Selecting the right provider ensures access to cutting-edge technology and a skilled team tailored to your needs, relieving your security team from these tasks. This approach not only reduces costs but also allows your team to focus on strategic security initiatives that add greater value.



Total number of respondents = 12

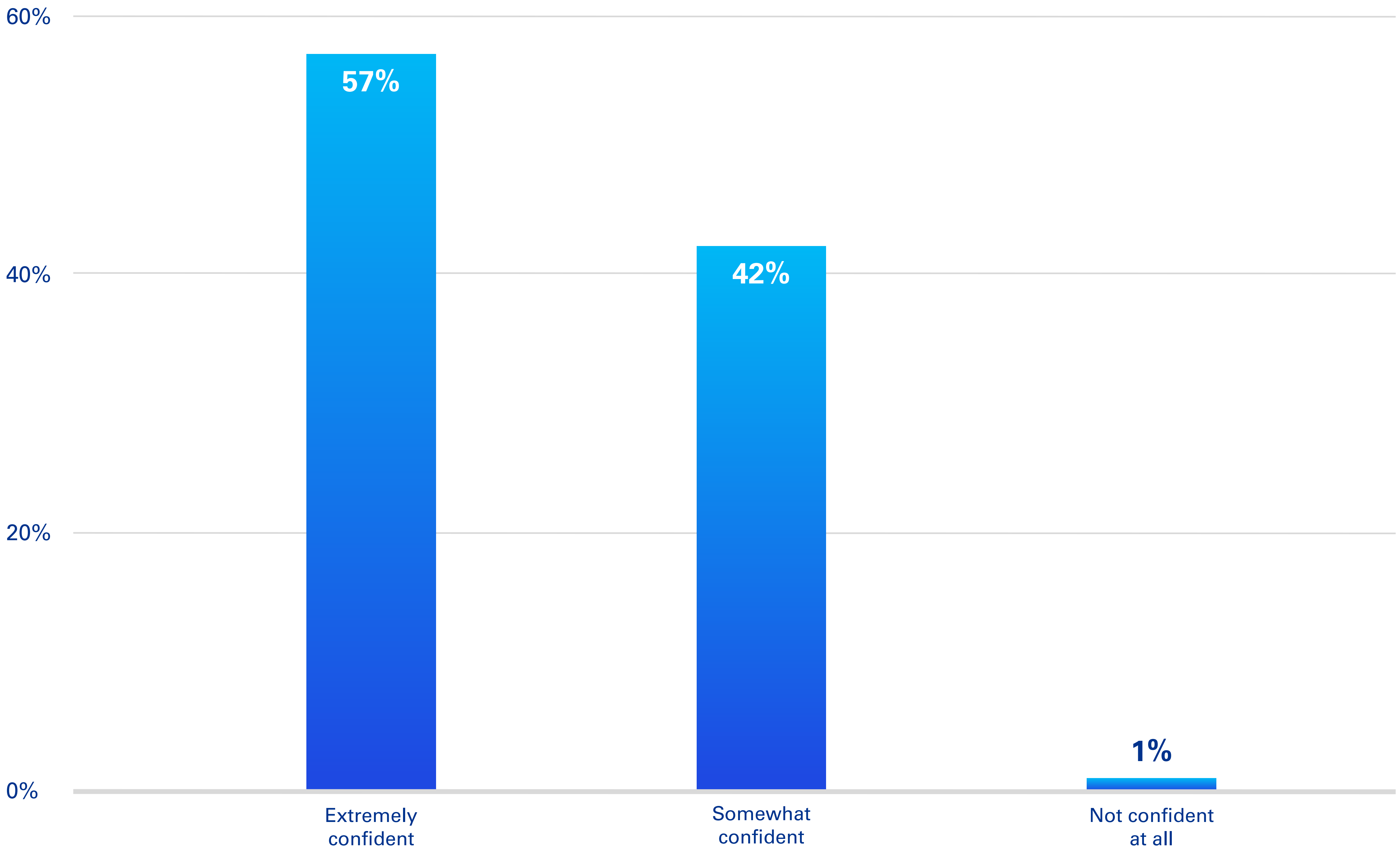
Confident, yet concerned.

Is this really the right MSSP for me?

Nearly all respondents believe their IT teams can prevent cyberattacks, with 89% also confident in their ability to recover from security incidents. However, this confidence may be overestimated, as many may not have faced severe enough incidents to truly test their cybersecurity measures. The real test of cybersecurity effectiveness is often only revealed after a failure.

Although most respondents believe that their current MSSPs and security teams can protect them from cyberattacks, it's important to remember that defenders might only need to be wrong once. With so much at stake, can you afford to be uncertain in your selection of vendors or service providers?

