CYBEREDGE GROUP

2023 STATE OF THREAT INTELLIGENCE

A survey of cybersecurity managers and practitioners on how they are using threat intelligence, where they get it, and their plans to improve it

October 2023

A CYBEREDGE RESEARCH STUDY SPONSORED BY:

Recorded Future®

Table of Contents

Introduction

The 2023 State of Threat Intelligence report examines how and why most organizations have made the collection and analysis of threat intelligence a central element of their cybersecurity programs – and extended its use cases beyond traditional cybersecurity activities.

In August 2023, we surveyed 400 cybersecurity managers and practitioners from a range of countries and industries with knowledge about their organization's use of threat intelligence. We asked about important use cases and benefits, sources, and plans for improving threat intelligence in the future. We inquired about organizational issues, such as the level of maturity of their threat intelligence efforts and whether they have dedicated threat intelligence organizations. We also requested information on their criteria for selecting threat intelligence vendors.

Our objective is to provide CIOs, CISOs, cybersecurity managers, and others with information on how their peers are utilizing threat intelligence and areas they are seeking to improve.

CyberEdge would like to thank our research sponsor, Recorded Future, who conceived this report and whose support has been essential to its success.

Top Five Insights

This report contains dozens of actionable insights on the state of threat intelligence. Here are our top five takeaways:

1. **Use cases and benefits have expanded.** Today, most organizations are leveraging threat intelligence for as many as 10 use cases. Although threat intelligence programs grew up as resources for a few core cybersecurity tasks, such as strengthening existing security tools, triaging alerts, incident response, and vulnerability management, they have expanded their reach. In addition to core operational cybersecurity tasks, intelligence is also playing an important role in risk assessment and cybersecurity program management, and in supporting the activities of marketing, physical security, third-party risk management, and fraud prevention teams.

Survey Demographics

- **Responses received from 400 qualified cybersecurity managers and practitioners**
- **All from organizations with more than 1,000 employees**
- **Representing 7 countries across North America, Europe, and Asia Pacific**
- **Representing 8 major industries and several others**

2. **Comprehensive sources of threat intelligence are the way to go.** More than 90% of organizations currently obtain threat intelligence from at least five sources. These include their own staff, free and paid threat data feeds, and security tools on their networks. They also rely on threat intelligence vendors that collect data from multiple sources (including the dark web), generate automatic alerts, and provide in-depth threat analysis.

3. **Vendors supply specialized skills and knowledge.** Most organizations work with threat intelligence vendors primarily to leverage their specialized skills and knowledge. That includes knowledge about adversaries and their tactics, techniques, and procedures (TTPs), about discussions and activities on the dark web, and about threats targeting specific industries, applications, and systems. The organizations also value the ability of vendors to provide up-to-date intelligence delivered in real time and to integrate threat feeds with existing cybersecurity workflows.

4. **Dedicated, mature, threat intelligence teams.** Today, threat intelligence programs are on a very solid footing. A strong 71% of organizations have a dedicated threat intelligence team, and 87% of them consider their threat intelligence activities to be at an "intermediate" or "advanced" maturity level. Moreover, an overwhelming 98% of the survey respondents agree that comprehensive threat intelligence is essential for their cybersecurity programs.

Introduction

5. **Enhancements planned.** Emerging threats and the expanding number of use cases are giving enterprises plenty of reasons to enhance and improve their threat intelligence capabilities. Goals include more, better, faster data gathering, using intelligence for risk analysis and cybersecurity program management, and helping outside of traditional cybersecurity areas, such as brand protection and third-party risk management.

About This Report

The findings of this report are divided into three sections:

Section 1: Threat Intelligence Use Cases and Benefits

What are organizations using threat intelligence for? This section of the report looks at the incidence of 10 use cases, ranging from increasing the accuracy of existing security tools, to guiding cybersecurity planning and investments, to reducing online fraud. It also quantifies interest in specific operational benefits related to the activities of SOCs, incident response, vulnerability management and other cybersecurity teams, and in specific strategic benefits related to managing security programs and communicating with executive management.

Section 2: Threat Intelligence Sources and Vendors

In theory, organizations can gather and analyze threat intelligence using their own resources. In practice, this is extremely rare. This section of the report examines why. It reviews what sources most organizations leverage and why they are working with threat intelligence vendors. It also provides insights into what characteristics organizations are looking for when selecting threat intelligence vendors.

Section 3: Threat Intelligence Organizations and Plans

How are organizations organizing and supporting their threat intelligence activities, and what are they planning for the future? This section of the report examines where people working on threat intelligence are located in the cybersecurity group and where survey respondents place their organization on a maturity scale for threat intelligence activities. It also reviews plans for working with threat intelligence vendors and priorities for improving intelligence activities.

Navigating This Report

We encourage you to read this report from cover to cover so you can catch all of the useful details. However, if you are seeking out specific topics of interest, there are three other ways to navigate through the report:

- **Table of Contents.** Each item in the Table of Contents pertains to specific survey questions. Click on any item to jump to its corresponding page.
- **Research Highlights.** The Research Highlights page showcases the most significant headlines of the report. Page numbers are referenced with each highlight so you can quickly learn more.
- **Navigation tabs.** The tabs at the top of each page are clickable, enabling you to conveniently jump to different sections of the report.

Research Highlights

Threat Intelligence Use Cases and Benefits

- **Use cases.** Organizations are now leveraging threat intelligence for as many as 10 different use cases. Intelligence is not only a force multiplier for cybersecurity teams, it also provides value for marketing, physical security, third-party risk management, and fraud prevention groups, among others (page 6).
- **Operational benefits.** Top operational benefits include improving the accuracy of threat detection and prevention tools, identifying more malware types and malicious URLs, describing threat actors and their TTPs, and improving threat hunting (page 8).
- **Strategic benefits.** Important strategic benefits start with improving the ability to justify cybersecurity investments, anticipating attacks that could threaten new technology and business initiatives, and enhancing visibility into emerging threats (page 10).
- **Importance for cybersecurity.** An overwhelming majority of survey respondents either somewhat agree (14%) or strongly agree (85%) with the statement "comprehensive threat intelligence is essential for an effective cybersecurity program" (page 11).

Threat Intelligence Sources and Vendors

- **Sources.** More than 90% of the enterprises surveyed obtain threat intelligence from at least five sources. The primary ones include research by their own staffs, security tools vendors, threat intelligence solutions vendors, and paid threat feeds (page 12).
- **Reasons for working with vendors.** Organizations work with threat intelligence vendors to have access to specialized skills, to enable integration with existing security tools and workflows, and for information about adversary TTPs, among other reasons (page 13).
- **Criteria for selecting vendors.** Organizations are looking for threat intelligence vendors that can support many security teams, provide up-to-date intelligence in real time, and provide excellent customer support. Cost is *not* one of the top criteria (page 15).

Threat Intelligence Organizations and Plans

- **Threat intelligence organizations.** Of the organizations surveyed, 71% have a dedicated threat intelligence team. Another 19% have people on existing security teams who work full time collecting and analyzing intelligence (page 17).
- **Maturity of programs.** A solid 46% of organizations consider their threat intelligence programs to be at an "intermediate" maturity level. Another 41% describe themselves as "advanced." Only 13% put themselves at "beginner" or "basic" levels (page 18).
- **Adequacy of investment.** A full 92% of survey respondents either somewhat agree or strongly agree with the statement "my organization is making an adequate investment in threat intelligence" (page 19).
- **Plans for working with vendors.** A full 44% of organizations plan to continue working with about the same number of threat intelligence vendors they have now. About 17% are consolidating, while 28% plan to work with more (page 20).
- **Plans to improve threat intelligence.** Organizations plan to improve and expand their use of threat intelligence in several ways. Top priorities include using intelligence to enhance risk analysis, combining external and internal threat data to gain more insights, integrating threat intelligence with additional cybersecurity workflows, and using threat intelligence to improve communication with leadership and board members (page 21).

Threat Intelligence Use Cases

How does your organization leverage threat intelligence?

