Enterprise Strategy Group™
by TechTarget

Cyber-threat Intelligence Programs: Ubiquitous and Immature

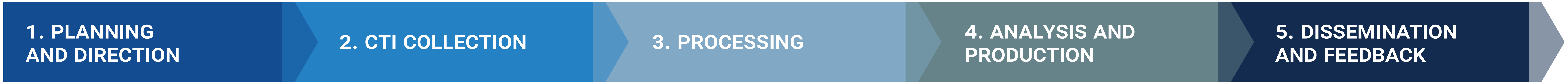
Jon Oltsik, Senior Principal Analyst & Enterprise Strategy Group Fellow

DECEMBER 2022

Research Objectives

Cyber-threat intelligence (CTI) is analyzed information about cyber-threats that helps inform security decision making. Although security professionals recognize the value of cyber-threat intelligence, many organizations still consume it on a superficial basis. Rather than collect, process, analyze, and disseminate cyber-threat intelligence to internal stakeholders, they simply look to cyber-threat intelligence for indicators of compromise (IoCs) like malicious IP addresses, web domains, and files that could be blocked by firewalls, email gateways, and endpoint security tools. Unfortunately, an IoC-based approach to CTI is extremely limited as adversaries can easily change IoCs, thus circumventing security controls, signatures, and blocking rules. Recognizing these limitations, most organizations have established CTI teams to gain a better understanding of the cyber-threats, adversaries, and attacks with the potential to disrupt business operations or steal sensitive data. This is the right decision, but establishing a productive CTI program isn't easy.

CTI program success depends upon a lifecycle approach spanning five phases:



1. PLANNING AND DIRECTION

2. CTI COLLECTION

3. PROCESSING

4. ANALYSIS AND PRODUCTION

5. DISSEMINATION AND FEEDBACK

Mature CTI programs formalize this lifecycle approach, gain a thorough understanding of adversary behavior, and respond with appropriate countermeasures. Immature CTI programs are fraught with waste, overhead, and constant questioning of program results and value.

Are organizations establishing mature CTI programs? What are the key success factors? In order to gain insights into these trends, TechTarget's Enterprise Strategy Group surveyed 380 IT and cybersecurity professionals at organizations in North America (US and Canada) with knowledge of and participation in their organization's CTI programs.

This study sought to:

Determine the current state of cyber-threat intelligence programs.

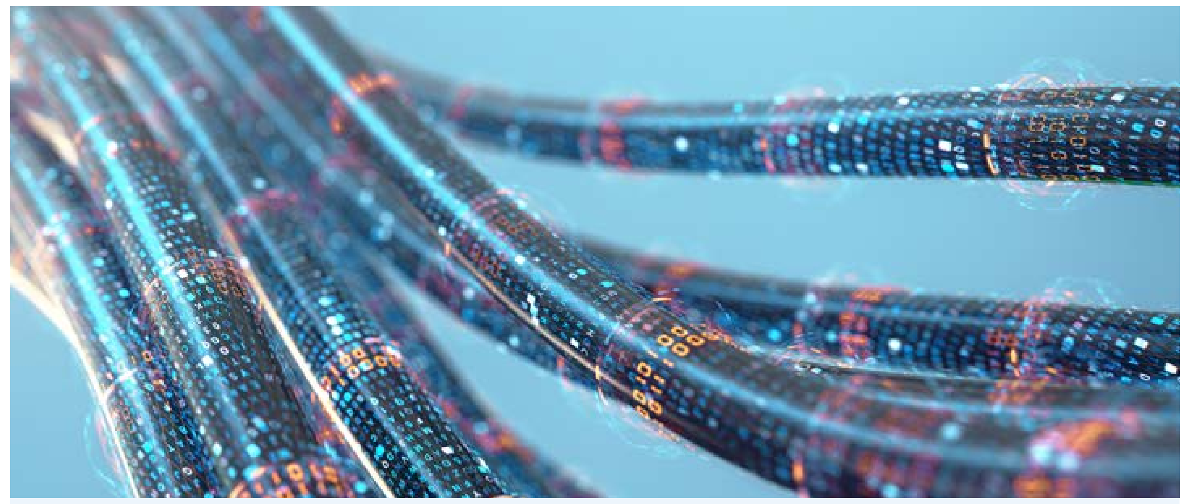
Highlight CTI program challenges and strategic plans.

Identify the stakeholders using cyber-threat intelligence and for what purposes they do so.

Establish the behavior and use cases of mature CTI programs.

KEY FINDINGS

CLICK TO FOLLOW

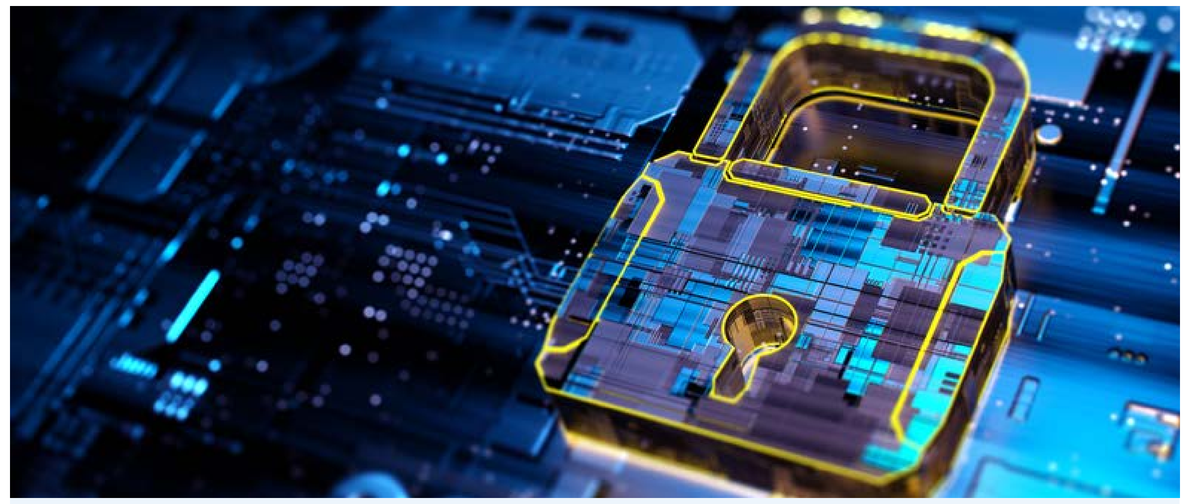


Cyber-threat Intelligence (CTI) Programs Are Pervasive

PAGE 4

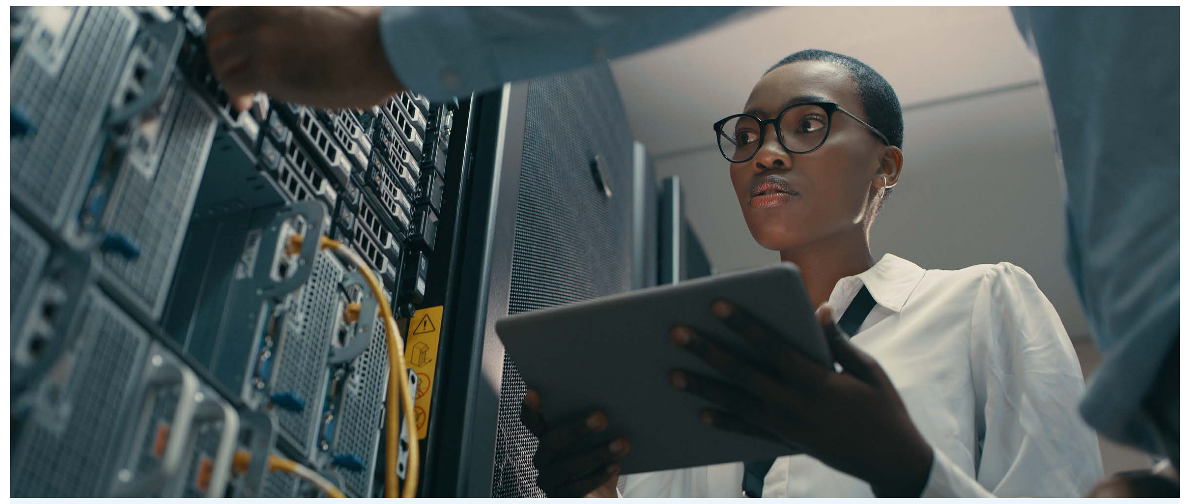
CTI Programs Remain Tactical

PAGE 10



Digital Risk Protection (DRP) Is Becoming an Essential Part of CTI Programs

PAGE 14



The MITRE ATT&CK Framework Is Mainstream and a CTI Program Driver

PAGE 17

CTI Programs Require Managed Services

PAGE 19

CTI Investments Are Planned

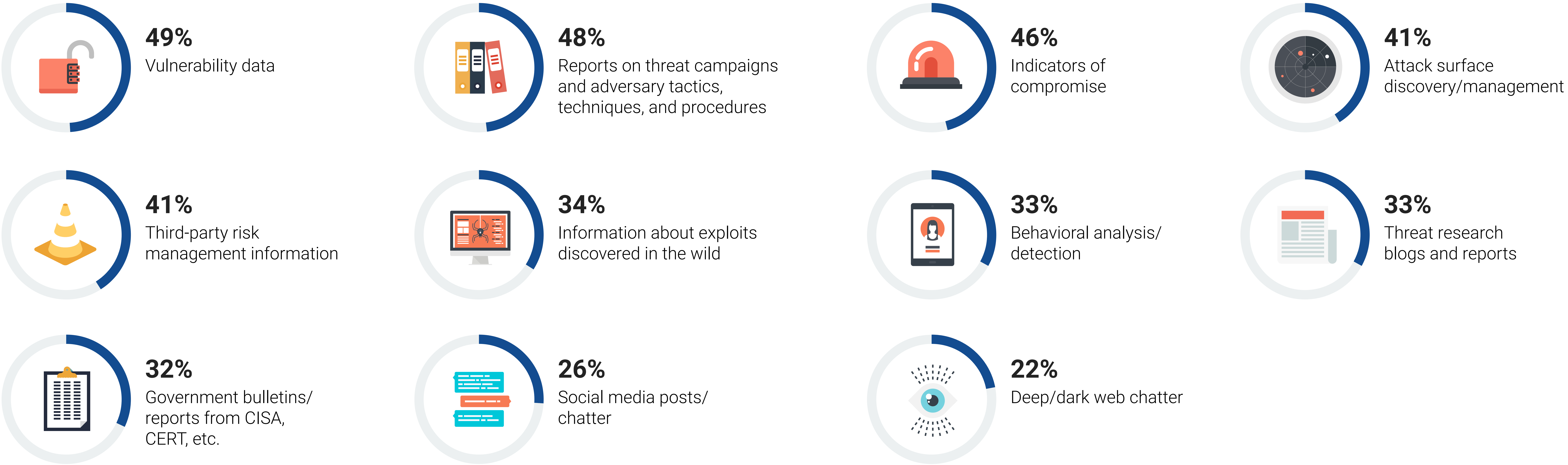
PAGE 22

Cyber-threat Intelligence (CTI) Programs Are Pervasive

Little Consensus on the Definition of CTI

Cyber-threat intelligence includes a wide variety of sources, consumed differently by different organizations. Common definitions include telemetry like vulnerability data, reports on threat campaigns, indicators of compromise, attack surface discovery, and third-party risk information. Organizations should determine their cyber-threat intelligence definitions based on their own requirements such as where they are located, their industry, and the types of cybercrimes or state sponsored attacks they are most likely to encounter.

Various definitions of cyber-threat intelligence.



49% Vulnerability data

48% Reports on threat campaigns and adversary tactics, techniques, and procedures

46% Indicators of compromise

41% Attack surface discovery/management

41% Third-party risk management information

34% Information about exploits discovered in the wild

33% Behavioral analysis/detection

33% Threat research blogs and reports

32% Government bulletins/reports from CISA, CERT, etc.