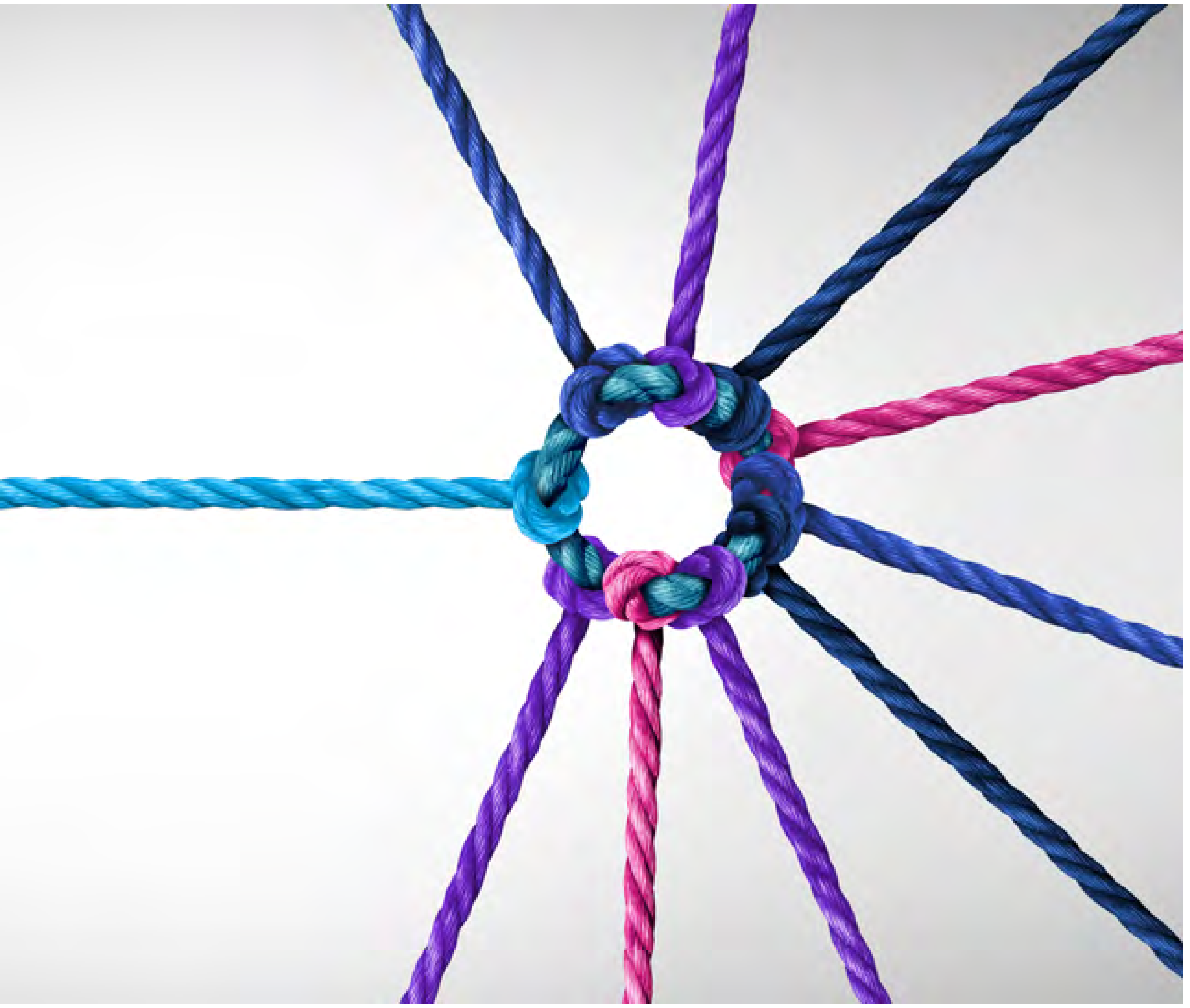
How confident are you that your information-technology (IT) team can protect your organization and prevent cyberattacks?



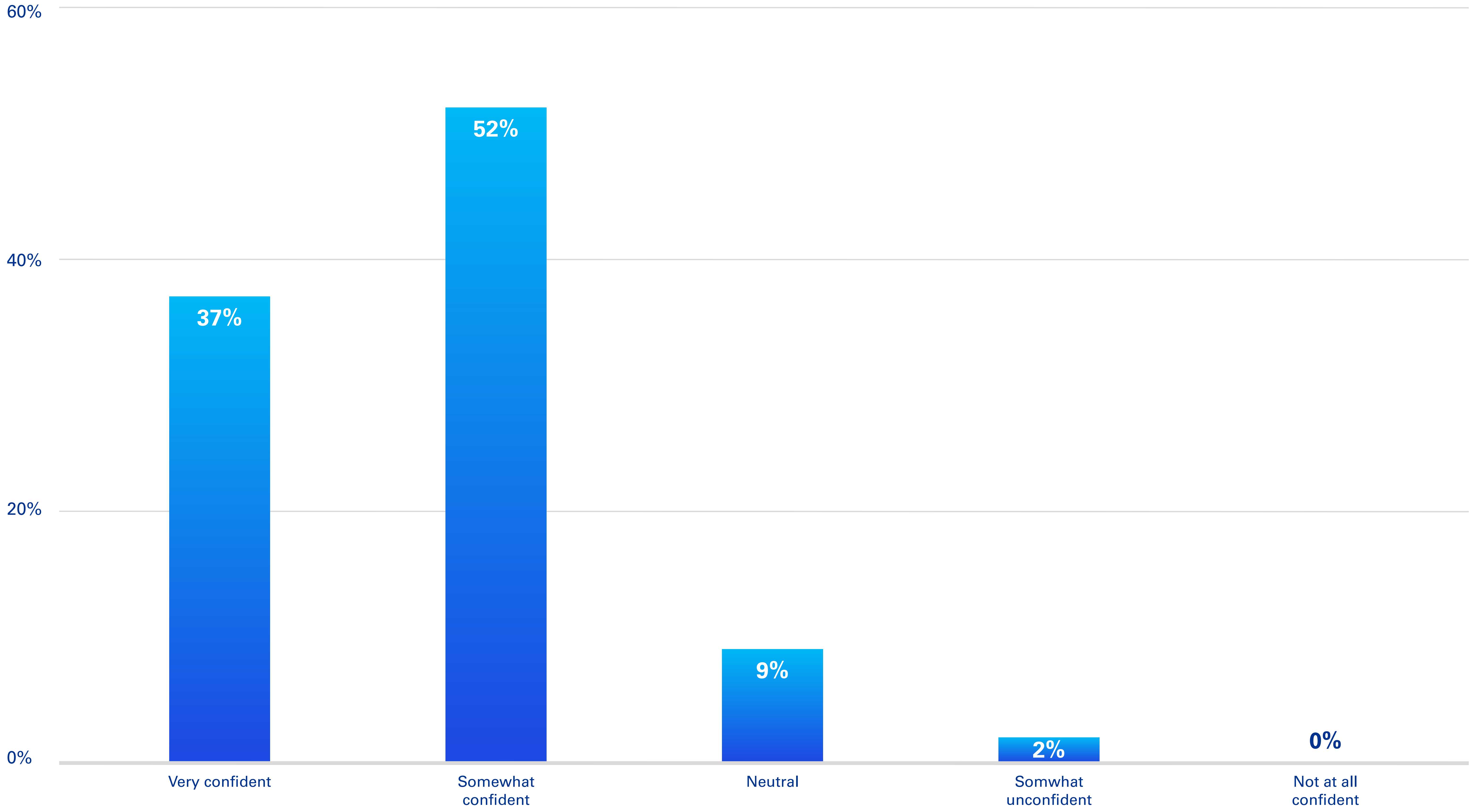
Total number of respondents = 105

How confident are you in your organization's ability to recover from a cybersecurity incident or data breach?