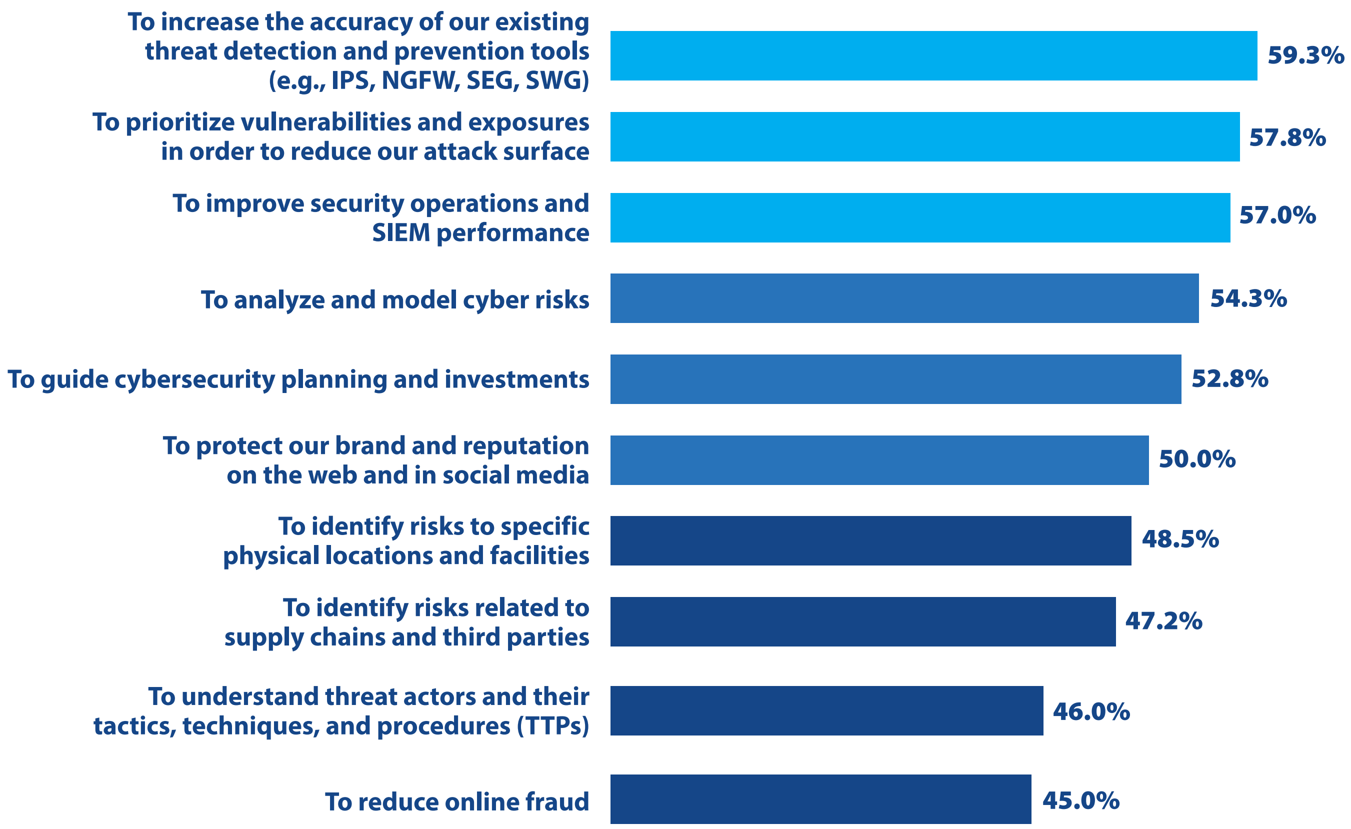

Figure 1: Most important use cases for threat intelligence.

A few years ago, most cybersecurity groups looked at threat intelligence primarily as a resource for detecting attacks and prioritizing vulnerabilities. Our survey data shows that organizations are now leveraging threat intelligence for as many as 10 different use cases, several of them providing value to groups outside of cybersecurity (see Figure 1).

The most popular use case, cited by 59.3% of respondents, is increasing the accuracy of existing security tools such as firewalls, intrusion prevention systems (IPS), secure email and secure web gateways (SEGs and SWGs), and antimalware solutions. This involves primarily automated data feeds that provide malware signatures, suspicious URLs, domains, and IP addresses, and other indicators of attack (IoA) and indicators of compromise (IoC) so security tools can filter out harmful content and block communication with adversaries. Threat intelligence is effectively a force multiplier for existing security investments, enabling them to perform their functions more effectively and reliably.

Section 1: Threat Intelligence Use Cases and Benefits

> **"Our survey data shows that organizations are now leveraging threat intelligence for as many as 10 different use cases, several of them providing value to groups outside of cybersecurity."**

Very close behind are two core operational uses: prioritizing vulnerabilities and exposures (57.8% of organizations) and improving the performance of security operations centers (SOCs) and security information and event management (SIEM) systems (57.0%).

Notably, threat intelligence is also being used by security leaders for program management and strategic planning. More than half of all organizations are using intelligence to help analyze and model cyber risks and to guide cybersecurity planning and investment (54.3% and 52.8%, respectively).

As new types of threats have emerged, groups outside of cybersecurity have found ways to leverage threat intelligence. This includes marketing groups using intelligence to protect brands and reputations on the web and social media (50.0% of organizations), physical and geopolitical security groups identifying risks to physical locations and facilities (48.5%), supply chain and third-party risk management teams monitoring third party risks (47.2%), and fraud prevention teams trying to reduce fraud (45.0%).

Operational Benefits

Which of the following operational benefits from threat intelligence are the most significant for your organization? (Select up to five.)

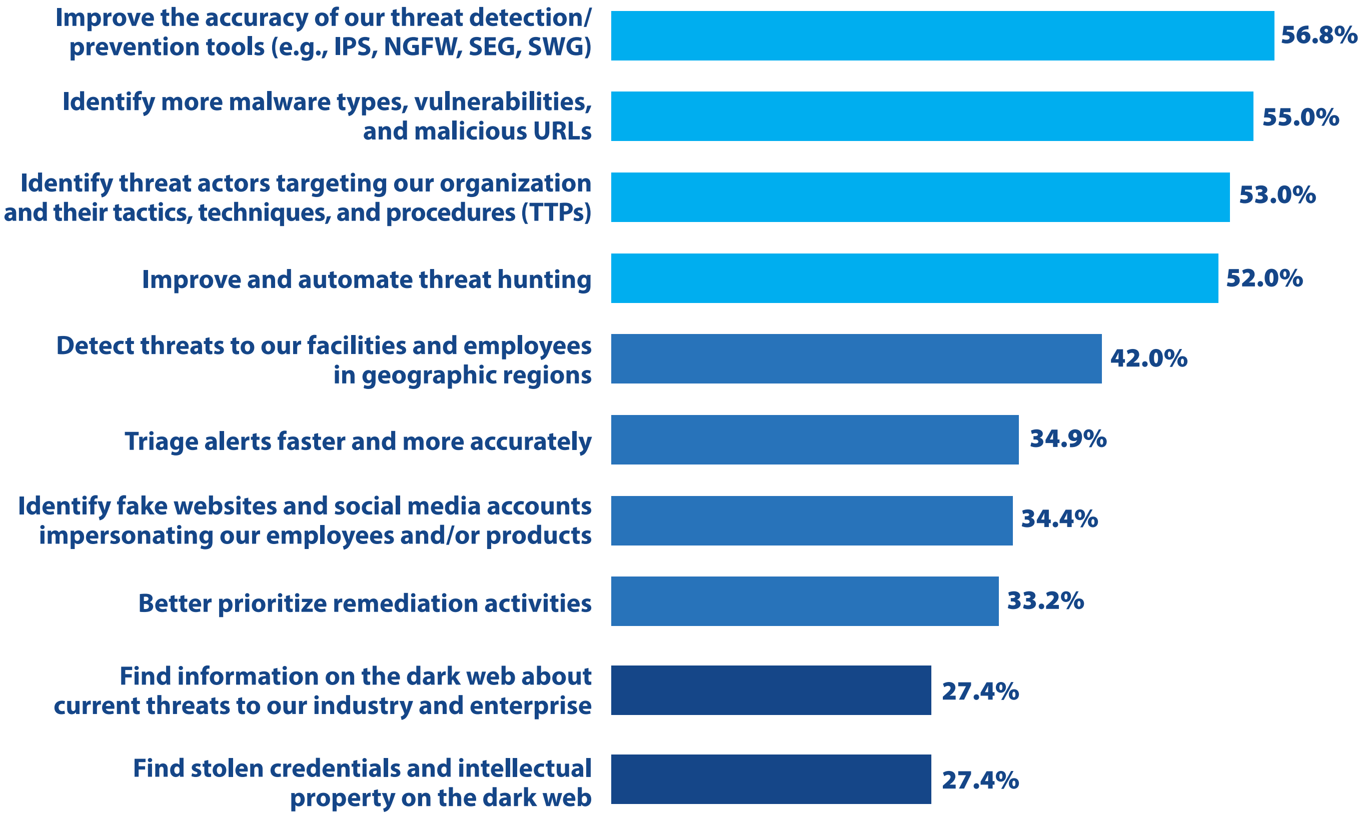

Figure 2: Operational benefits of threat intelligence.

We asked respondents to select up to five operational benefits that are most significant for their organization. Strategic benefits are covered in the next question.

The operational benefits cited most often are improving the accuracy of threat detection and prevention tools (selected by 56.8% of respondents) and identifying more malware types, vulnerabilities, and malicious URLs (55.0%) (see Figure 2). Today, comprehensive, timely intelligence is critical because adversaries are continuously launching attacks from new domains, creating new botnets, and tweaking malware files.

Section 1: Threat Intelligence Use Cases and Benefits

Identifying relevant threat actors and their tactics, techniques and procedures (TTPs) comes third on this list, at 53.0%. Information on TTPs is used by cybersecurity teams to speed up incident response, provide hypotheses for threat hunting, prioritize remediation of vulnerabilities, and align investments with threats.

Improving and automating threat hunting was selected as a top priority by 52.0% of organizations. It was the #1 operational benefit in the government and retail sectors. Threat hunters create hypotheses about likely attacks based on the TTPs of known attackers, then hunt for IoCs associated with them.

Detecting threats to facilities and employees in geographic locations was highlighted by 42.0% of respondents. Public and dark web sources can reveal threats against assets in far-flung locations that might otherwise evade physical security teams and local managements.

The next tier of operational benefits consists of triaging alerts faster and more accurately, identifying fake websites and social media accounts, and better prioritizing remediation activities. Each was selected by about one-third of the respondents.

Monitoring the dark web to find information about current threats and stolen credentials and intellectual property were chosen by just over a quarter of the respondents. This is consistent with other evidence in the survey showing that, while some organizations value monitoring the dark web, most aren't doing it yet.

Strategic Benefits

Which of the following operational benefits from threat intelligence are the most significant for your organization? (Select up to three.)