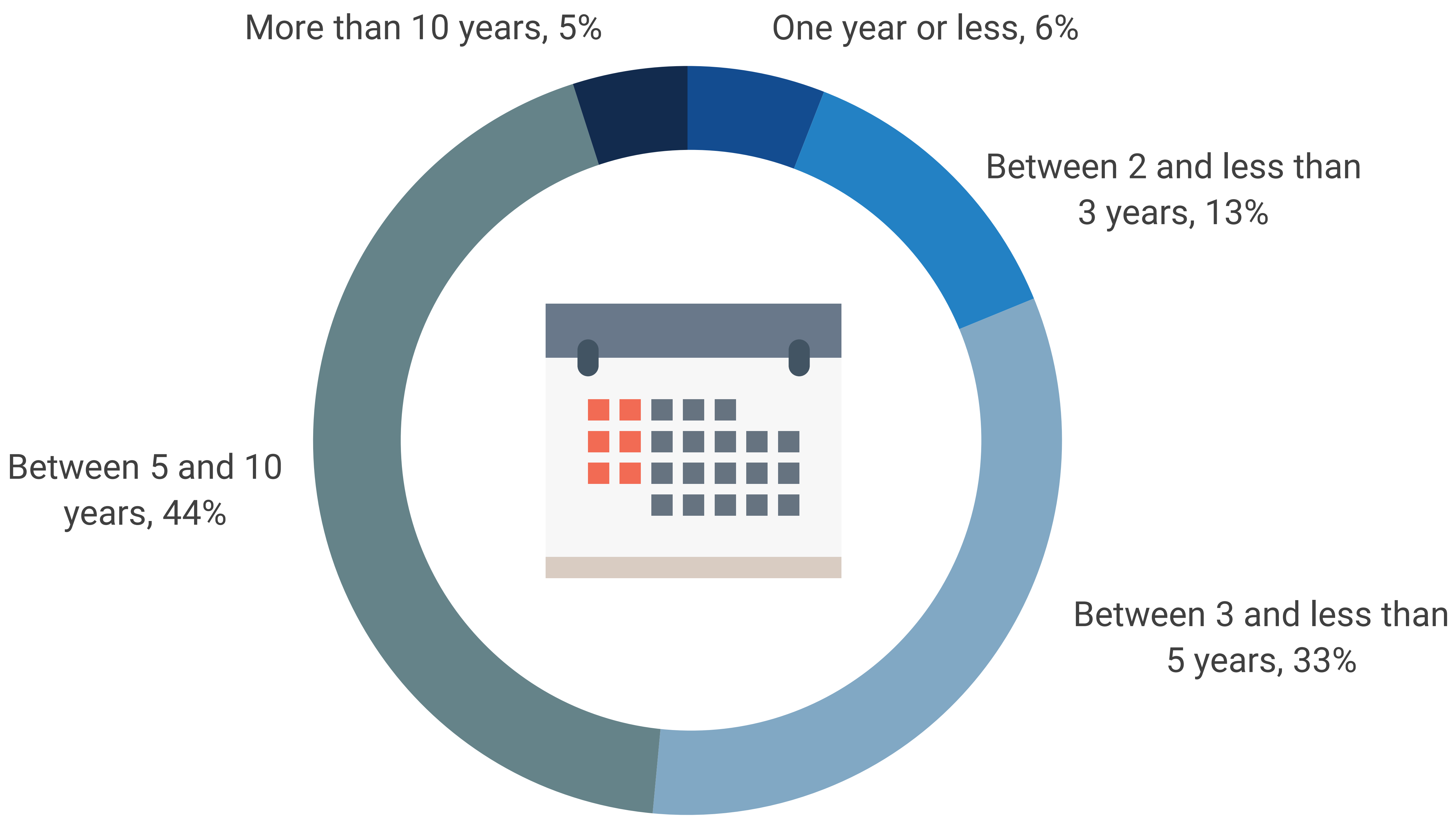
26% Social media posts/chatter

22% Deep/dark web chatter

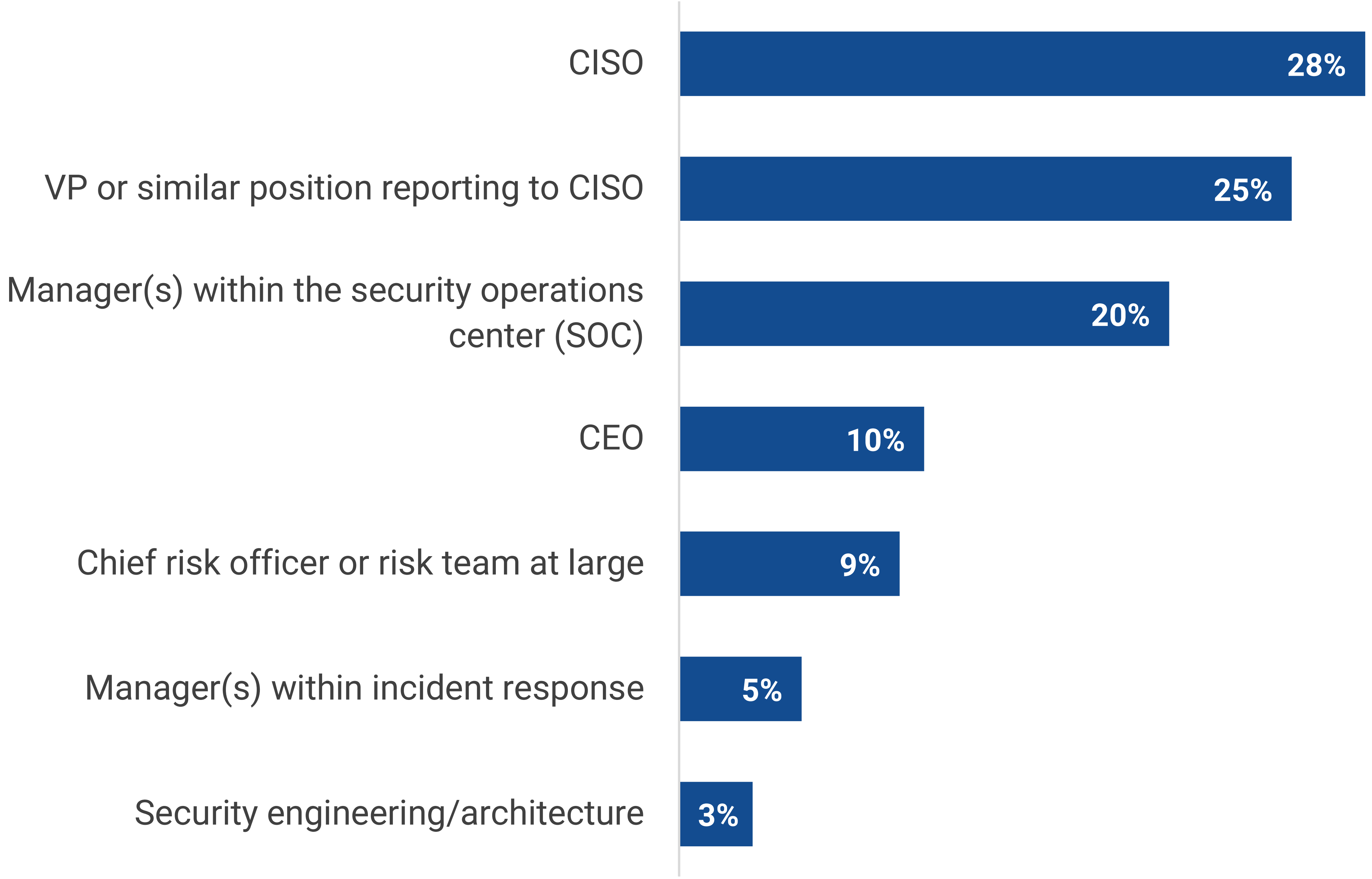
Many Well-established and High-visibility Cyber-threat Intelligence Programs

Nearly half of organizations have had a CTI program in place for longer than five years, with the CTI team reporting to different supervisors. Specifically, more than half report to at least the VP level, whether it's a VP reporting to the CISO (25%) or the actual CISO (28%), and another 20% cite a manager within the security operations center (SOC). A direct reporting pipeline to CISOs creates an opportunity to make CTI programs more strategic.

Length of time CTI programs have been in place.



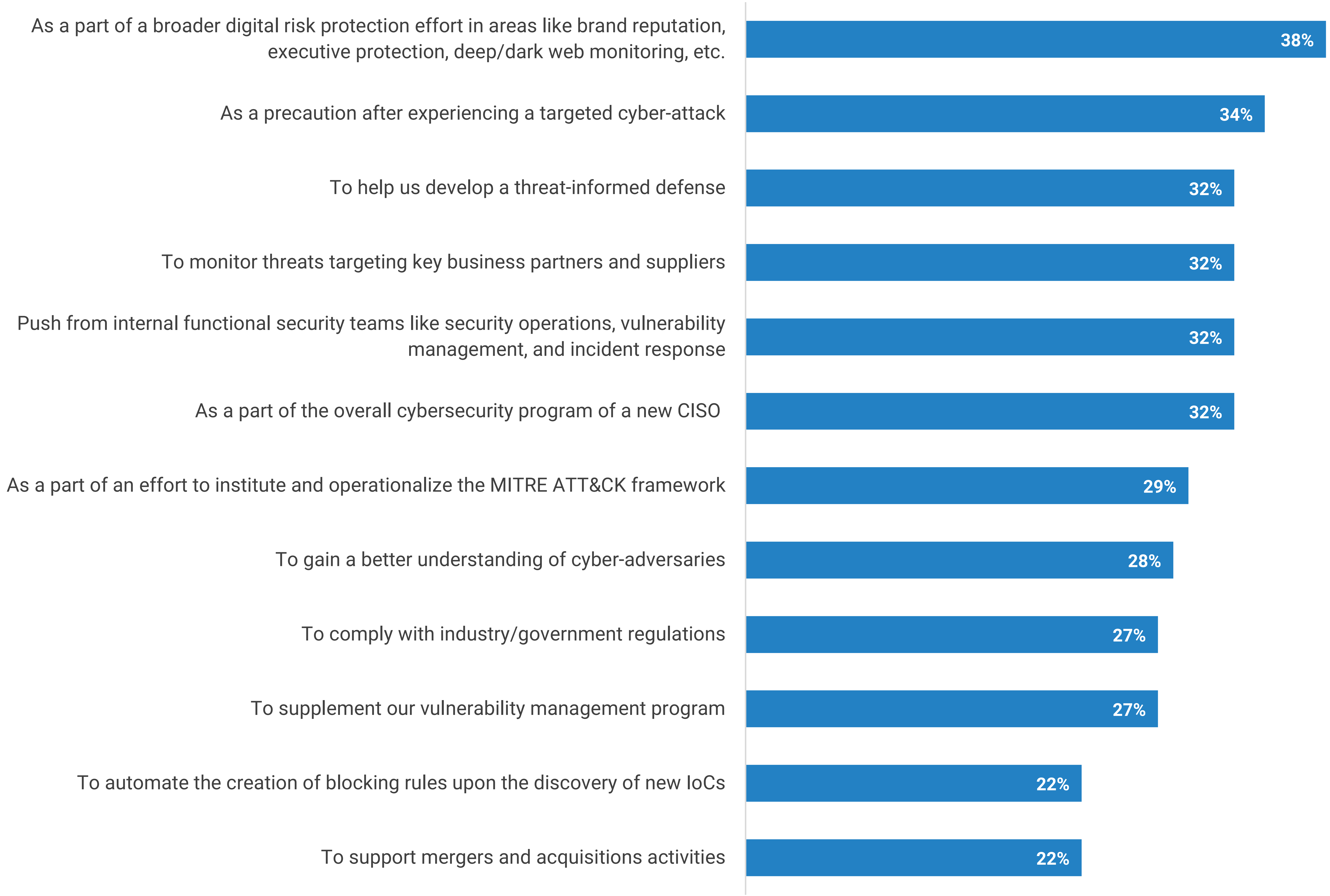
To whom cyber-threat intelligence teams report.



Primary Reasons for Starting a CTI Program

Cyber-threat intelligence programs can be implemented proactively to better understand threats and reinforce existing security processes and controls, but they can also be reactive based on the cyber-threat landscape generally or cybersecurity events specific to an organization. What is driving CTI program development? Organizations have established CTI programs for a multitude of reasons, including as part of a broader digital risk protection initiative, as a reaction to experiencing a cyber-attack, to help them develop a threat-informed defense, and to monitor threats to third parties. Additionally, CISOs often initiate a CTI program when they start a new job.

Primary reasons organizations established a CTI program.