Canadian companies, while confident, also face challenges with selecting MSSPs and getting the greatest value from them. Two thirds (66 percent) have buyer's remorse and wish they had done more research before choosing the vendor they're currently using, 65 percent say they can't find the right MSSP vendor for their needs, and 69 percent are concerned about their MSSP's security practices.

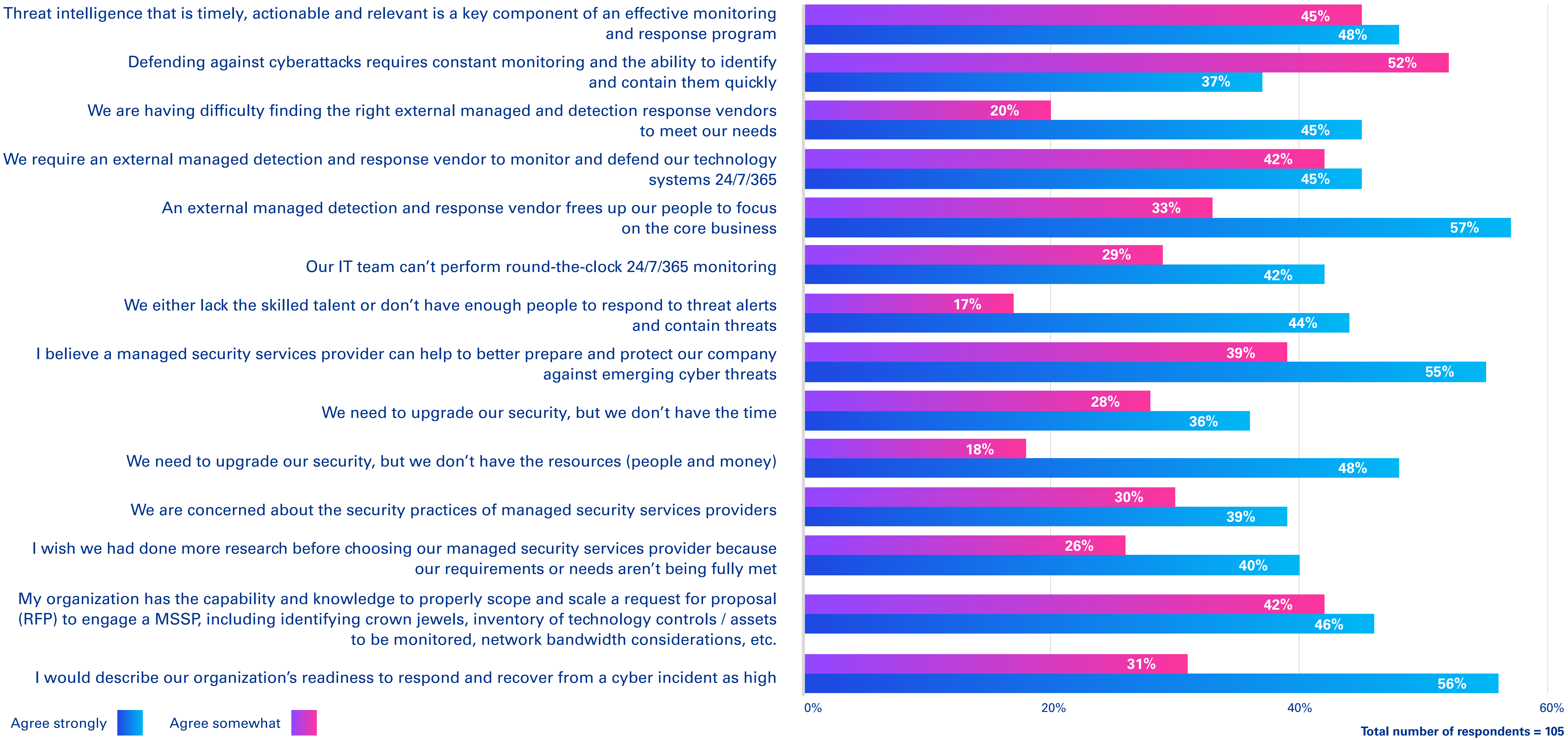


Taking a strategic approach to determine your cybersecurity requirements and aligning them to vendors' capabilities is a key step toward selecting the right MSSP. Spending more time on this up-front planning is critical to improving and ensuring you get the most out of your MSSP relationship – now and in the future.



Total number of respondents = 105

Please indicate if you believe (or agree with) the following statements



Total number of respondents = 105

Strategic steps in selecting your MSSP

In our recent publication, How to select the right Managed Detection and Response vendor for your organization, we detail the 10 key steps to consider when selecting a MDR vendor, which you can also apply to selecting your MSSP:

For successful MDR or MSSP implementations, you'll also need to:

- Maintain a small internal security team to liase with and support the MSSP in addressing priority issues for your business.
- Offload resource or time-intensive security functions from your internal security team that are better suited to your MSSP.
- Establish an IT asset inventory and IT asset management program to support your security functions.
- Ask your vendor what your key implementation risks are any how they plan to manage them.