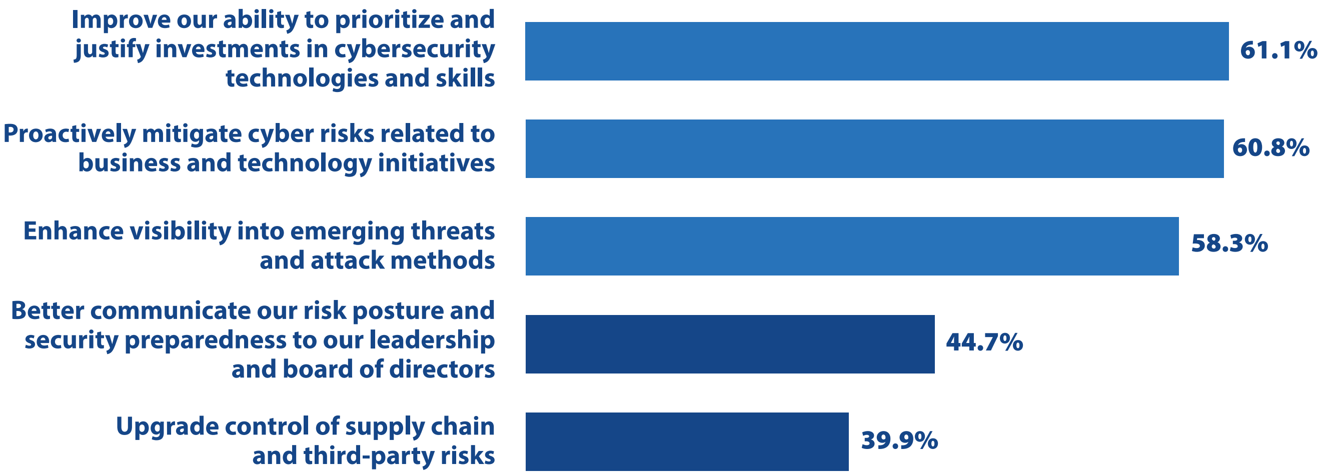

Figure 3: Strategic benefits of threat intelligence.

What about intelligence that describes the broad threat landscape, charts trends in cybercrime and state-sponsored attacks, and highlights new threats on the horizon? We asked respondents to select the three most significant strategic benefits of threat intelligence for their organization.

A previous CyberEdge Group survey found that in 97% of organizations security leaders are engaging directly with their boards (see the CyberEdge Group 2023 Cyber Defense Report, page 48). Threat intelligence helps them present objective information about current and emerging threats to their organization and the associated risks.

For example, three of every five organizations (61.1%) are using threat intelligence to prioritize and justify cybersecurity investments (see Figure 3). It helps them determine which threats are most relevant so they can compare the potential impact with the costs of mitigation. A related finding is that 44.7% of organizations are using threat intelligence to better communicate their risk posture and security preparedness to corporate leadership and boards. However, this practice varies by geography; it's cited as a major benefit by at least half the respondents in the US, Australia, and Germany, but barely over a quarter in Japan and France.

Over 60% of organizations use threat intelligence to mitigate cyber risks related to business and technology initiatives. For example, a company preparing to deploy a new wireless technology might use intelligence to anticipate attacks against that technology, or one expanding into a new geographic market might prepare for threats targeting that region.

Another major benefit is visibility into emerging threats and attack methods (58.3%), which allows organizations to start early implementing the right defenses. It's the strategic benefit cited most often in three of the seven countries in the survey: France, the UK, and Germany.

Using threat intelligence to help manage supply chain and third-party risk is a relatively new use case, but it was cited by about 40% of respondents. This probably reflects the recent visibility of the SolarWinds breach and similar attacks that affected hundreds of organizations.

The Importance of Threat Intelligence for Cybersecurity

Select the option that best describes your agreement with the following statement: "Comprehensive threat intelligence is essential for an effective cybersecurity program."

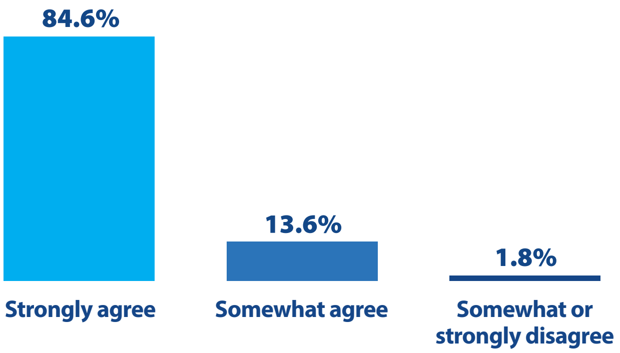

Figure 4: Agreement with the statement that comprehensive threat intelligence is essential for an effective cybersecurity program.

Do cybersecurity managers and practitioners think that excellent threat intelligence is a must-have today? They do – overwhelmingly. As shown in Figure 4, 84.6% of survey respondents strongly agree with that statement "comprehensive threat intelligence is essential for an effective cybersecurity program," and another 13.6% somewhat agree. There are very few doubters: a mere 1.8% of respondents somewhat or strongly disagree with that statement. In fact, as shown in Figure 5, the percentage of those who somewhat or strongly disagreed did not exceed 4% in any country surveyed.

> **"Do cybersecurity managers and practitioners think that excellent threat intelligence is a must-have today? They do – overwhelmingly."**

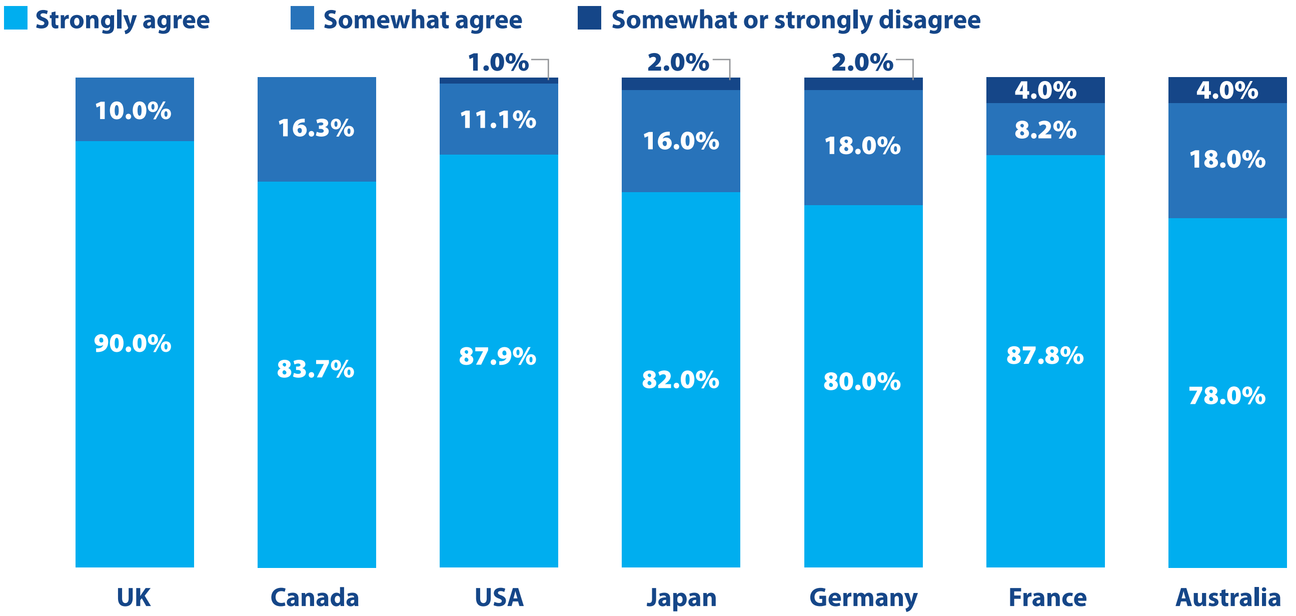

Figure 5: Agreement that comprehensive threat intelligence is essential for cybersecurity, by country.

Sources of Threat Intelligence

How often does your organization obtain threat intelligence from each of the following sources?

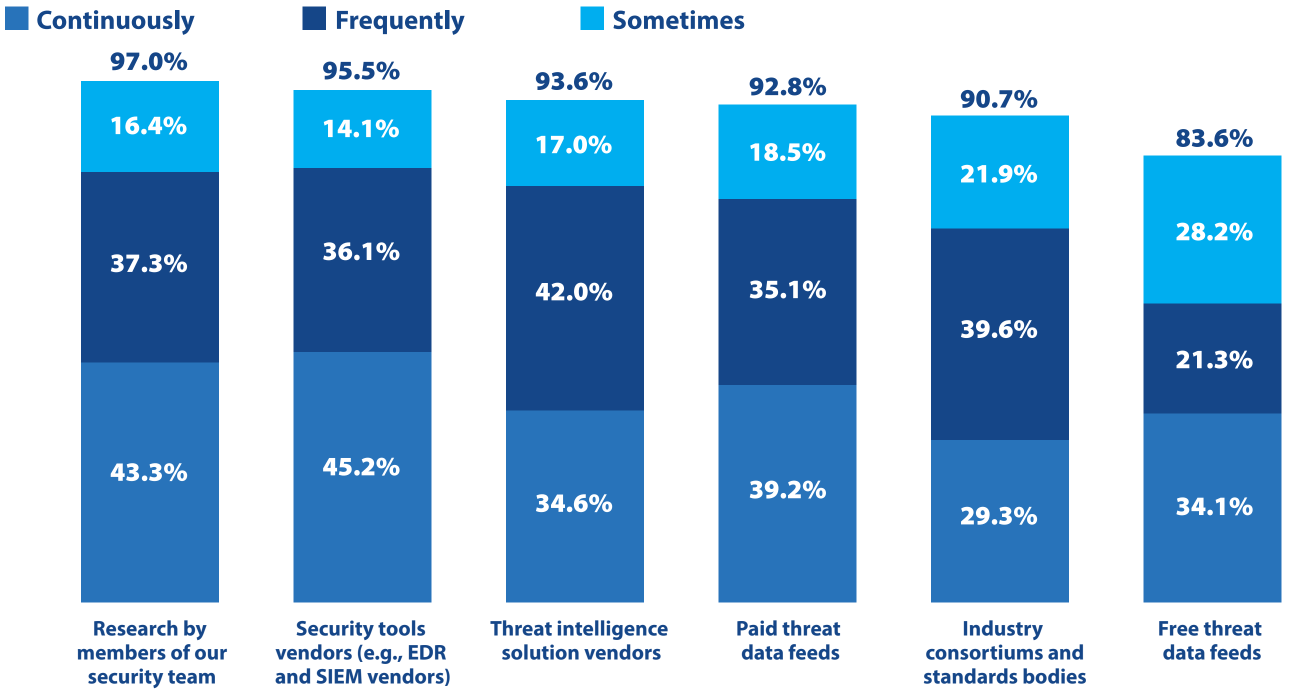

Figure 6: How often organizations obtain threat intelligence from sources.