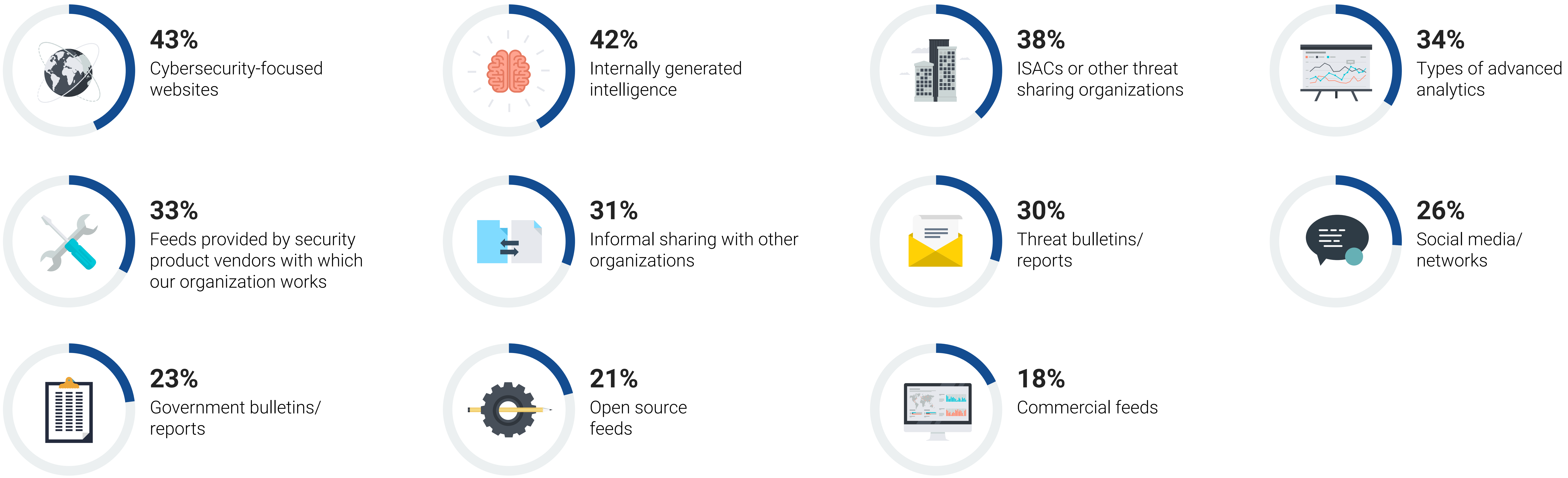


BACK TO CONTENTS

Wide Variety of CTI Sources Used, Illustrating the Complexity of Collection and Analysis

To track and understand cyber-threats and adversary behavior, cyber-threat intelligence analysts must become fluent with numerous sources like cybersecurity websites, internally generated telemetry, intelligence from ISACs, advanced analytics, and vendor feeds. This combination of data sources can easily overwhelm threat analysts struggling to find valuable needles in haystacks of cyber-threat intelligence data. Developing strong data collection, processing, and analytics skills is key for program maturity.

| Cyber-threat intelligence sources organizations currently use.



43% Cybersecurity-focused websites

42% Internally generated intelligence

38% ISACs or other threat sharing organizations

34% Types of advanced analytics

33% Feeds provided by security product vendors with which our organization works

31% Informal sharing with other organizations

30% Threat bulletins/ reports

26% Social media/ networks

23% Government bulletins/ reports

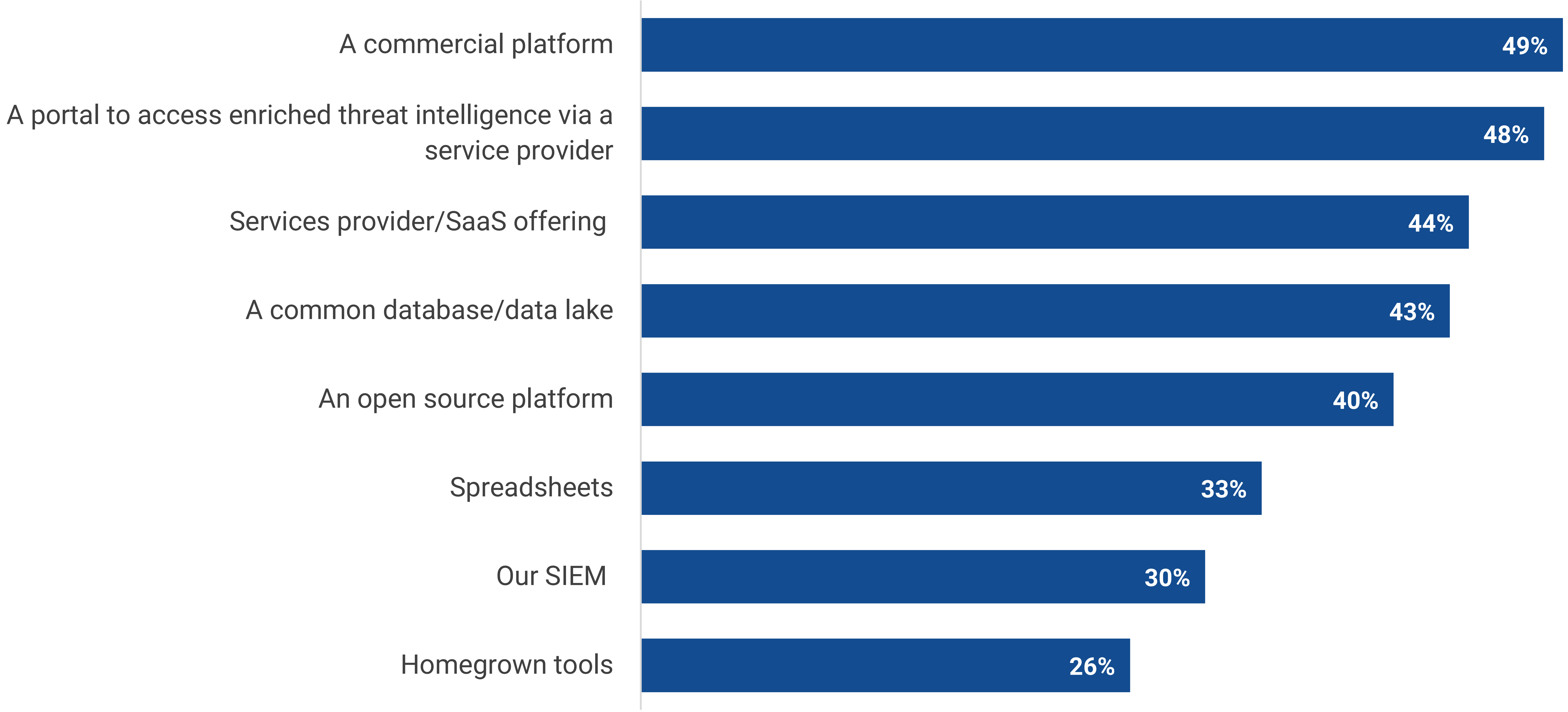
21% Open source feeds

18% Commercial feeds

BACK TO CONTENTS

“Deploying, configuring, and operating various cyber-threat intelligence technologies **adds overhead and complexity to CTI programs...”**

How organizations organize and gain context about external cyber-threat intelligence information.



Technologies Used to Gain CTI Context

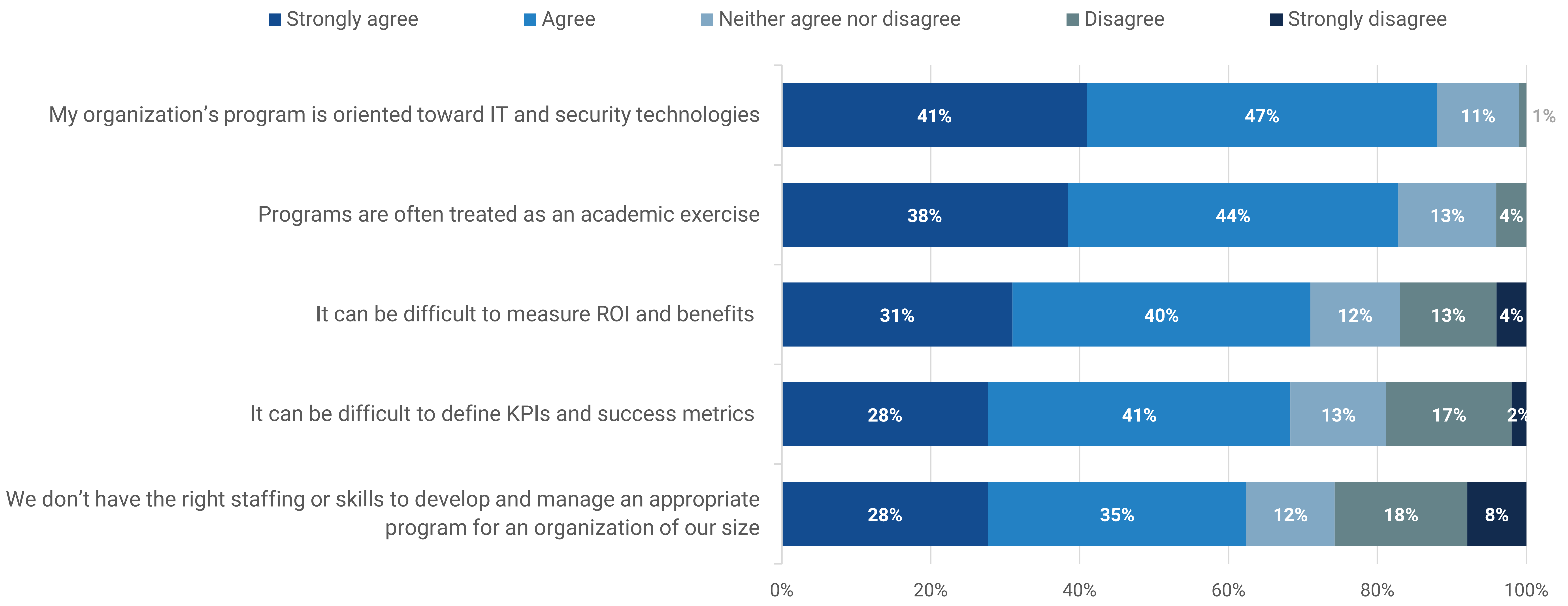
Cyber-threat intelligence teams need an assortment of technologies to help them collect, process, and analyze external cyber-threat intelligence, as well as to disseminate the subsequent outputs to multiple internal constituents. The most common of these tools include commercial platforms (i.e., cyber-threat intelligence platforms), service provider portals, SaaS offerings, databases/data lakes, and open source platforms (e.g., CRITS, MISP, etc.). Deploying, configuring, and operating various cyber-threat intelligence technologies adds overhead and complexity to CTI programs, driving the need for cloud-based solutions and help from third-party services.

CTI Programs Remain Tactical

CTI programs Have a Good Foundation but Lack Structure, Processes, and Objectives

While organizations strive for the right cyber-threat intelligence program objectives, it can be difficult to gain measurable tactical, operational, and strategic value from CTI programs. Many organizations tightly integrate cyber-threat intelligence analysis with security operations, as evidenced by the fact that 88% of respondents agree that their organization's CTI program is oriented toward IT and security technologies. Other issues are also evident: A majority (82%) of security professionals agree that their CTI program is treated as an academic exercise, leading to threat analyst accolades but limited program success. Little wonder then that more than two-thirds of security pros say it can be difficult to measure program ROI (71%) and/or define the right KPIs and success metrics for CTI programs (69%). Cyber-threat intelligence management and analysis also requires specialized skills, which are in short supply: 63% of survey respondents believe that their organization doesn't have the right CTI skills or staffing to manage a CTI program effectively.

| Opinions on CTI programs.