1 Understand the problem you're trying to solve

2 Define your short-term and long-term goals

3 Research MSSP providers

4 Create your shortlist and evaluate vendors' capabilities

5 Assess vendors' ongoing service commitment

6 Assess vendors' reputations and credibility

7 Consider pricing

8 Evaluate the contract terms

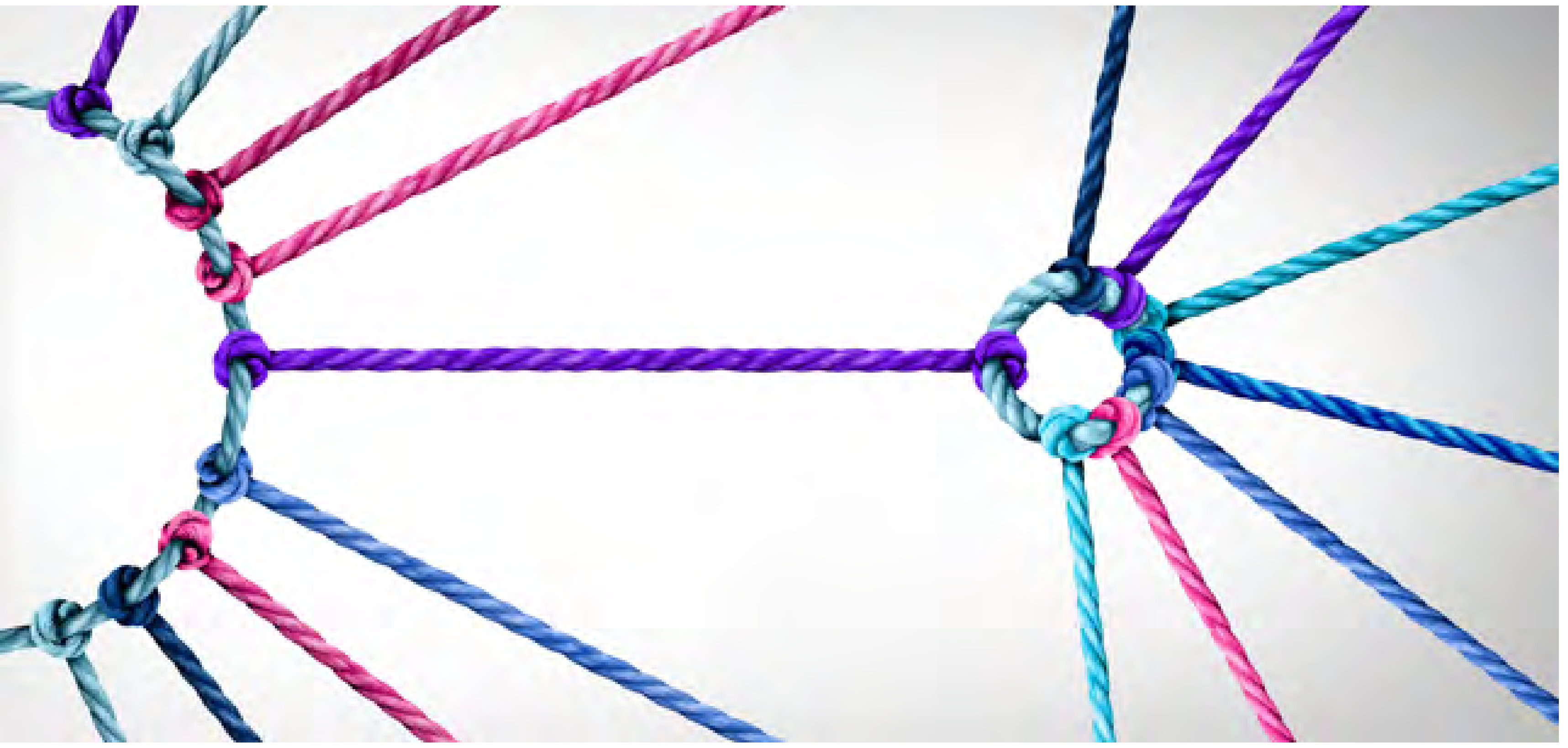
9 Consider differentiators

10 Request a demo

A matter of trust

What has my MSSP done for me lately?

Respondents are split on how involved they expect to be in managing their MSSP relationships. One of the key benefits of engaging an MSSP is they can take on the majority of day-to-day monitoring and security operations activities. Although they may execute these tasks under strict service level agreements (SLAs), it's important to remember you have ultimate accountability and oversight. At minimum, you fulfil a "trust and verify" requirement, but you also bring institutional knowledge and a business strategy focus that your MSSP won't consider when prioritizing or recommending actions.