Cybersecurity groups are acquiring comprehensive intelligence from multiple sources. More than 90% of the enterprises surveyed use at least five sources (see Figure 6). Two-thirds obtain intelligence "frequently" or "continuously" from those five (versus "rarely," "sometimes," or "never").

The biggest source is internal teams. Someone in the cybersecurity group performs threat research in all but 3% of organizations. Also pervasive: tracking IoAs and IoCs with internal security tools (95.5%) and working with threat intelligence solution vendors (93.6%). The latter were defined as "vendors collecting data from multiple sources, generating automated alerts and reports, and providing analysis."

Paid threat data feeds are also widely used (92.8%), and so are free ones, although not quite as often (83.6%). Finally, industry consortiums and standards bodies also play an important role, often providing industry-specific insights and peer advice not available from other sources.

Reasons for Working with Threat Intelligence Vendors

On a scale of 1 to 5, with 5 being highest, rate the importance of each of the following reasons for working with threat intelligence vendors.

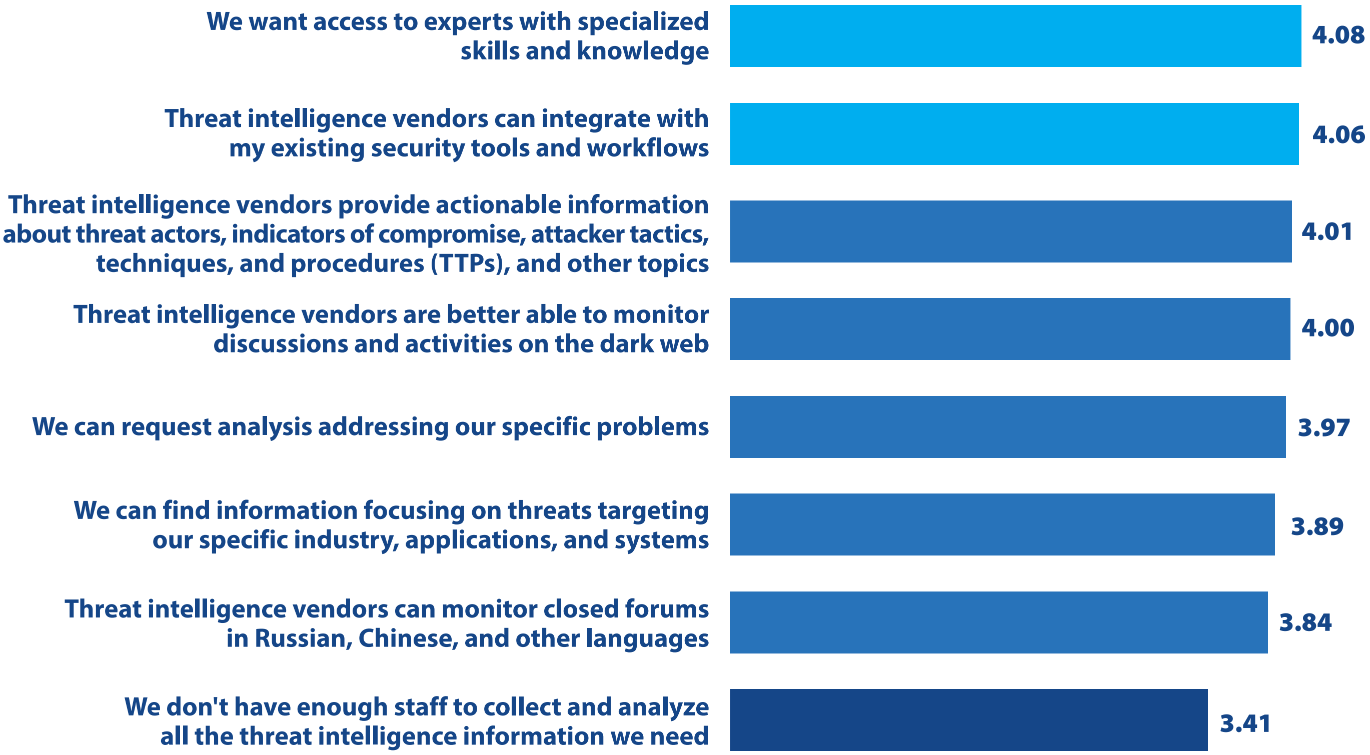

Figure 7: Reasons for working with threat intelligence vendors, on a scale of 1 to 5 with five highest.

Given that 97% of organizations have people doing threat research (see previous question), why use the services of threat intelligence vendors as well? Several reasons stand out.

A huge factor is the worldwide shortage of experts with the skills for acquiring and analyzing threat intelligence. Vendors provide access to those skills (see Figure 7).

Equally important is the fact that threat intelligence vendors have already integrated their output with a wide variety of security and analytics tools. The integration facilitates the orchestration and automation of security workflows, enabling organizations to detect and respond to attacks faster.

Also near the top of the list: Threat intelligence vendors provide actionable information about adversary TTPs, and also have the skills and experience to monitor discussions and activities on the dark web (many of which are conducted in "members only" forums, often in Russian or Chinese, that are difficult to crack).

Not all threats are risks to every organization. Threat intelligence vendors help organizations sort out which threats are relevant to their industry, applications, and technologies. They do this by automatically providing relevant contextual information about attacks, as well as offering custom inquiries, in-depth reports, and searchable intelligence databases with information specific to the organization's environment.

> **"Not all threats are risks to every organization. Threat intelligence vendors help organizations sort out which threats are relevant to their specific industry, applications, and technologies."**

Criteria for Selecting Threat Intelligence Vendors

Which of the following characteristics are most important when selecting a threat intelligence vendor? (Select up to five.)

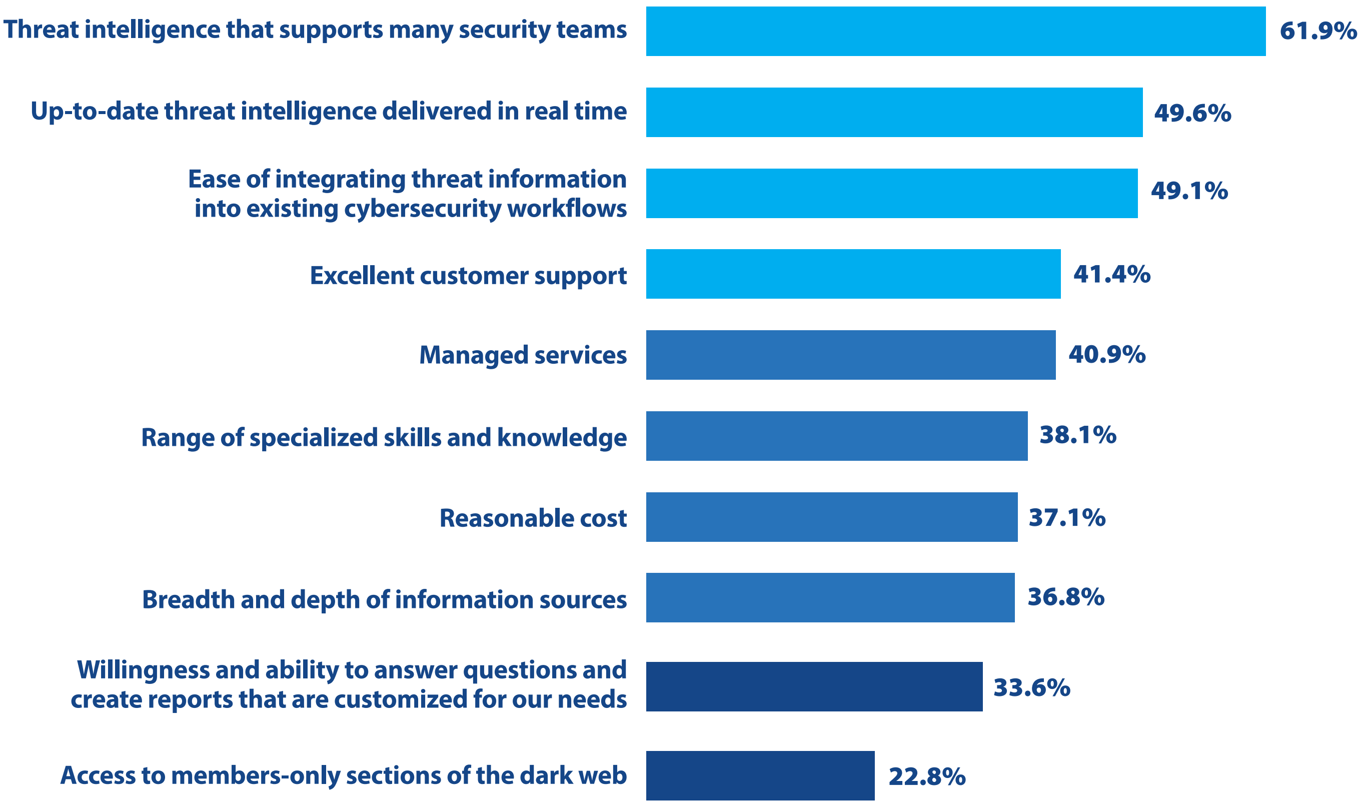

Figure 8: Characteristics most important for selecting a threat intelligence vendor.