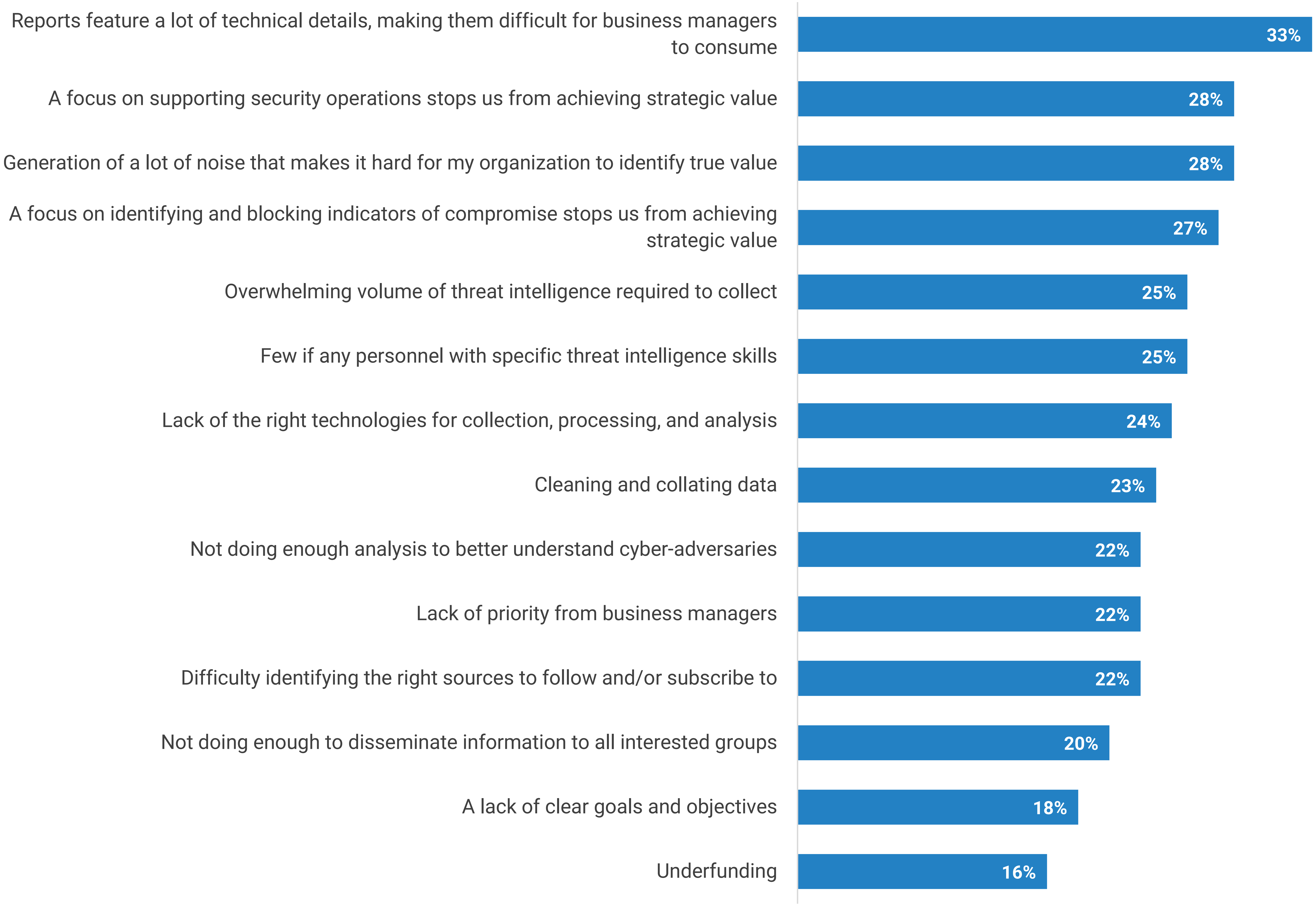
> "82% **of security professionals agree** that their CTI program is treated as an academic exercise."

CTI Challenges Suggest Program Immaturity

With the wide range of data sources, technologies, processes, and skills needed to support a CTI program, there is bound to be many program challenges. In fact, security professionals report challenges spanning the cyber-threat intelligence lifecycle such as overly technical reports for the business (i.e., dissemination and feedback), a focus on supporting security operations (i.e., planning and direction), and the generation of lots of noise (i.e., collection, processing, and analysis).

These challenges can be perceived as evidence of immature programs. When cyber-threat intelligence teams don't receive the right guidance and directives, they tend to collect and process data with a notion that "more is better." Consequently, they are often buried in volumes of redundant, noisy threat information. When this happens, all upstream activities are compromised: Data analysis is difficult, reports are overly complex, and cyber-threat intelligence consumers can't integrate strong CTI into their decision making.

Biggest challenges with cyber-threat intelligence programs.



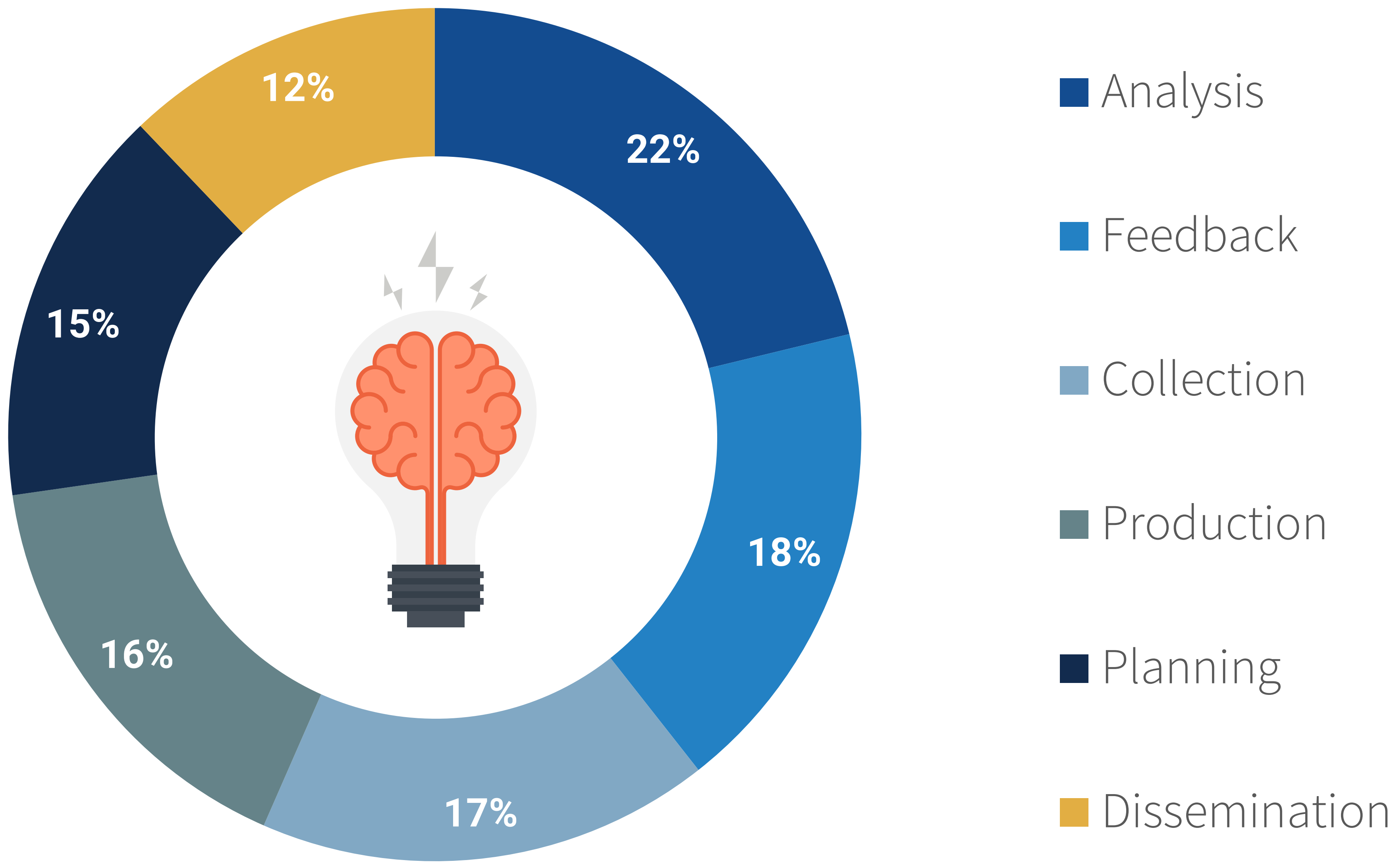
BACK TO CONTENTS

Lack of Proficiency Spread across All Phases of the Intelligence Lifecycle

The data also indicates that many organizations struggle at all phases of the cyber-threat intelligence lifecycle. While the results are fairly evenly split, the largest percentage of respondents report cyber-threat intelligence analysis as their area of least proficiency, which can only lead to incomplete reporting and inefficiencies in all downstream phases. Some aren't receiving proper feedback from CTI customers, limiting the ability to improve reporting and the program at large. Other issues through the collection and production phase plague CTI teams with an overwhelming volume of noisy and inaccurate data.

CISOs would be well served to get back to basics, starting with greater participation from CTI consumers. Organizations need more input defining priority intelligence requirements and regular feedback on what else is needed.

Phase of the CTI lifecycle in which organizations are **least** proficient.



> “While the results are fairly evenly split, the largest percentage of respondents report **cyber-threat intelligence analysis as their area of least proficiency.”**

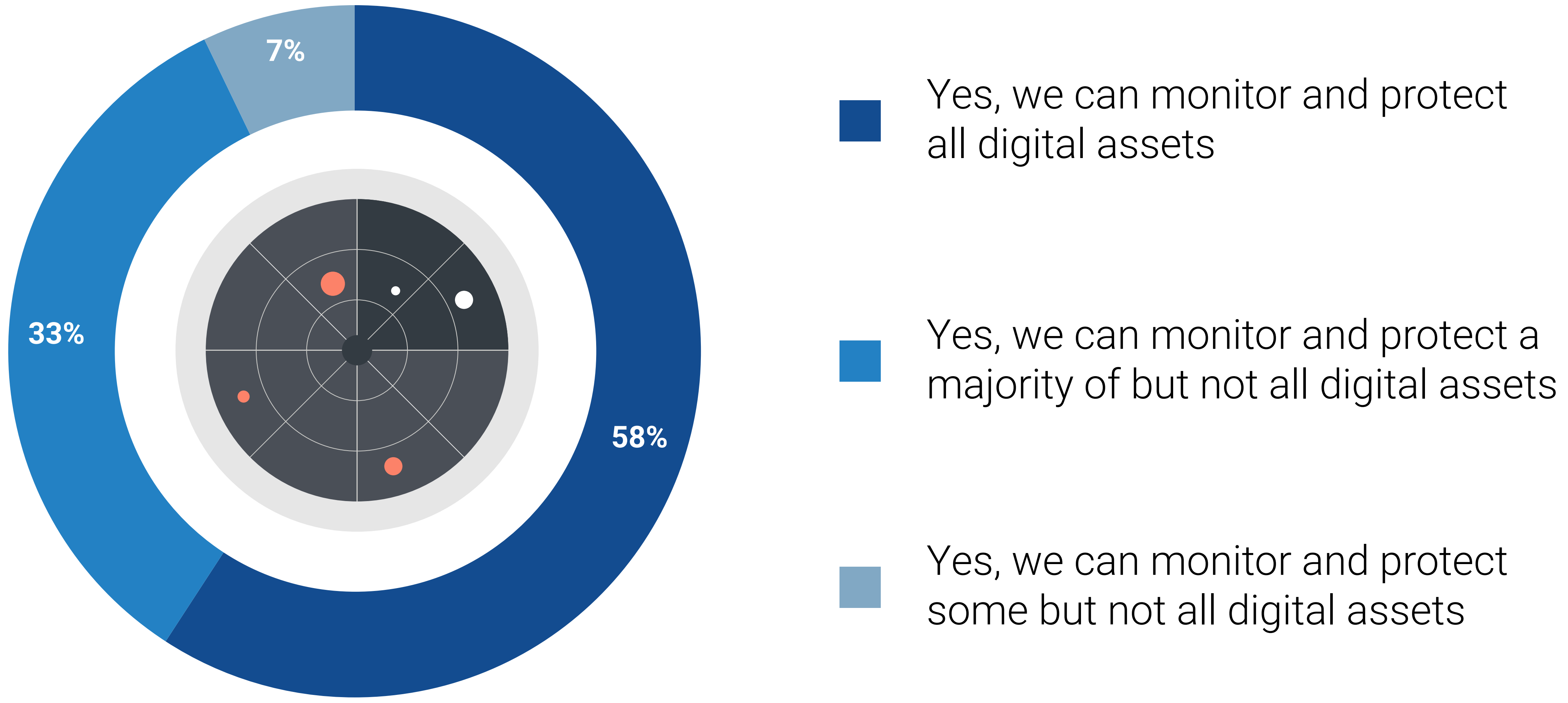
BACK TO CONTENTS

Digital Risk Protection (DRP) Is Becoming an Essential Part of CTI Programs

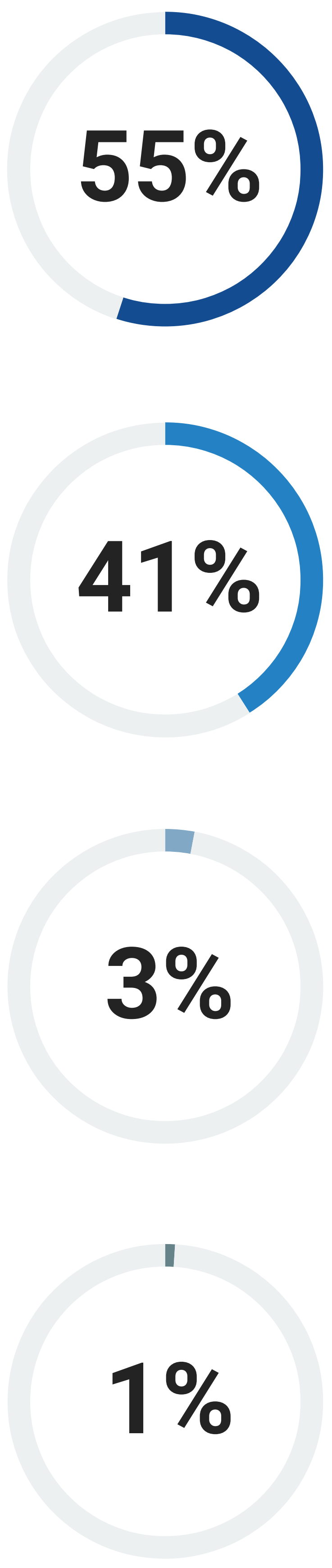
Scope of DRP Programs Is Typically Extensive and Well-aligned with Cyber-threat Intelligence

As mentioned previously, 38% of security professionals indicated that their organization’s CTI program was part of a broader effort around digital risk protection (DRP). Indeed, the majority of organizations have a DRP program in place today, and more than half (58%) believe they can monitor and protect all digital assets. In some cases, DRP and CTI programs are managed collectively with disparate data sources, tools, and intelligence feeds, while others use aggregate DRP and CTI with common data sources, tools, and intelligence feeds, which likely involves the help of a service provider of some kind.