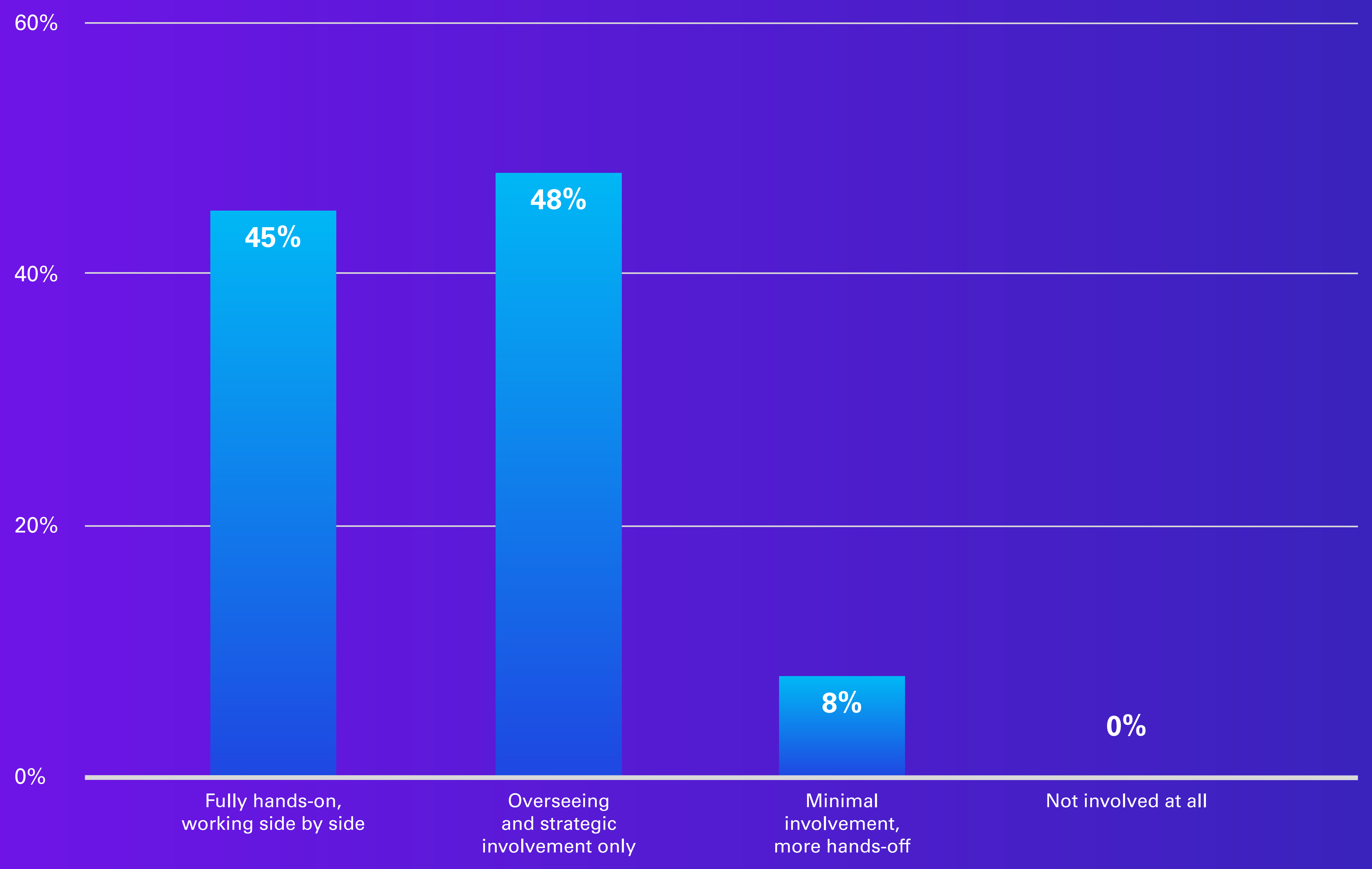


You can help enhance your relationship with your MSSP by having transparent conversations to ensure your MSSP meets your needs. After all, transparency goes two ways – it's important to communicate your strategy, and to understand how they will enable it. By better understanding your short- and long-term business and security objectives, MSSPs can be more accommodating, providing the added touch points and relevant communication you want, beyond what's outlined in the SLA.

Our survey found that respondents are looking for a breadth of education and knowledge sharing add-ons from their MSSPs. When companies put their security in the hands of MSSPs, in many cases the providers become one-stop-shops for all the cybersecurity services their clients require to protect themselves and address any incidents. This can include training for their internal teams, regular updates to stay informed on the latest cybersecurity threats, and advisory support on how to continuously enhance their defences.

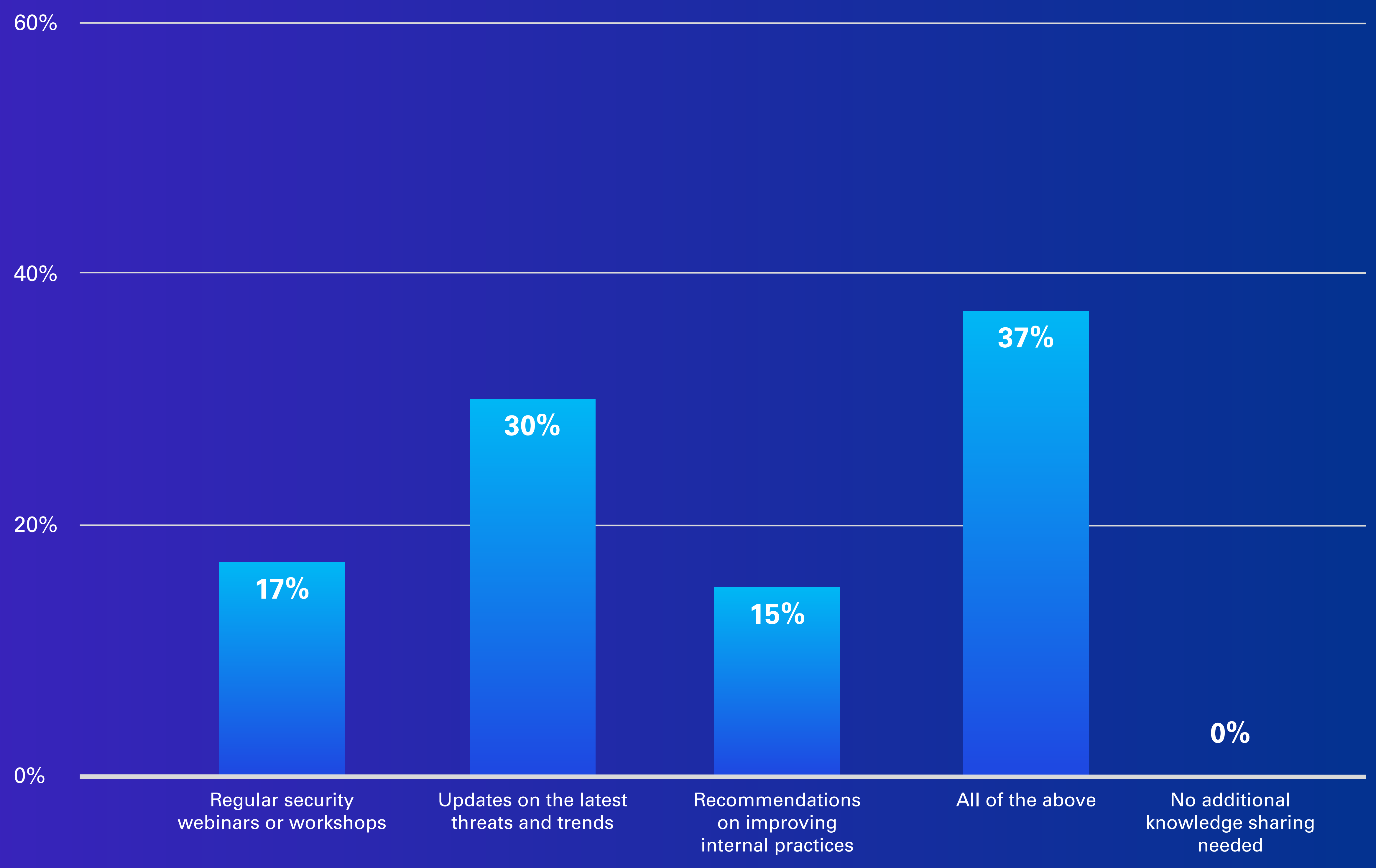
While more than half of respondents say they plan to oversee MSSP activities and only get involved at a strategic level or have only minimal involvement, the remaining 45 percent want their IT teams to work side-by-side with their MSSPs in a more hands-on capacity. This suggests they want a more detailed view of what their MSSPs do (and how they do it). They're looking for more touch points, communication, and insights to have confidence their MSSPs do the right things and do them well. This suggests there's room for improvement in the level of trust between companies and their MSSPs.

How involved do you expect your internal IT team to be in MSSP operations?



Total number of respondents = 105

What kind of educational or knowledge-sharing initiatives do you expect from an MSSP?



Total number of respondents = 105

Everything you should expect from your MSSP

In addition to providing cybersecurity services, education, and training, your MSSP should offer timely, actionable, and relevant insights to your business, and open, honest, and transparent communications.