We wanted to know what characteristics organizations are looking for in their threat intelligence vendors, and asked respondents to choose the top five from a list.

The number one requirement by a large margin is the ability to support many security teams, e.g., security operations, vulnerability management, supply chain security, brand protection, and risk management. This was highlighted by 61.9% of the respondents (see Figure 8). The strong interest in supporting multiple use cases aligns with the data from an earlier question showing that most organizations are leveraging threat intelligence for many purposes (see Figure 1 on page 6).

Also at the top of the list: up-to-date data delivered in real time to counteract attacks that mutate rapidly (49.6%) and ease of integration into cybersecurity workflows, to automate and accelerate detection and response (49.1%).

The next tier of selection factors includes excellent customer support (41.4%), the availability of managed services (e.g., alert triaging and domain takedown services – 40.9%), and a wide range of specialized skills and knowledge (38.1%).

"Reasonable cost" is considered a significant factor by 37.1% of the organizations in the survey – which means it is *not* one of the top five for almost two-thirds (62.9%). This finding indicates that organizations are more concerned with data quality, speed, and other non-financial factors than with cost. It is also consistent with the opinion of a large majority of respondents that their organizations are adequately funding threat intelligence activities (see page 19).

Threat Intelligence Organizations

Do you have a dedicated threat intelligence team?

Cybersecurity groups typically progress through a series of organizational steps as their threat intelligence capabilities grow. They start with nobody explicitly responsible for intelligence, to having some people working on it part time, to having specialists on several teams, to having a team dedicated to gathering and analyzing threat intelligence. Today, a strong majority (70.9%) have a dedicated threat intelligence team (see Figure 9).

As shown in Figure 10, among industries, the leaders are Technology & Electronics (81.7%), Telecom & Internet (80.6%), and Finance (75.0%). The laggards are Manufacturing (60.0%), Retail and Consumer Durables (56.1%), and Education (53.8%).

The widespread commitment to investing in threat intelligence is demonstrated by the fact that in every country and in every major industry included in this survey, at least 80% of organizations have people working full time on collecting and analyzing intelligence, either on existing security teams or on a dedicated threat intelligence team.

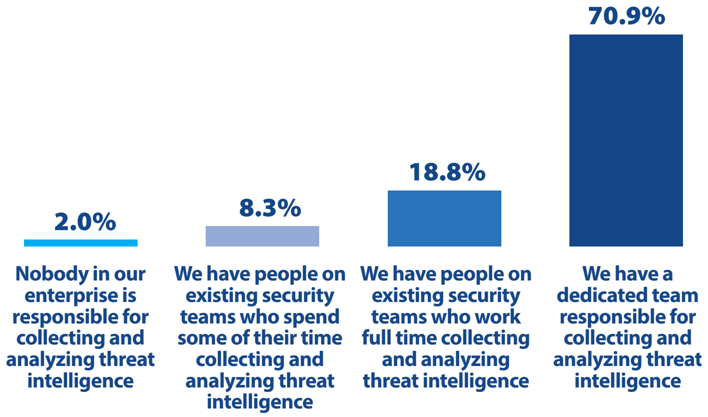

Figure 9: Responses to the question "Do you have a dedicated threat intelligence team?

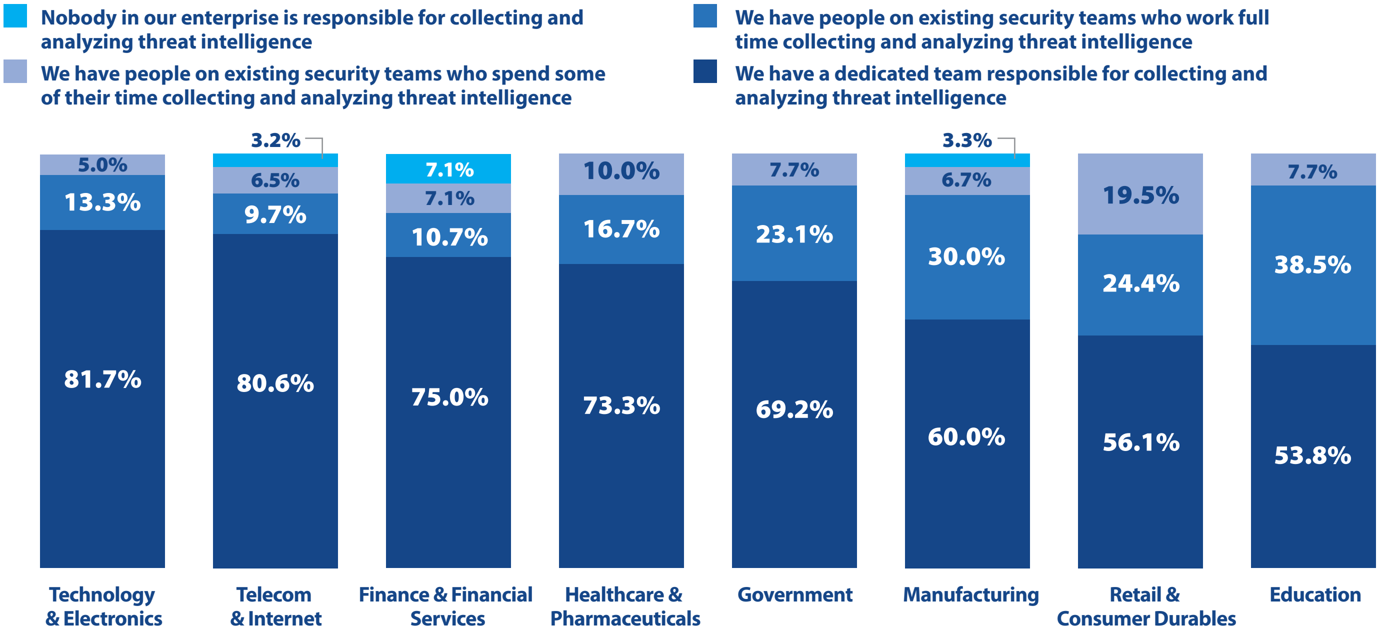

Figure 10: Responses by industry to the question, "Do you have a dedicated threat intelligence team?"

Maturity of Threat Intelligence Programs

Select the response that best describes the maturity of your threat intelligence efforts.

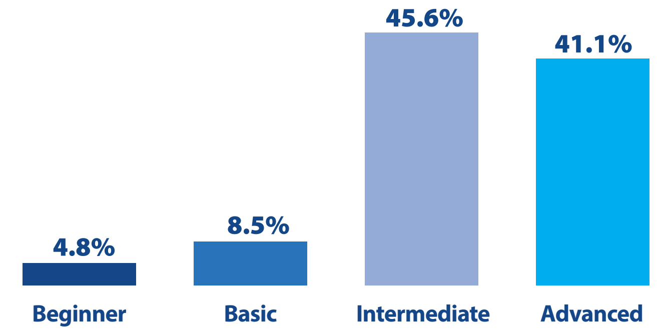

Figure 11: Maturity of threat intelligence efforts.

KEY

Beginner: We primarily consume threat intelligence via our detection tools and/or free threat data feeds.

Basic: We use a few threat data feeds, our threat intelligence analysts wear many hats, and we mostly react to alerts.

Intermediate: We use multiple independent threat intelligence sources, have threat intelligence specialists integrated into different security teams, and have structured workflows that integrate threat intelligence with a few key security activities.

Advanced: We have tools that combine outputs from multiple threat intelligence sources, a dedicated threat intelligence team, and automated workflows that integrate threat intelligence with most security activities including business risk assessment.

We asked respondents to assess the maturity of their threat intelligence programs. Only a few organizations consider themselves at beginner or basic levels (4.8% and 8.5%, respectively – see Figure 11). A plurality (45.6%) describe themselves as intermediate, while a sizeable number believe they deserve to be considered advanced (41.1%).

As shown in Figure 12, countries exhibit quite a range in the percentage of organizations considering themselves advanced. They start at 62.0% and 47.0% in the UK and USA and fall to 28.6% and 22.0% in Japan and Australia. Interestingly, the country with the most organizations willing to rate themselves as beginner was the US (10.0%).