Does your organization have a digital risk protection (DRP) program in place?



How DRP and cyber-threat intelligence programs align.



55% Programs are managed by one organization with dedicated data sources and tools for DRP and others for cyber-threat intelligence

41% Programs are managed by one organization with common data sources and tools

3% Programs are managed by different organizations with dedicated data sources and tools for DRP and others for cyber-threat intelligence

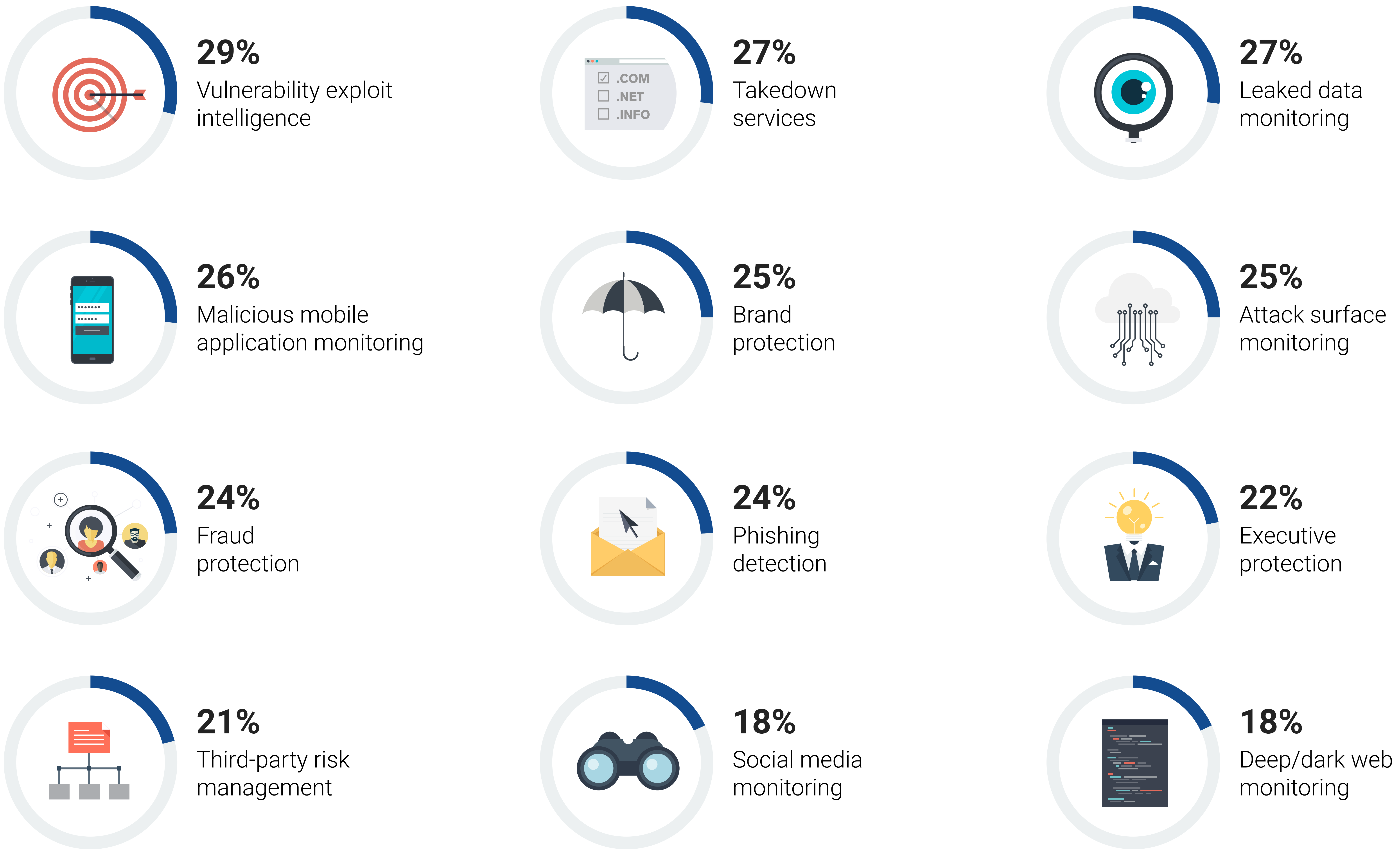
1% Programs are managed by different organizations with common data sources and tools

Many Important DRP Functions Indicates Its Growing Importance

Organizations should understand that digital risk protection coverage will add many dimensions to their already broad CTI programs. Important DRP functions are wide ranging, including vulnerability exploit intelligence, takedown services, leaked data monitoring, malicious mobile application monitoring, and brand protection. Even attack surface discovery and monitoring, once considered a standalone function, is merging into DRP services. DRP extends even further into areas like fraud protection, phishing detection, executive protection, and third-party risk management.

A comprehensive DRP program will likely discover assets and exposures well beyond those that security and IT operations teams are tracking today. Organizations should approach DRP with a process mindset. Beyond digital risk discovery, security teams must be prepared to prioritize risks based on their potential for business disruption. Additionally, intelligence teams must integrate DRP into their intelligence lifecycle phases.

Most important DRP functions.



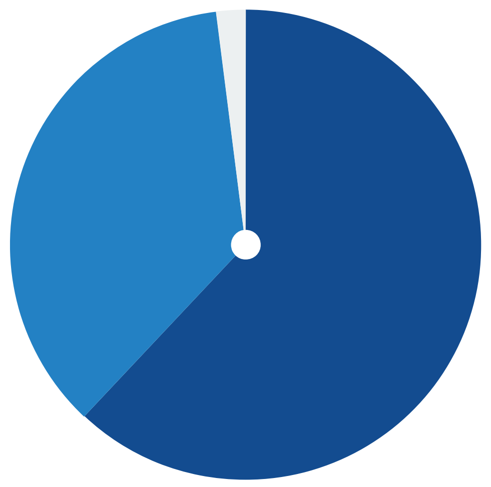
BACK TO CONTENTS

The MITRE ATT&CK Framework Is Mainstream and a CTI Program Driver

Mainstream Use and Operationalization of the MITRE ATT&CK Framework

MITRE ATT&CK has become the "lingua franca" of security operations, including CTI programs. An overwhelming majority (97%) of organizations already use MITRE ATT&CK extensively or on a limited basis. Of those using MITRE ATT&CK, 62% have operationalized MITRE ATT&CK extensively while another 38% have done so on a limited basis.

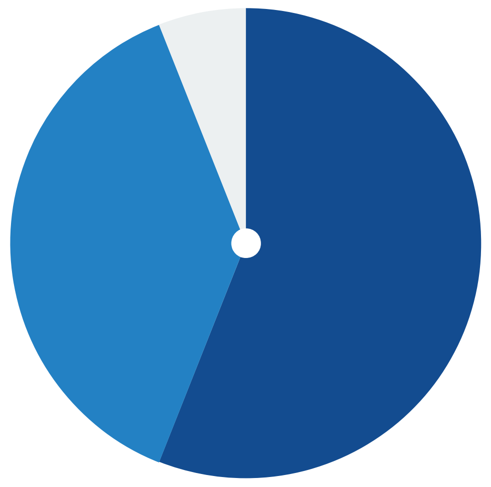
The MITRE ATT&CK framework can enhance the value of cyber-threat intelligence. Organizations use MITRE ATT&CK for a wide range of CTI program actions like understanding adversary TTPs, assessing the quality and relevance of intelligence, enriching security alerts, and addressing threats to industrial control systems. MITRE ATT&CK with CTI programs gives organizations a way to interpret and contextualize cyber-threat intelligence that aligns with their security controls and technologies. It helps them understand the effectiveness of their security defenses and identify gaps. Combined with the cyber-threat intelligence lifecycle, MITRE ATT&CK can also help organizations gain tactical, operational, and strategic value from CTI programs. This alone will drive more investment in CTI alignment with MITRE ATT&CK over the next 12 to 24 months.



Does your organization **utilize** the MITRE ATT&CK framework for security operations?

■ **62%** Yes, extensively

■ **36%** Yes, on a limited basis

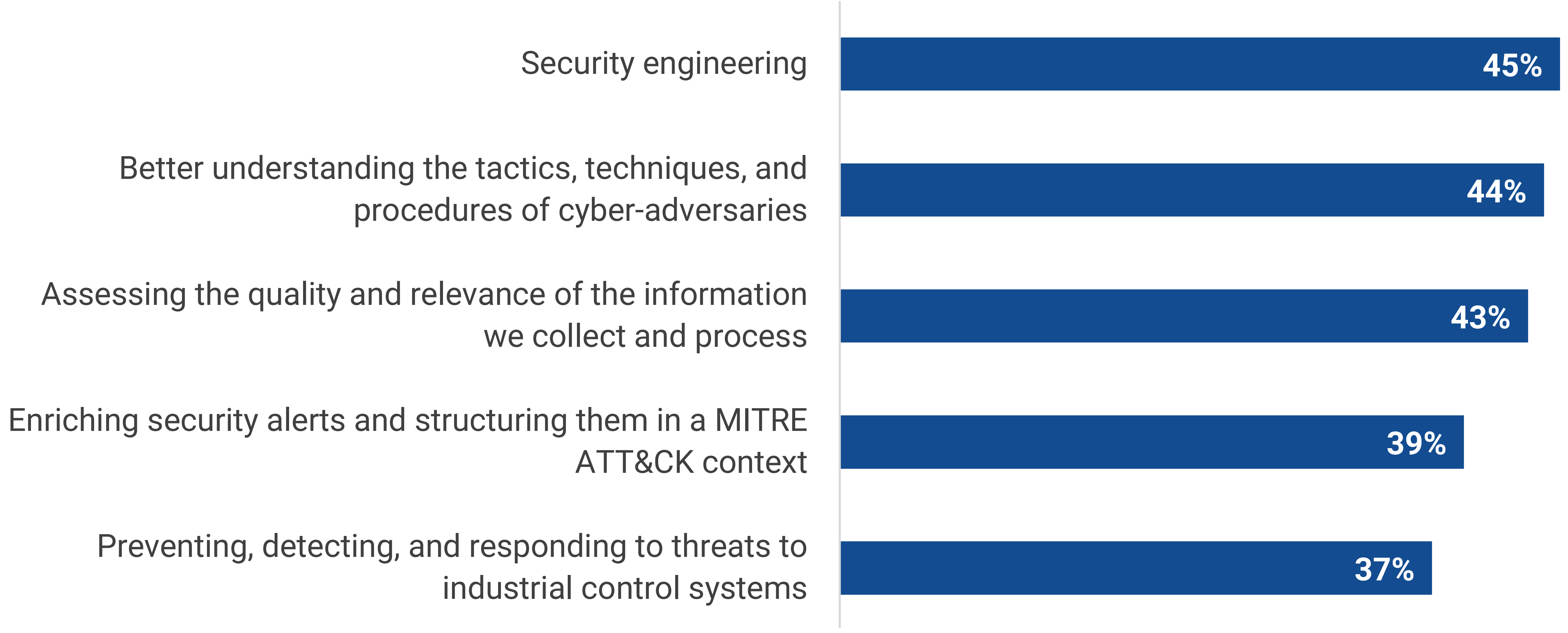


Has your organization **operationalized** its usage of the MITRE ATT&CK framework?

■ **56%** Yes, extensively

■ **38%** Yes, on a limited basis

Top 5 areas in which the MITRE ATT&CK framework supports cyber-threat intelligence programs.