The MSSP should also provide:

1
Expertise about your industry

2
Global trends and insights

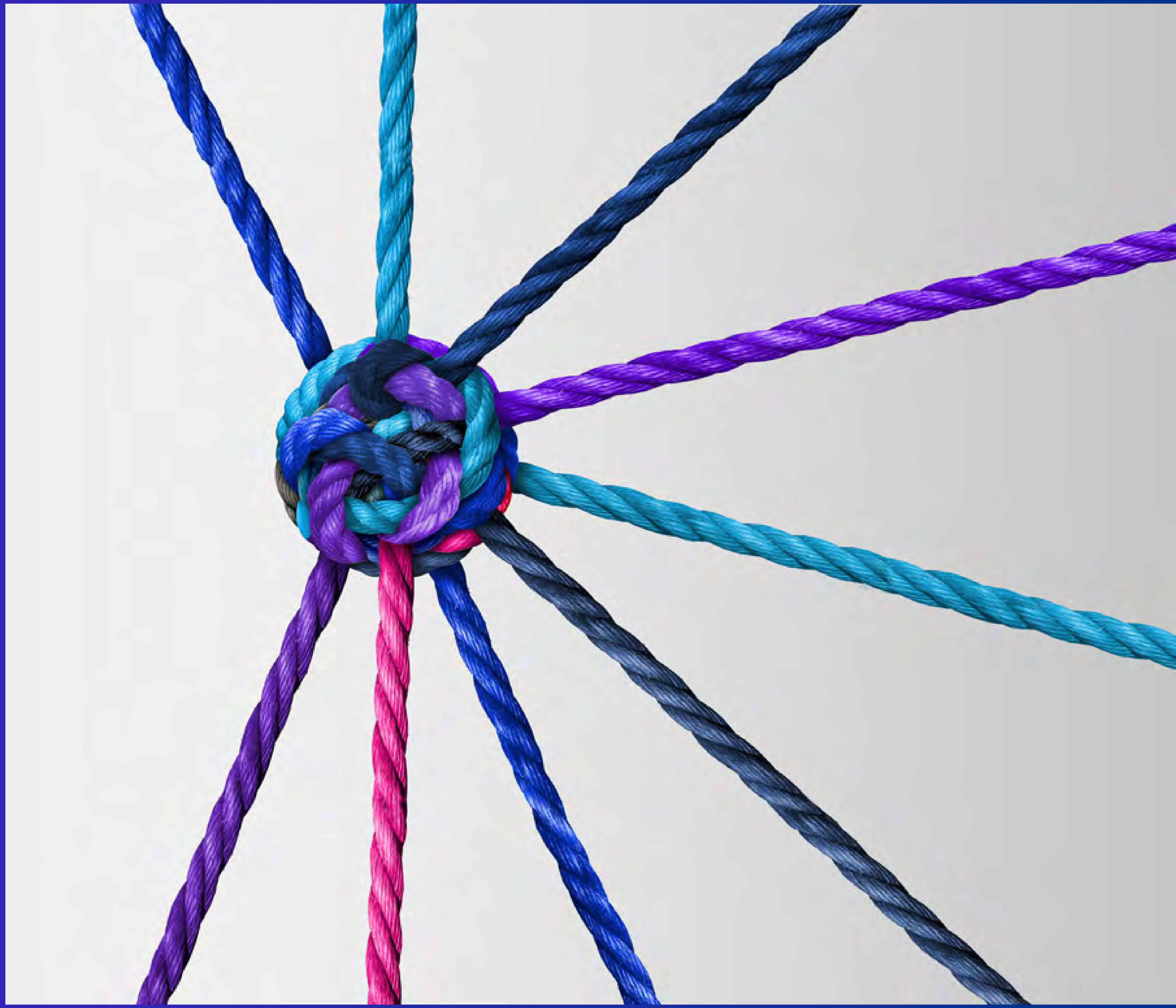
3
Enhancements to add programmatic risk reduction

4
Continuous improvement from the cybersecurity services they provide

5
Access to non-cybersecurity services and the professionals who support them

6
Boardroom experience and the ability to obtain and relay insights and connections across peers at the C-suite or Board level to foster collaboration

The "P" in MSSP not only stands for "Provider" but could also signify "Partner." High-quality MSSPs provide personalized service, acting as an extension of your team, aligning with your objectives, and partnering with you in preventing cybercrime.



KPIs and budget challenges

How do I prove cybersecurity ROI?

Measuring the effectiveness of cybersecurity monitoring services has always been a challenge for many organizations. The types of key performance indicators (KPIs) Canadian companies use vary widely including everything from threat detection rates (60 percent) to incident response times (48 percent).

While these high-level and more easily identified KPIs provide valuable views of how organizations' cybersecurity programs perform, other KPI's provide even more valuable data for organizations to learn from and help improve their cybersecurity positions.

Using the right KPIs

Your leadership needs KPIs and associated Key Risk Indicators (KRIs) that adequately represent your organization's readiness to manage risks. From an MSSP perspective, these KPIs and KRIs are often lacking, but most MSSP's won't have access to full data sets with which they can provide the level of detail needed. One area where MSSP's can (and should) do better, is providing more open reporting on the incidents they've handled. Often, we see "number of incidents opened/closed" by the MSSP, sometimes sorted by severity or classification, and framed in the context of the vendor's SLA. These are good, but can lead to KRIs that show increasing or decreasing risk that's usually limited only to what the MSSP can see or is accountable for, contractually.

Other metrics, like Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) can be helpful, but MSSP's should also be clear when it comes to false positive reporting – and highlighting true false positives versus non-incidents. MTTD and MTTR metrics can highlight if your MSSP is meeting its obligations or if your organization needs to invest more in controls or processes to improve detection rates.

Also, by providing a running list of service observations and recommendations, and "management response" to them, you can highlight the added value your MSSP provides, and what's being done with those recommendations when they're assessed as valid gaps.

Finally, tracking the number of remediation items identified (either as lessons learned from incident response activities, or valid findings from the MSSP), the time they remain open, and the success of the remediation activities are other useful metrics to justify security spend or identify constraints that may introduce additional risk. By automating tracking these kinds of indicators, you can uncover where some of your biggest risks lie – and have the information you need to help champion remediation with those who control the finances, address the gaps, and enhance your cybersecurity position.

Managing budget constraints

When we asked Canadian companies what their biggest challenges are in managing cybersecurity today, the evolving threat landscape was the top response (45 percent). A close second, however, was budget constraints (40 percent).