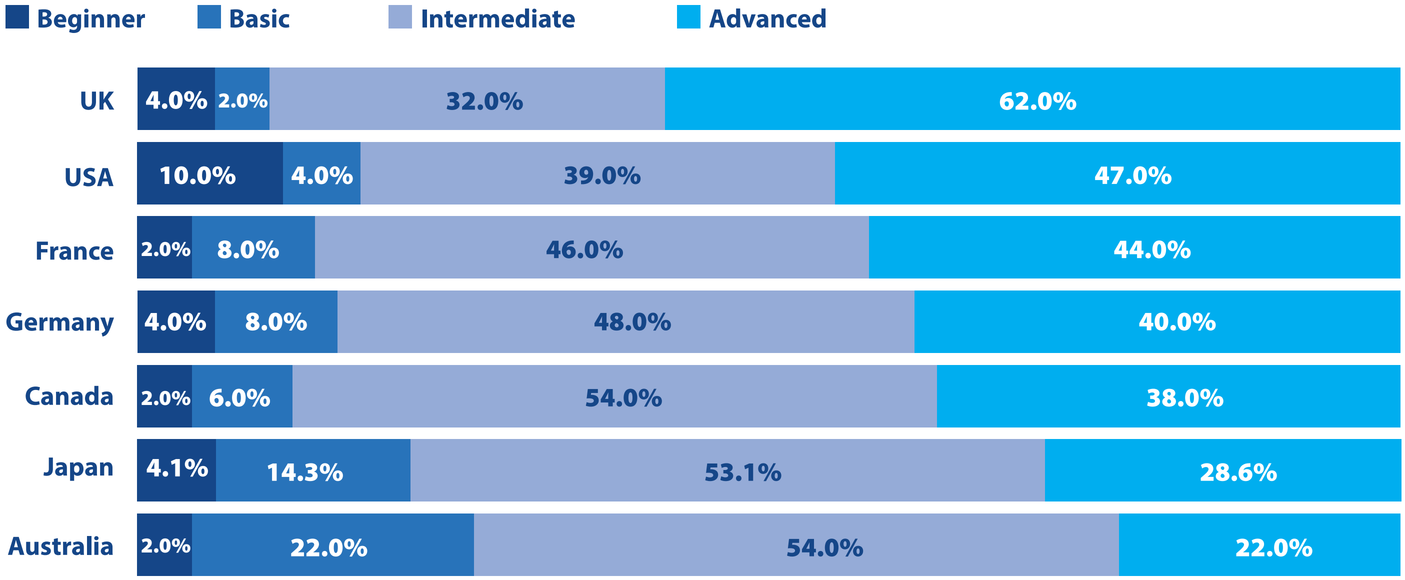

Figure 12: Maturity of threat intelligence efforts, by country.

Investment in Threat Intelligence

Select the option that best describes your agreement with the following statement: "My organization is making an adequate investment in threat intelligence."

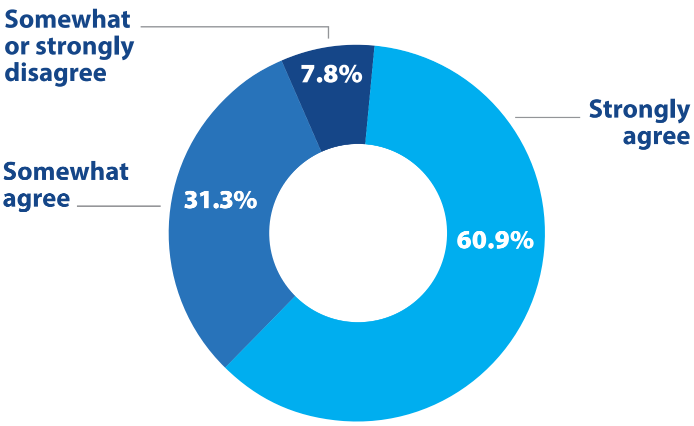

Figure 13: Responses to the statement "My organization is making an adequate investment in threat intelligence."

Fortunately, the powers that be in the great majority of enterprises appear to have recognized that threat intelligence is critical for cybersecurity and needs to be well funded. A full 92.2% of survey respondents somewhat or strongly agree that their organization is making adequate investments in threat intelligence (see Figure 13). That includes a full 100% of respondents in the US. Only a modest 7.8% feel their threat intelligence budget is underfunded.

However, there are pockets of discontent. For example, the number of respondents who disagree that threat intelligence funding is adequate is relatively high in Education (15.4%) and in Healthcare & Pharmaceuticals (16.7%) (see Figure 14).

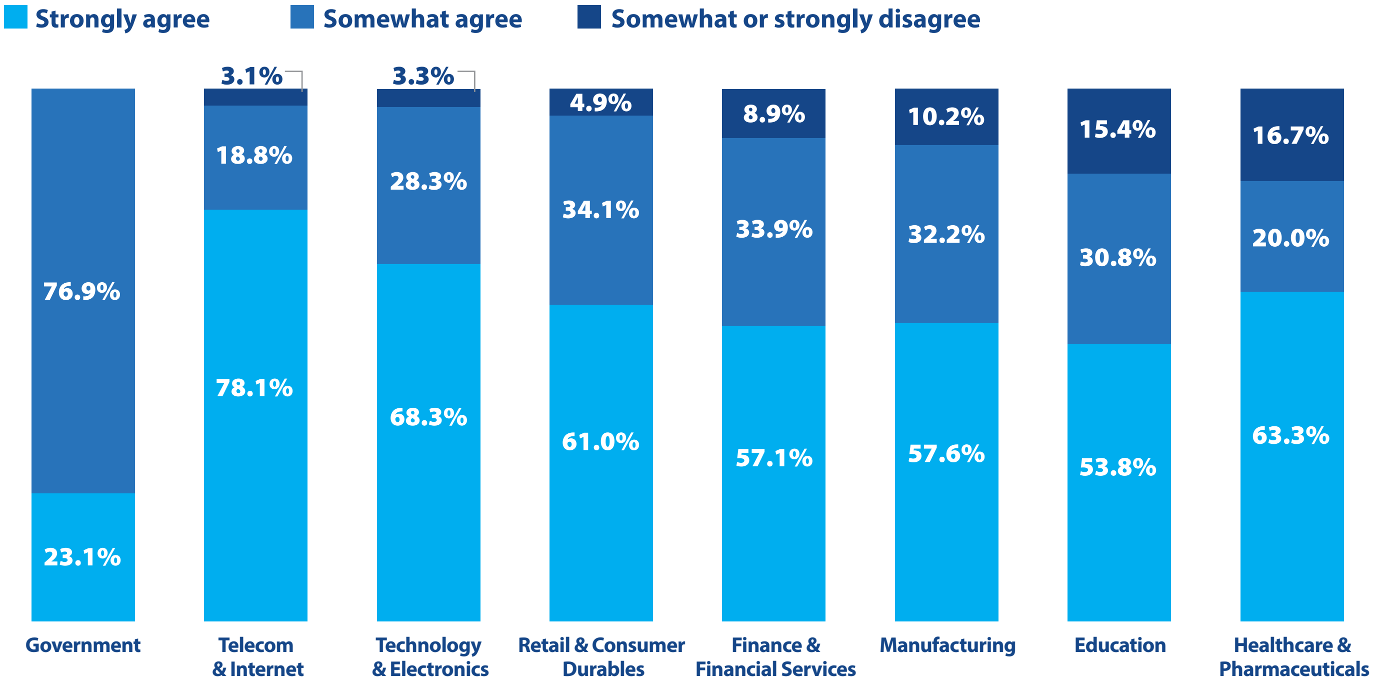

Figure 14: Responses to the statement "My organization is making an adequate investment in threat intelligence" by industry.

Plans for Working with Threat Intelligence Vendors

Select the response that best describes your organization's plans for working with threat intelligence vendors.

Most organizations are leveraging multiple sources of threat intelligence (see Figure 6 on page 12). But what are their plans for working with intelligence vendors in the future – are they planning to consolidate or add new ones?

Our data tells us that a plurality (44.4%) expect to keep the number of threat intelligence vendors they work with about the same (see Figure 15).

Of organizations contemplating changes, more are planning to increase the number of vendors (27.8%) than decrease them (17.2%). We think this reflects both an increasing appetite for threat intelligence in general, and the expanding number of use cases where intelligence is providing value.

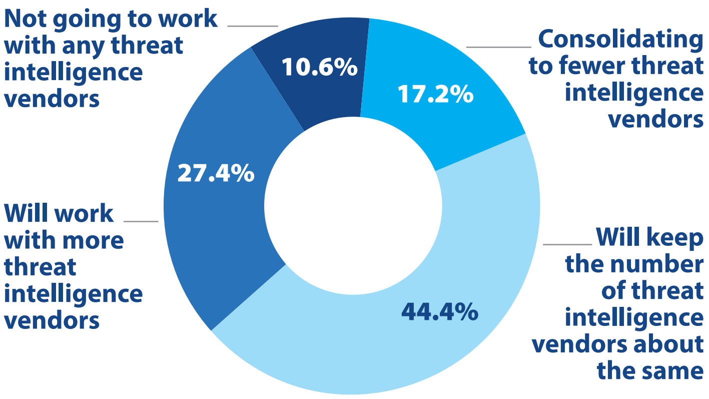

Figure 15: Organizations' plans for working with threat intelligence vendors.