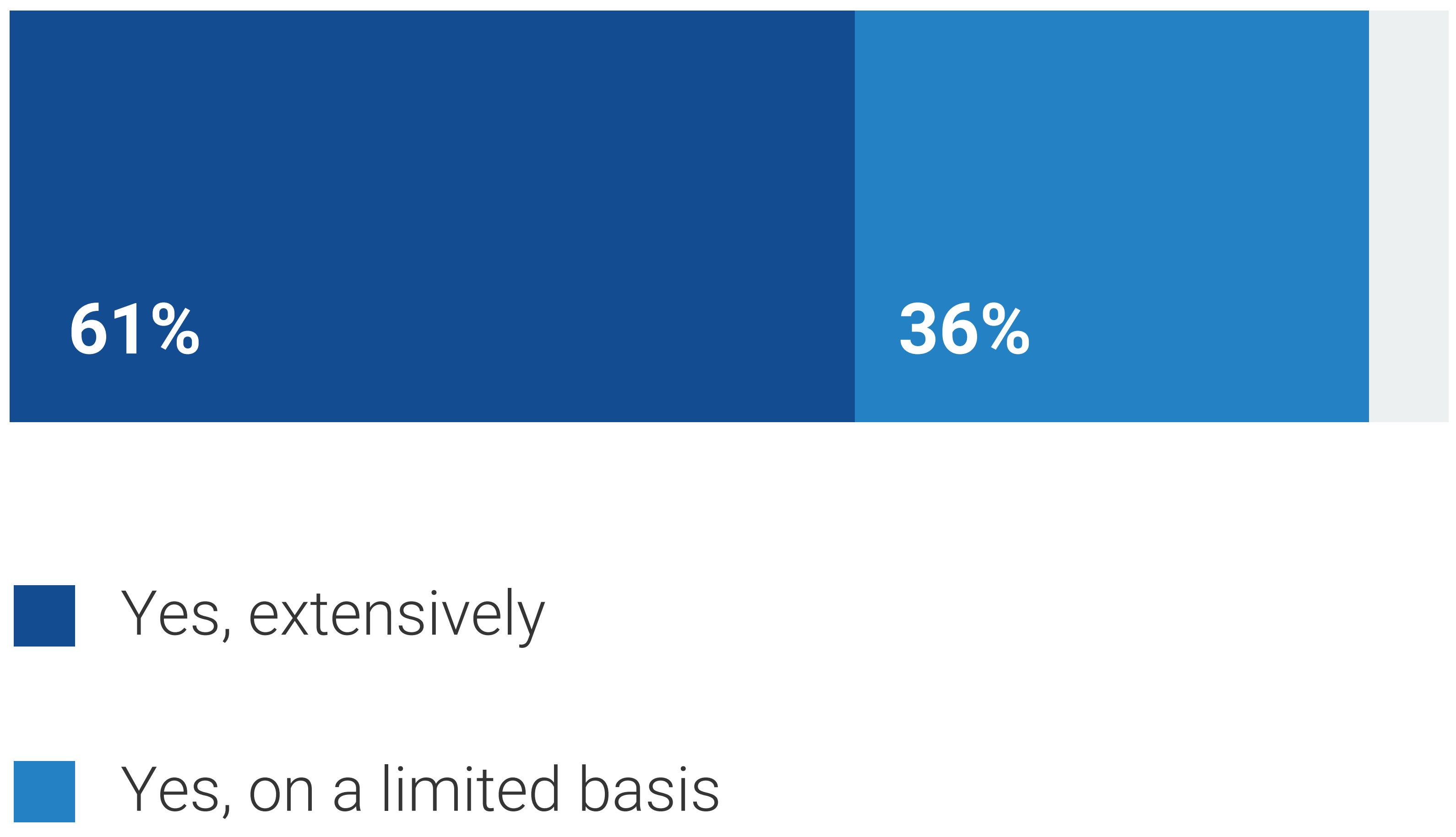


CTI Programs Require Managed Services

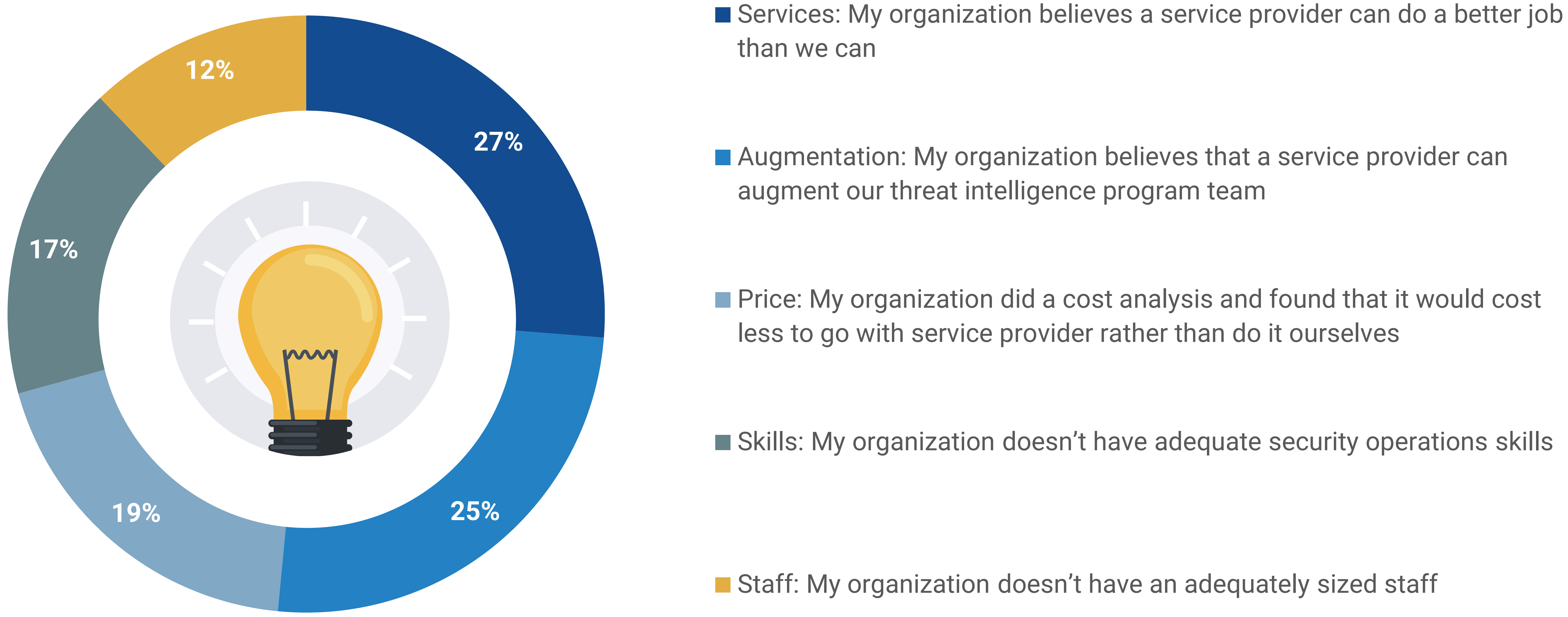
Primary Reasons for Using Managed CTI Services

Since cyber-threat intelligence requires advanced and esoteric skills, many organizations can't recruit, hire, train, and retain an adequate number of specialists. Therefore, CISOs often look to cyber-threat intelligence service providers to bridge this gap. In fact, 97% of organizations use managed services for their CTI programs. Managed service providers are employed because they can support a CTI program better than the security staff, to augment an existing cyber-threat intelligence program, or because organizations believe that service providers can deliver a cyber-threat intelligence program at a lower cost than they can achieve on their own.

Does your organization use managed services for its threat intelligence program?

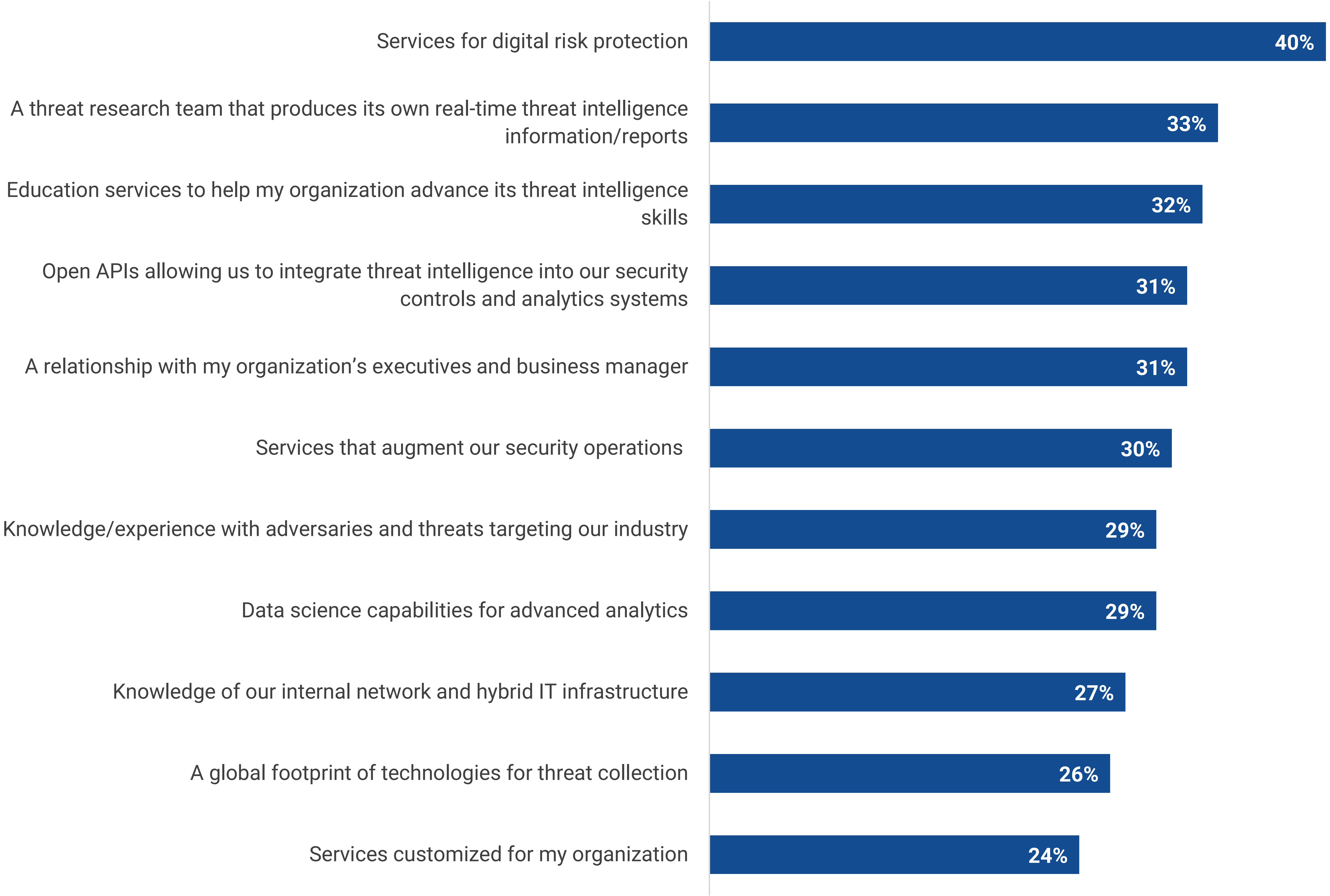


Primary reason behind usage of or plans for managed cyber-threat intelligence services.



BACK TO CONTENTS

Most important attributes for MSPs focused on cyber-threat intelligence.