This too, is understandable. In the last five years as the cybersecurity landscape expanded and became more and more complex, organizations around the world significantly increased their cybersecurity budgets to keep pace – many by as much as five times. It's natural that the increase in cybersecurity spend should face a slowdown now, but it's one that's likely temporary. In the next few years, budgets will increase again, for several reasons:

1

Increasing number of transformation projects.

2

Heightened use of AI.

3

More use of cloud services.

4

Expanding attack surface.

5

Increasing scope and complexity of cyberthreats.

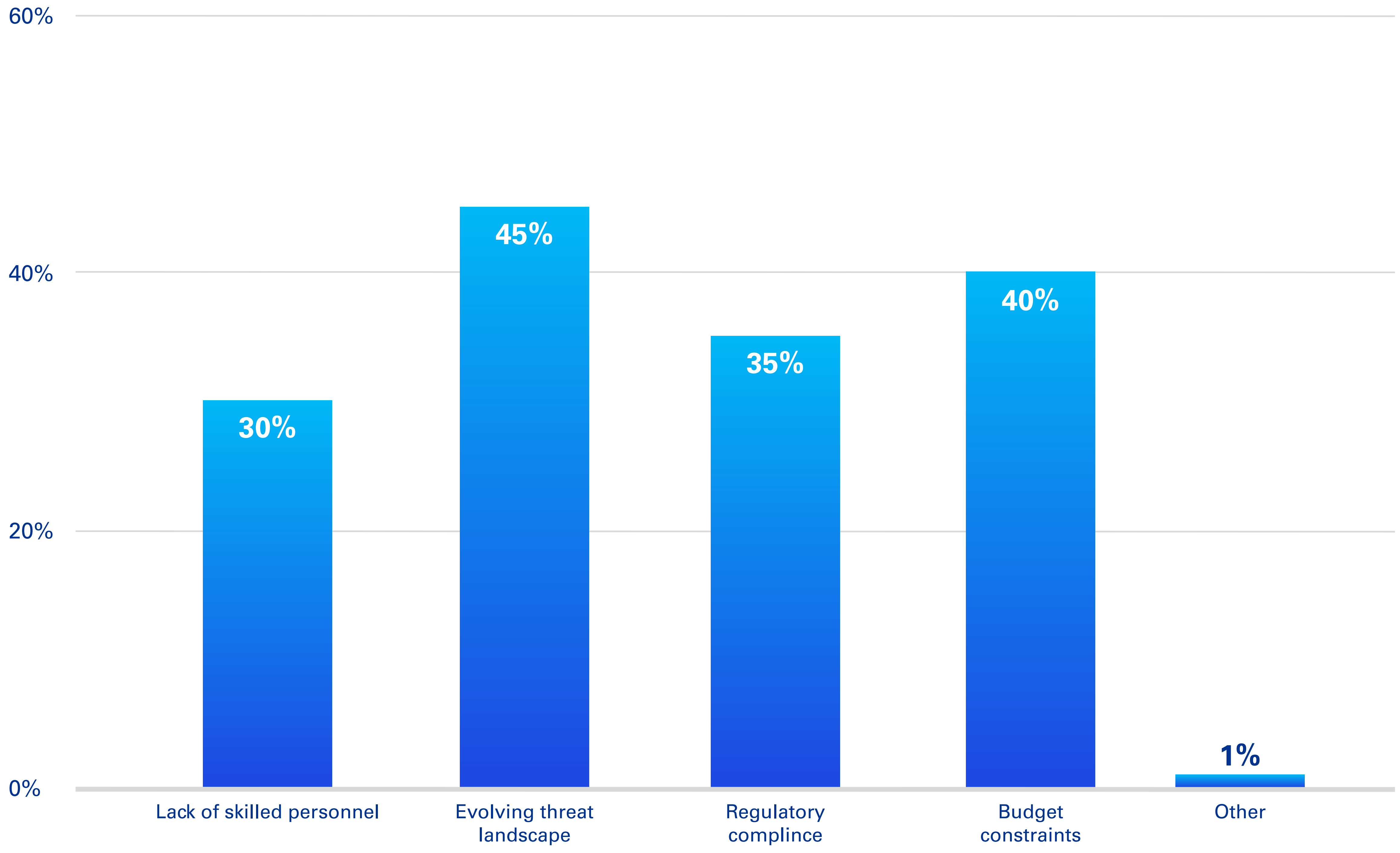
6

Increasing gap between cyberthreat maturity levels and the cybersecurity services organizations have in place to address them.

The challenge of establishing ROI can also lead to ongoing budget constraints for cybersecurity functions because it's difficult to prove the systems work and provide value – until they don't. A lack of significant incidents or breaches can lead C-suites and Boards into complacency, causing them to believe they've closed all the gaps and achieved the security levels they need. But the cybersecurity landscape relentlessly changes in scope and complexity, requiring constant enhancements and vigilance. Every cybersecurity program requires ongoing investments and enhancements to be effective and perform optimally.