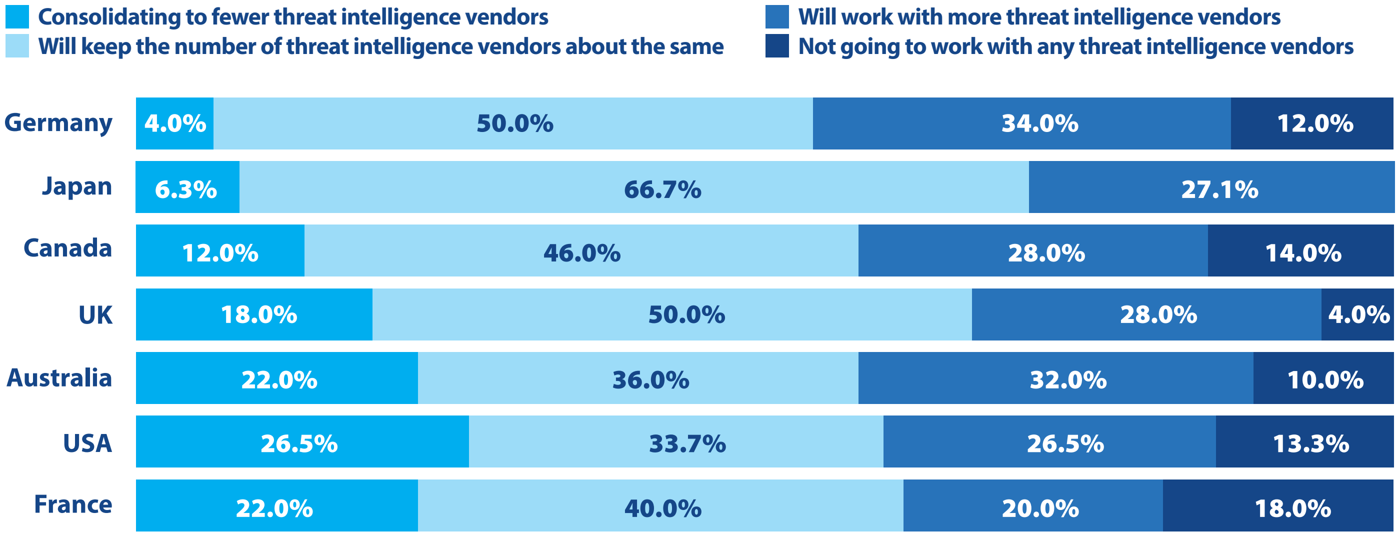

Figure 16: Organizations' plans for working with threat intelligence vendors, by country.

Plans varied significantly across countries. Germany, Japan, Canada, the UK, and Australia are planning to significantly increase the number of vendors they work with (net change = percent that will work with more vendors minus percent consolidating), while on average the US and France are standing pat (see Figure 16).

Plans to Improve Threat Intelligence

How does your organization plan to improve its use of threat intelligence over the next two years?

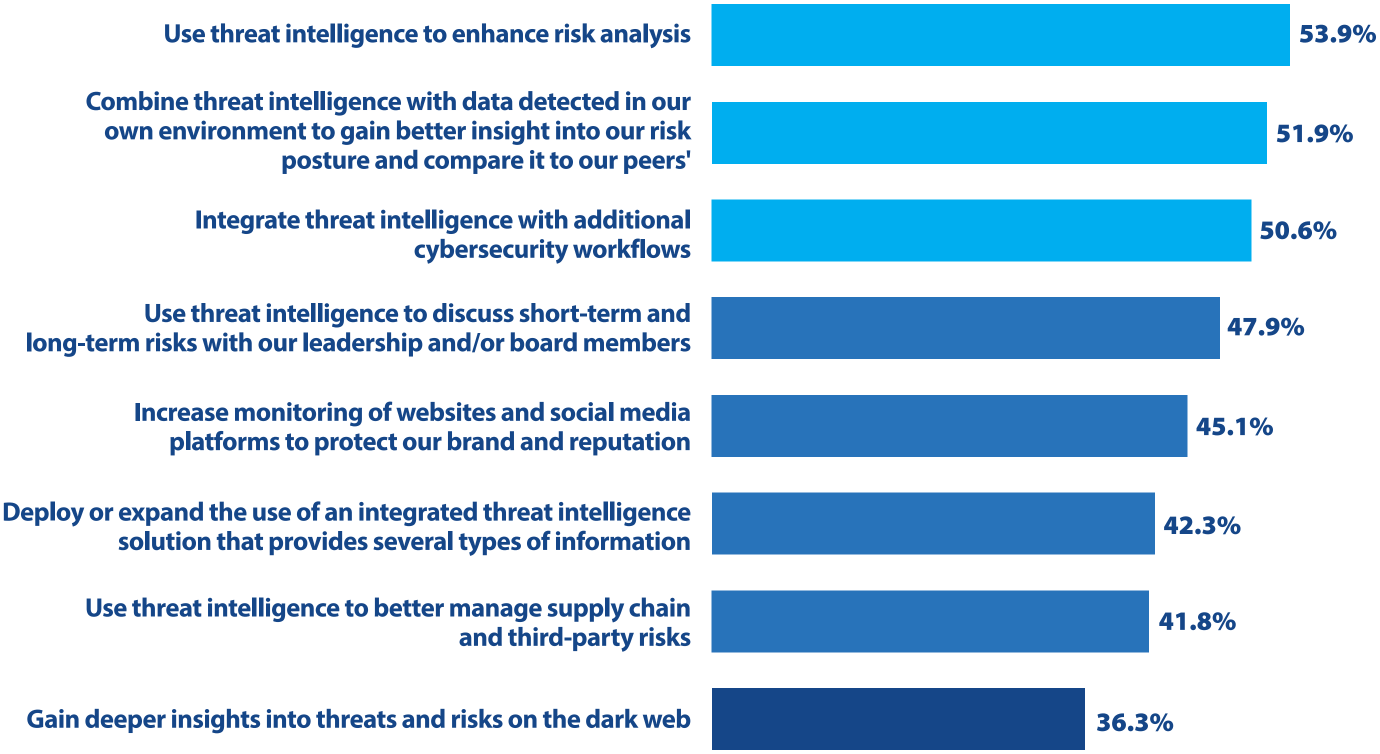

Figure 17: Plans to improve threat intelligence over the next two years.

The 400 respondents in our survey highlighted several priorities for improving and expanding their organizations' use of threat intelligence (see Figure 17).

First on the list is using intelligence to enhance risk analysis, planned by 53.9% of organizations. Threat intelligence will help enterprises align their cybersecurity investments with actual risks and business outcomes.

Also mentioned by at least half of our respondents are combining internal and external threat data (51.9%) and integrating intelligence with additional cybersecurity workflows (50.6%). These moves will make threat detection and incident response more accurate and faster.

Section 3: Threat Intelligence Organization and Plans

Just under half (47.9%) will use threat intelligence to improve communication with management and boards. Cybersecurity leaders have gained increased access to top decision makers now, and they need objective information to justify their proposed investments.

We mentioned on page 7 that groups outside of cybersecurity have found ways to leverage threat intelligence, including marketing and third-party risk management teams. This is illustrated by 45.1% of respondents indicating that their organizations are planning to increase their monitoring of websites and social media platforms to protect brands and reputations and 41.8% saying they plan to increasingly leverage threat intelligence to manage supply chain and third-party risks.

"The 400 respondents in our survey highlighted several priorities for improving and expanding their organizations' use of threat intelligence. First on the list is using intelligence to enhance risk analysis...Threat intelligence will help enterprises align their cybersecurity investments with actual risks and business outcomes."

Conclusions

Going deeper and branching out

Our survey provides ample evidence that threat intelligence is firmly established as a core element of cybersecurity while also branching out to address issues of key interest to additional groups in the enterprise. In fact, use cases and benefits can now be viewed as falling in three categories:

- **Operational –** improving the day-to-day performance of cybersecurity teams
- **Strategic –** helping security leaders and executive management accurately assess risks and align cybersecurity activities and investments with business needs
- **Specialized –** enabling groups outside of (but allied with) cybersecurity to achieve goals such as protecting the organization's brand and reputation online, protect physical facilities and employees globally, manage third party risks, and reducing online fraud

In the operational category, threat intelligence is acting as a force multiplier to make existing security tools more effective, helping SOCs triage alerts faster and more accurately, and keeping incident response and threat hunting teams up-to-date on the latest tactics of threat actors. These use cases are well established. The challenge now is to ensure that threat-related data collection and analysis can keep up with emerging threats and new types of adversaries, particularly state-supported hacking groups that are increasingly targeting commercial businesses in addition to governments and defense contractors.

In the strategic category, threat intelligence is helping security leaders fine-tune cybersecurity programs and communicate priorities to executive management and boards of directors. The challenge going forward is to increase the acceptance of intelligence in these roles, especially by converting information about the threat landscape into quantified assessments of risk and potential effect on the enterprise.

The specialized use cases are a growth area for threat intelligence. They partly reflect the need to respond to newer threats (e.g., typosquatting, creating fake social media accounts that post embarrassing and controversial material, embedding malicious software in third-party products) and the need to do a better job defending against existing threats such as online fraud.

Comprehensive data and threat intelligence platforms

Survey findings confirm that the vast majority of organizations are obtaining and using threat intelligence from five or more sources. Moreover, most are planning to maintain or increase the number of threat intelligence vendors they work with. This is being driven by requirements for comprehensive data and for access to an increasingly wide range of specialized skills and detailed information on a wide range of adversary TTPs. The same forces are pushing organizations to deploy threat intelligence platforms that can simplify the collection and correlation of data from multiple sources.

The need for an increasingly wide range of threat intelligence is likely to continue. However, as individual threat intelligence vendors add more types of intelligence to their portfolios, it is possible that the need could be met by fewer suppliers, leading to a consolidation in the number of vendors for the average organization.

Conclusions

Nobody resting on their laurels

Threat intelligence programs are not static. Organizations are planning to expand and improve their threat intelligence activities in all three of the categories we discussed above, for example:

- Combining external and internal threat intelligence and integrate intelligence with additional cybersecurity workflows (operational use cases)
- Using threat intelligence to enhance risk analysis and help communication with leadership and board members (strategic use cases)
- Increase monitoring of website and social media platforms to protect brands and using threat intelligence to better manage supply chain and third-party risks (specialized use cases)

Solid focus, funding, and maturity

The survey provides substantial evidence that threat intelligence is on a firm footing in most enterprises (at least those with 1,000 or more employees).