Important CTI MSP Attributes include DRP Services, Threat Research Skills, and CTI Program Education

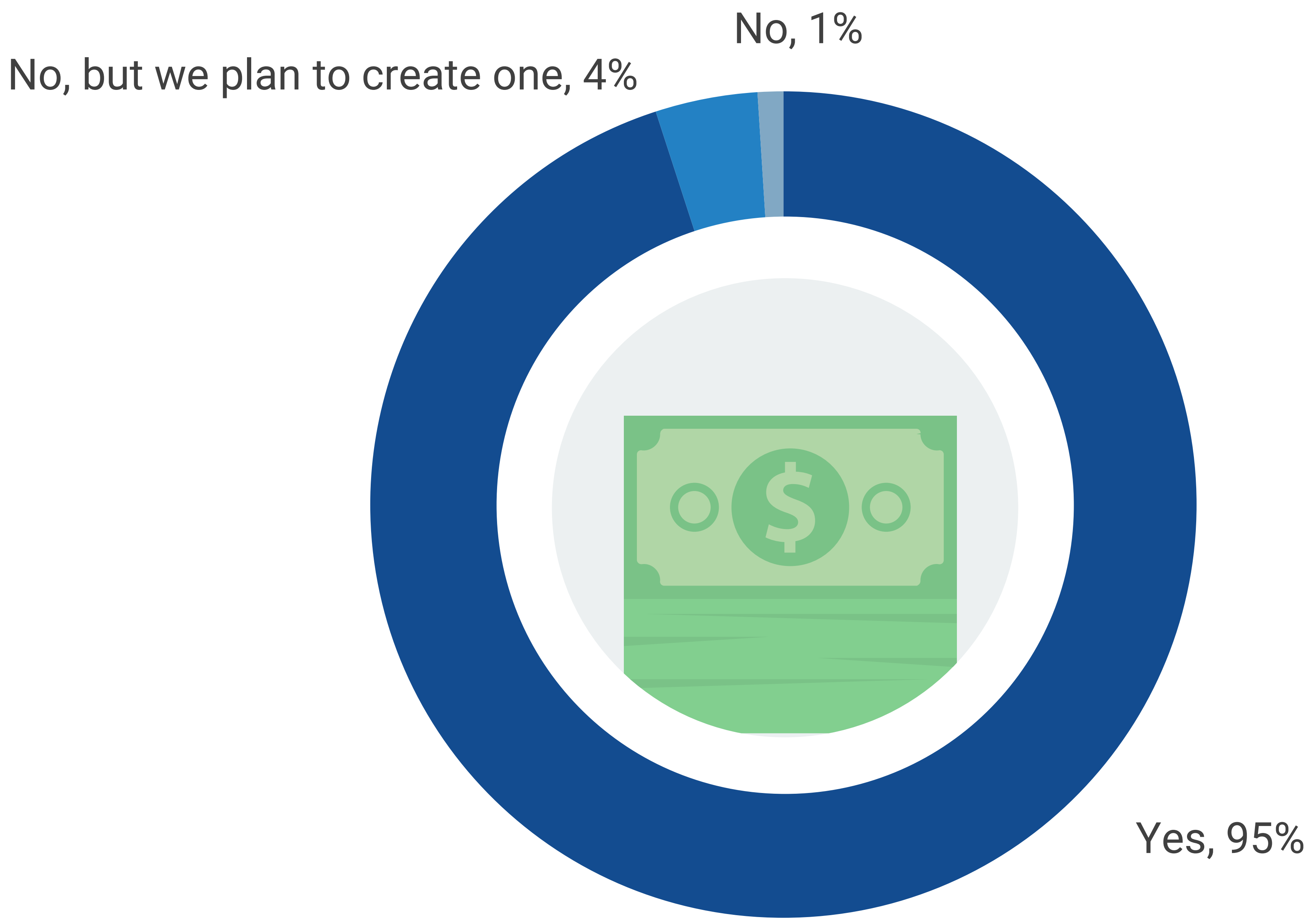
When shopping for CTI program managed services, organizations emphasize the need for providers with digital risk protection services, a threat research team, education services, and open APIs for cyber-threat intelligence integration. This suggests that organizations desire a complete menu of services that can help them throughout the intelligence lifecycle. DRP services that identify exposures can be used in the planning and direction phase to determine priority intelligence requirements. Open APIs can bolster data collection and processing. Threat research teams can help organizations analyze cyber-threat intelligence, and education services can help them train staff and develop more formal and documented CTI program processes.

CTI Investments Are Planned

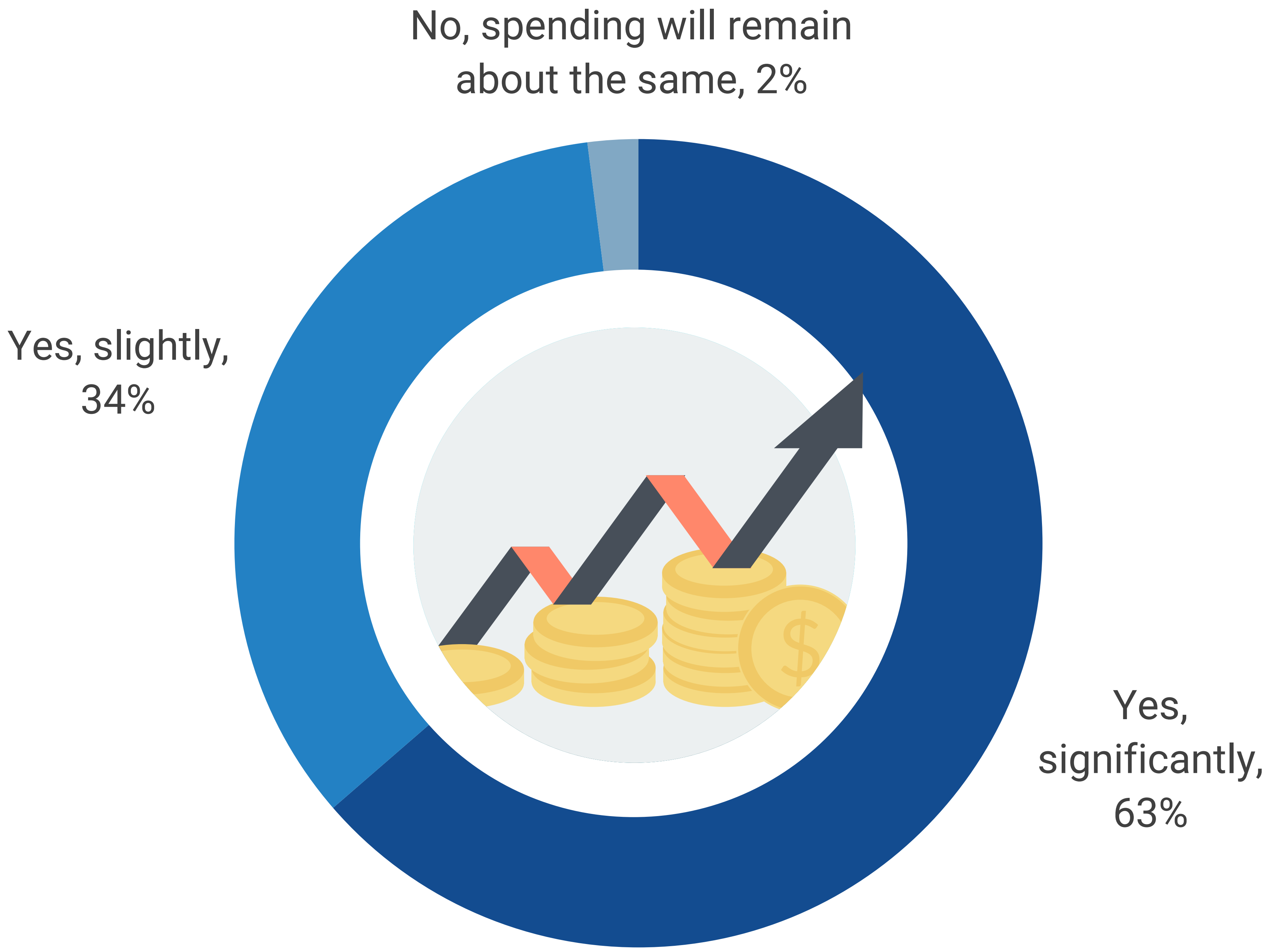
Dedicated and Increasing CTI Budget Should Ease Purchasing Friction

Nearly all organizations (95%) have a dedicated budget for cyber-threat intelligence programs. Despite potential economic headwinds, almost two-thirds (63%) expect their CTI program budget to grow extensively in the next 12-18 months, while another 38% claim their CTI program budget will grow to some extent during the same timeframe.

Do organizations have dedicated budgets for CTI programs?



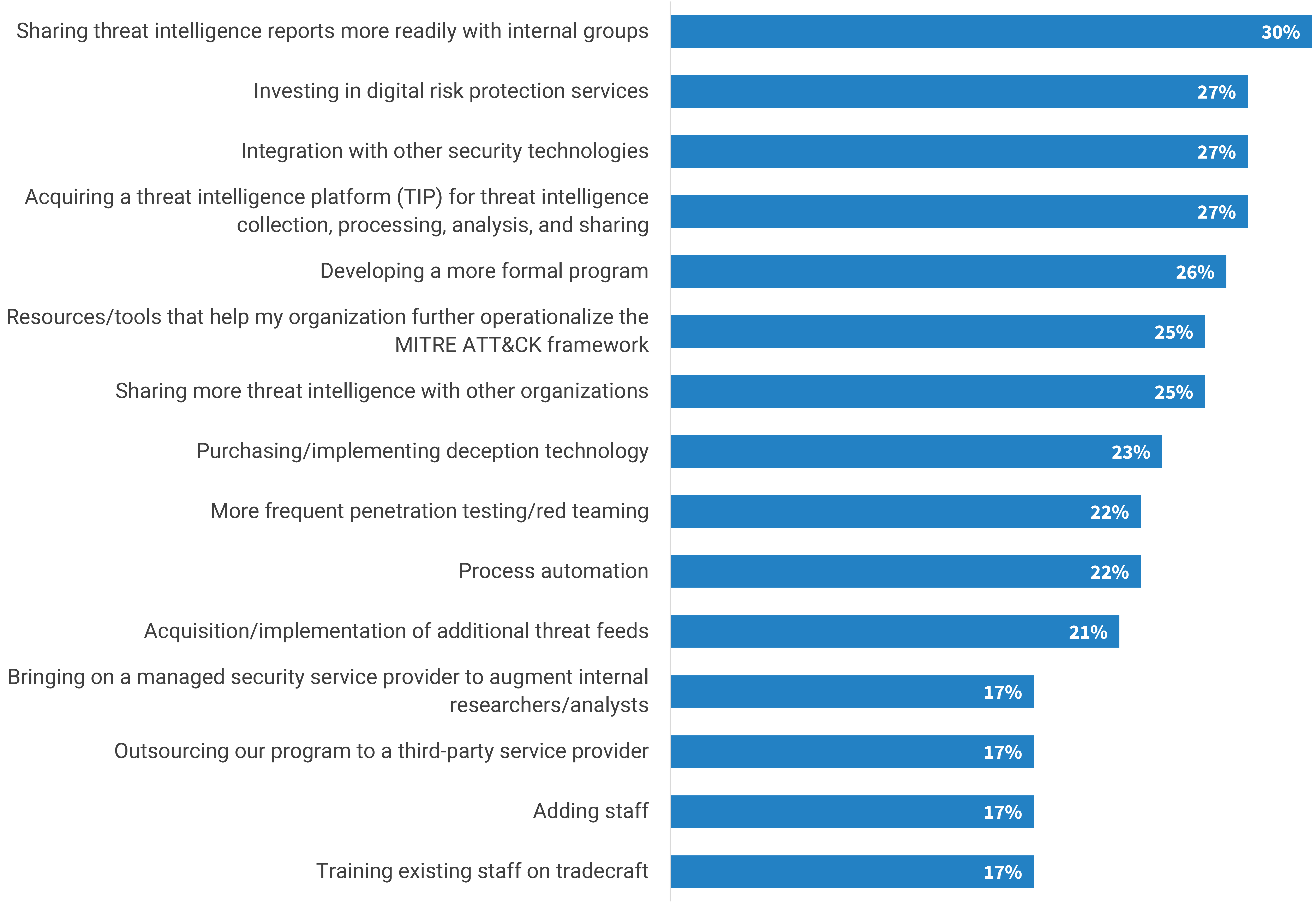
Will CTI program spending increase over the next 12-18 months?



CTI Priorities Include Desires for More Operational and Strategic Use

In terms of the future, security professionals say their organizations will prioritize sharing cyber-threat intelligence reports across their organizations, investing in DRP services, integrating CTI with more security technologies, and acquiring a commercial threat intelligence platform (TIP) to help them through the data collection, processing, and analysis phases of the cyber-threat intelligence lifecycle. It is also noteworthy that more than one-quarter (26%) of organizations prioritize the development of a more formal CTI program. This should include more upfront planning with various stakeholders, customizing cyber-threat intelligence reporting, and enlisting more feedback from CTI consumers. Since it's also likely that CTI programs will include managed services, CISOs must have third-party service management expertise in areas like negotiating contracts, managing relationships, developing SLAs, and determining division of labor.

Areas of CTI programs that will be prioritized over the next 12-18 months.