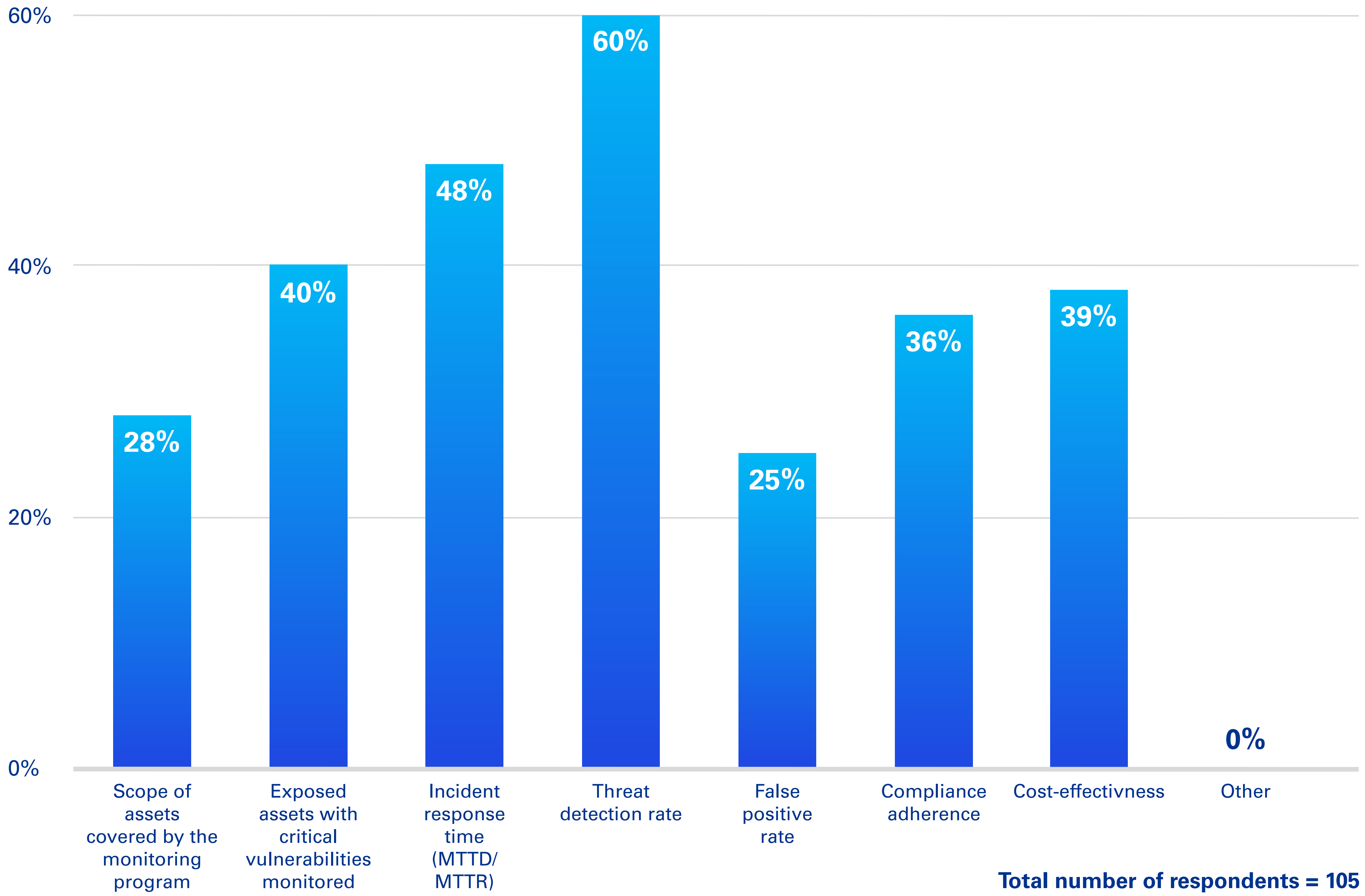
When we asked Canadian companies what their biggest challenges are in managing cybersecurity today, the evolving threat landscape the top response (45 percent). A close second, however, was budget constraints (40 percent).

What are the primary cybersecurity challenges your organization currently faces?



Total number of respondents = 105

What are the key performance indicators (KPIs) your organization uses to measure the effectiveness of your cybersecurity monitoring and response and/or incident response program?



Total number of respondents = 105

Rethinking your cybersecurity investment: The high cost of inaction and breach consequences

Making the case for cybersecurity budgets to Boards and C-Suites

The key to ensuring Boards and C-Suites understand the importance of investing in and continually enhancing cybersecurity programs is providing the right data. Ideally, MSSPs should report on what's working, what's not, and where your real risk exposures lie. By focusing on risk, you can frame these discussions around the impact and likelihood of cyber threats resulting in cyber incidents, and more effectively establish the cost of doing things properly vs. relying on luck as a primary strategy. For example:

- **Fines and penalties for non-compliance.** Use the EU's General Data Protection Regulation (GDPR) or similar regulatory benchmarks as an estimate of how much to spend vs the fines your organization could incur. GDPR penalties are $20MM or 4 percent of revenue for a data breach, demonstrating how much organizations stand to lose if they fail to make the right cybersecurity investments.
- **Use case examples and their costs.** Recent high-profile breaches at national and global organizations – that cost in the tens of millions – provide meaningful data about the high price organizations can pay for cyber and ransom attacks.
- **The average cost of a data breach.** Investing in robust MSSP services can pale in comparison to the cost of the average data breach – $4.5 MM globally and $5MM in Canada, according to IBM's Cost of a Data Breach Report 2023.
- **Lower staffing costs.** Engaging an MSSP to manage cybersecurity can reduce IT's FTE hours substantially and retarget the time and effort of higher-value staff.
- **Reduced insurance costs.** Demonstrating the effectiveness of the right cybersecurity program can lower insurance premiums.
- **Positive business benefits.** An effective cyber program can decrease costs from incidents and lower the frequency of business disruptive events.

Expertise, innovation, and trust

Driving cybersecurity programs to the next level

No organization is immune from cyberattacks and all must invest in cybersecurity approaches that work well for them. Taking a strategic approach to understand your needs, and having open and honest communication with your MSSP to increase trust and ensure they can meet your current and ongoing requirements are key steps in establishing a strong cybersecurity position.

It is equally important to make informed decisions about your cybersecurity programs and leverage meaningful KPIs to track your performance and better target your spend. Effective KPIs can help you to better equip your leadership to bolster your cybersecurity investment and maintenance over time.

By taking full advantage of your MSSP's expertise, IT and process innovation, and building trusted relationships with them, you can drive your organization's cybersecurity programs to the next optimal level, bridging the gaps between the cyberthreats of today and tomorrow – and how well placed you are to defend against them.

We can help

KPMG's **Managed Security Services & Security Operations Centre** combine leading technology, deep technical security expertise, and a proprietary threat intelligence model, with a dedicated Canadian cyber security delivery team to provide comprehensive, scalable, and fully customizable security solutions. Our **Managed Detection and Response** service, leverages the technologies you already have to power our correlation and automation tools. And our significant **Security Operations & Advisory** capabilities help enable continuous improvement and customization to meet your organization's unique security requirements to monitor, detect, and respond to cyberattacks on your behalf.

We can help you enhance your security capabilities, shorten response times, reduce costs, and minimize the impact of a threat event. We bring global reach and access to a pool of passionate subject matter experts who are committed to your success.

Contact us

Robert A Moerman

Partner, Cybersecurity Defense &
Managed Security Services Leader

General Toronto Area

416 777 8308 | rmoerman@kpmg.ca

Guillaume Clément

Partner, Cybersecurity and President of KPMG
Egyde Conseils

Quebec

418 653 5335 | guillaumeclement@kpmg.ca

KPMG

kpmg.com/ca

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.