ANOMALI

Anomali is the leader in modernizing and scaling security operations, delivering breakthrough levels of security visibility and intelligence-driven threat detection and response. In a world filled with SIEM, SOAR, and XDR, the Anomali Platform amplifies visibility, integrating with existing security controls and enriching them with actionable context to stop adversaries. Anomali helps customers and partners transform their SOC platform by elevating security efficacy and reducing their costs with automated processes at the heart of everything. The solution is anchored in big-data management and boasts the world's largest repository of global intelligence that supports native-cloud, multi-cloud, on-premises, and hybrid deployments. Founded in 2013, Anomali serves global B2B enterprise businesses, large public sector organizations, ISACs, ISAOs, service providers, and Global 1000 customers to help safeguard the world's critical infrastructure, companies, and people. Leading venture firms, including Google Ventures, General Catalyst, and IVP, back Anomali.

Experience intelligence-driven threat detection and response with Anomali. Schedule a live demo and learn how Anomali can help you enhance your detection capabilities with the power of threat intelligence.

GET A CUSTOM DEMO

ABOUT ENTERPRISE STRATEGY GROUP

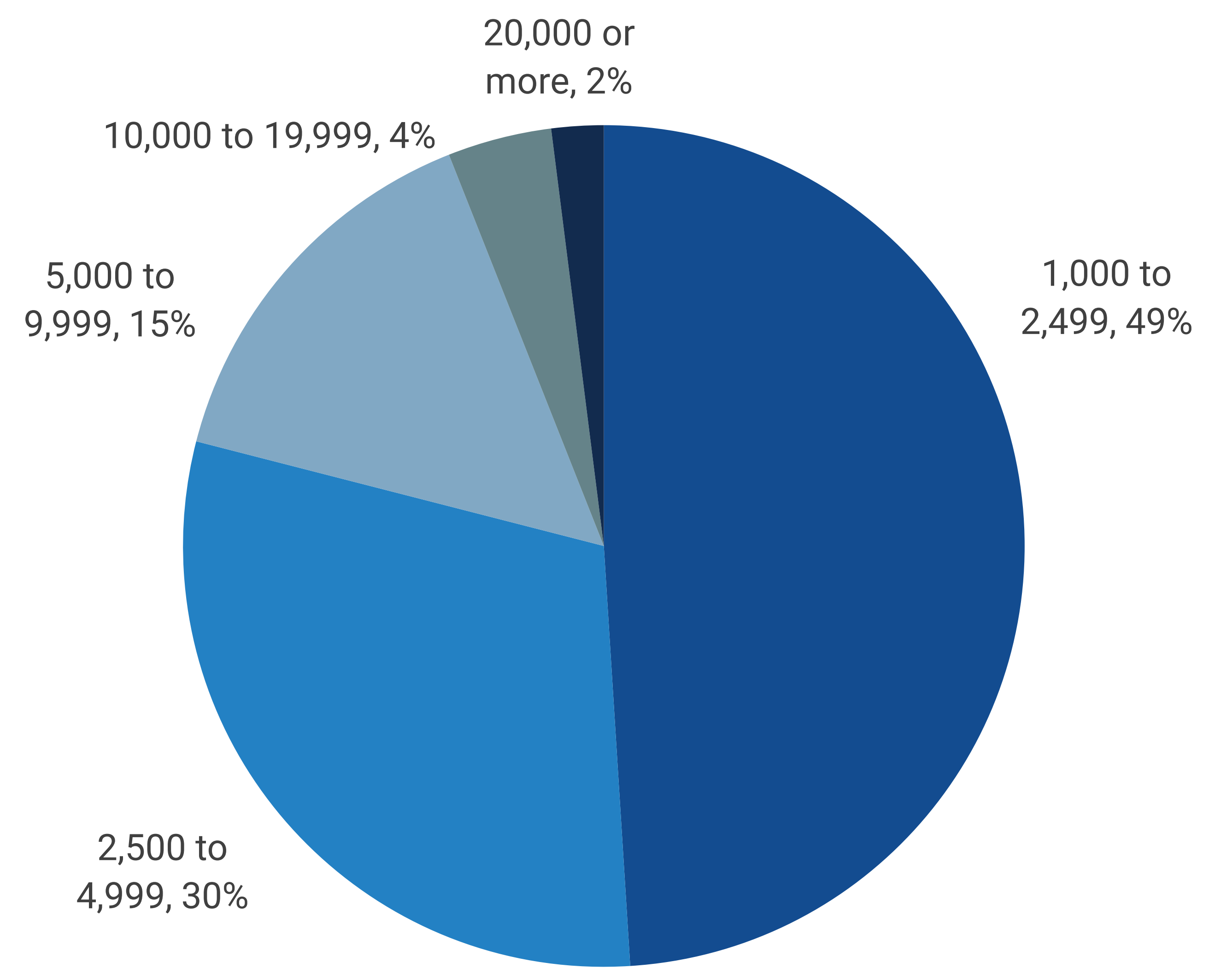
TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology and Demographics

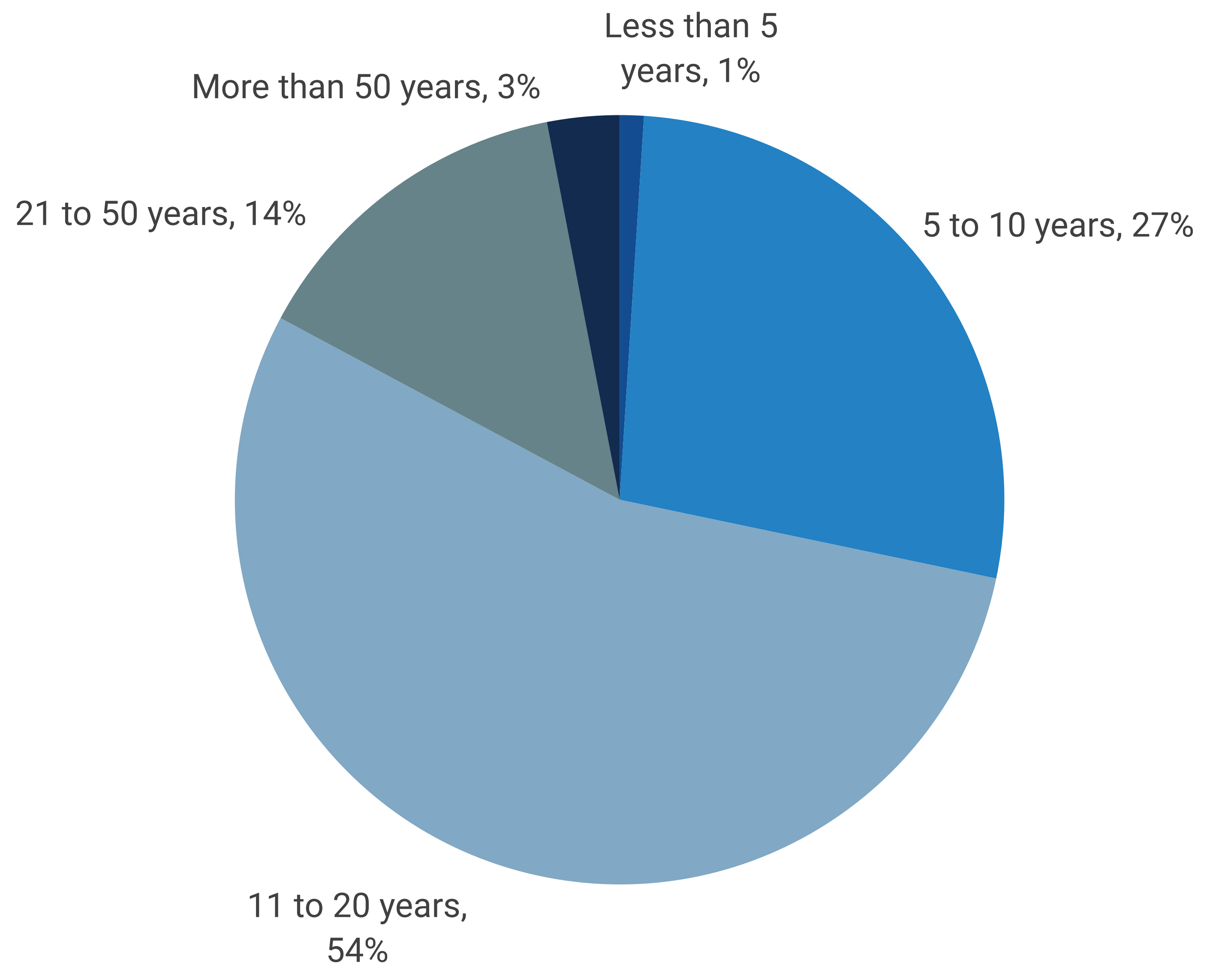
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of cybersecurity professionals from private- and public-sector organizations in North America between October 26, 2022 and November 6, 2022. To qualify for this survey, respondents were required to be cybersecurity professionals with knowledge of and participation in their organization's cyber-threat intelligence programs. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 380 cybersecurity professionals.

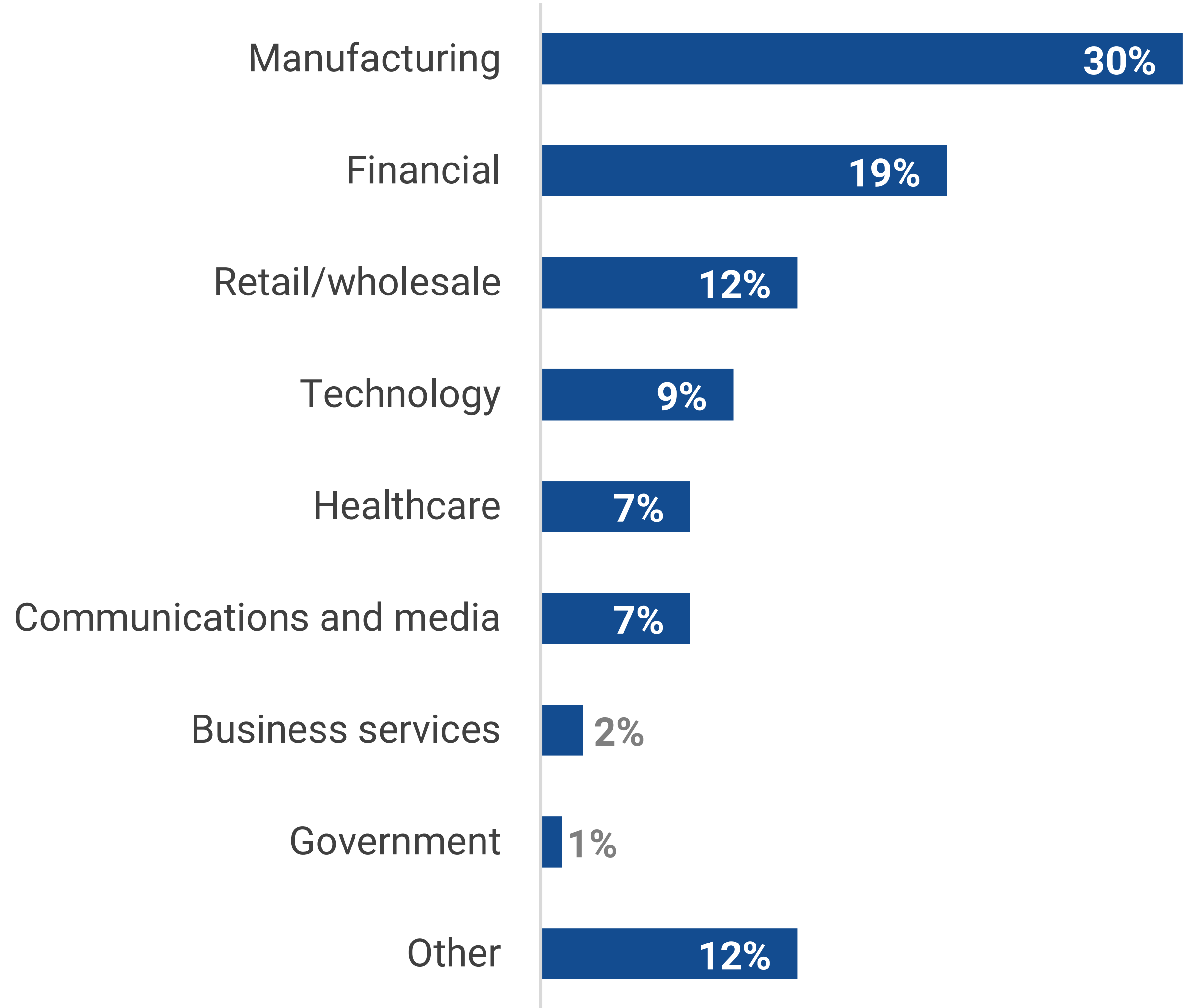
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Enterprise Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.