A solid 71% of organizations have a dedicated threat intelligence team. No less than 92% of respondents somewhat or strongly agree that their organizations are making an adequate investment in the program. And only 13% assess the maturity level of their threat intelligence efforts as "beginning" or "basic": the other 87% selected "intermediate" or "advanced." In other words, threat intelligence programs are now mainstream, valued contributors to cybersecurity programs in almost all organizations.

Appendix 1: Demographics

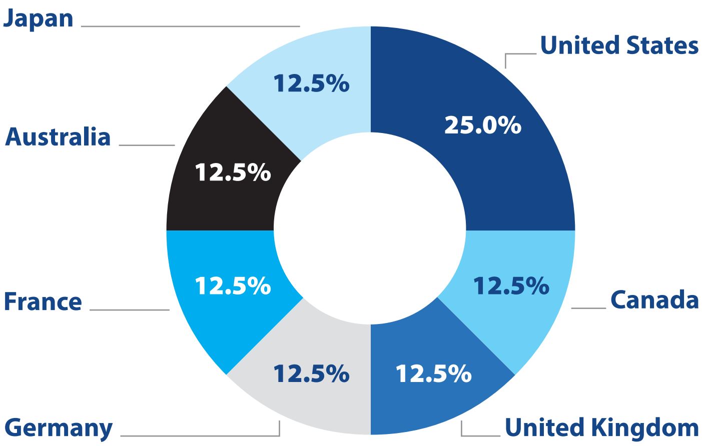

Figure 18: Survey respondents by country.

This report is based on survey results obtained from 400 qualified participants hailing from 7 countries (see Figure 18). Each participant was required to have a role as a cybersecurity manager or practitioner with knowledge about their organization's use of threat intelligence (see Figure 19). About two-thirds (67.5%) of our respondents held executive or managerial positions in cybersecurity.

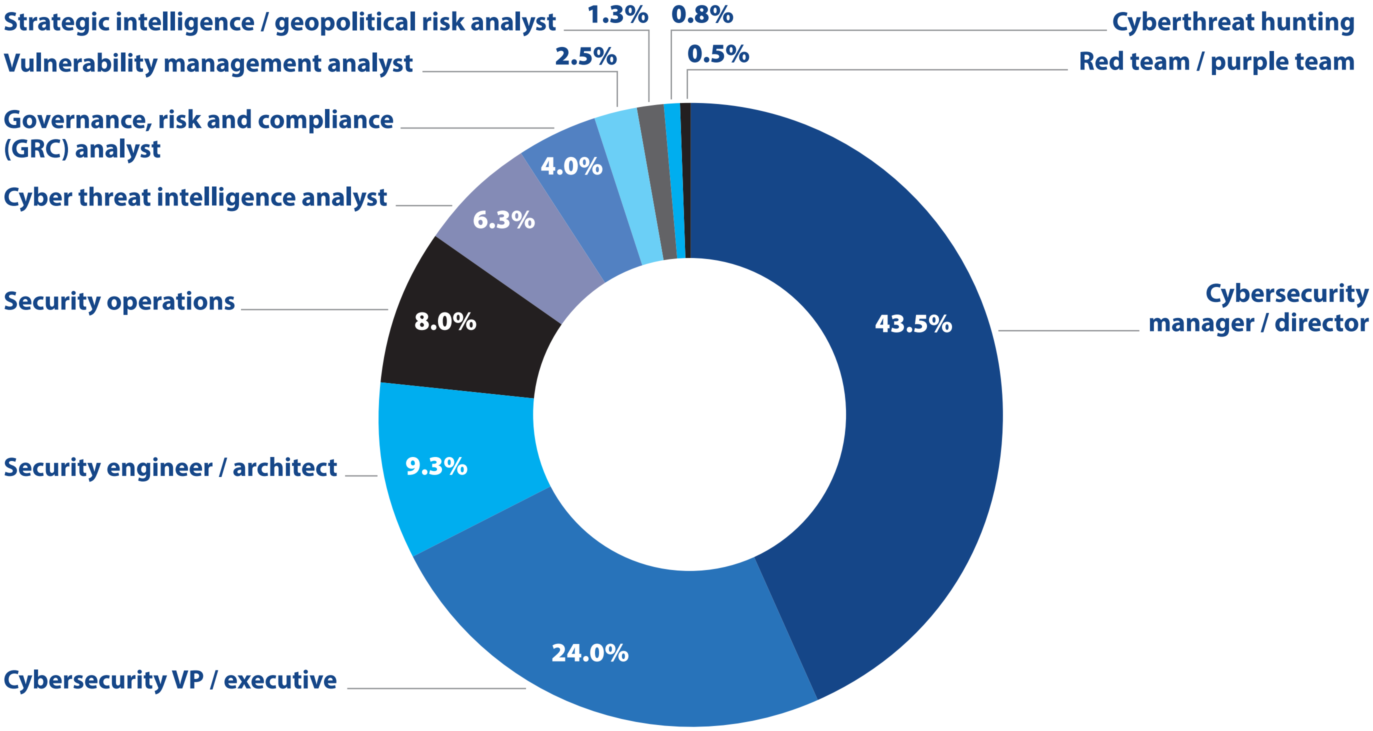

Figure 19: Survey respondents by role.

Appendix 1: Demographics

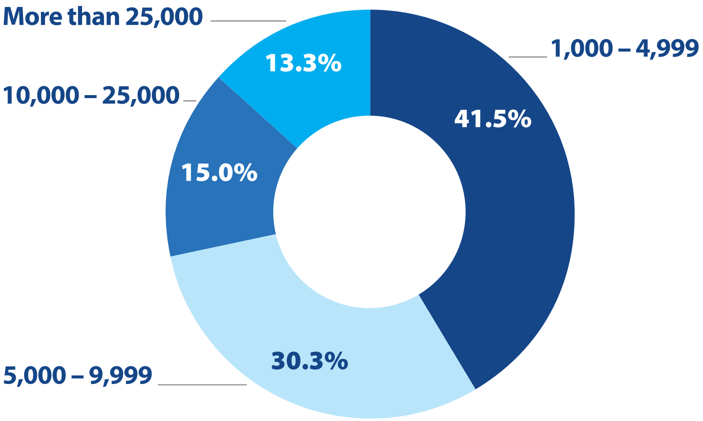

Figure 20: Survey respondents by organization employee count.

All participants in this survey were working for organizations with 1,000 or more employees (see Figure 20). They spanned 8 major industries (plus "Other") with no single industry composing more than 15% of the total participants (see Figure 21).

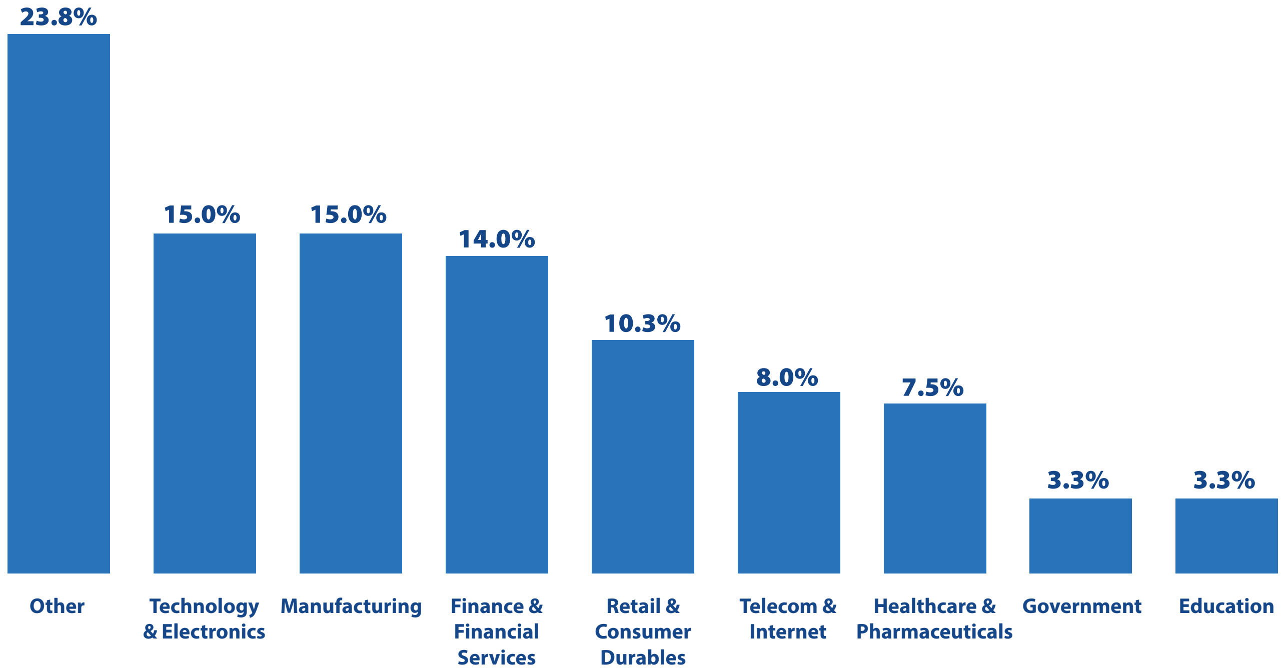

Figure 21: Survey respondents by industry.

Appendix 2: Research Methodology

CyberEdge developed a 15-question survey instrument in partnership in partnership with Recorded Future. The survey was completed by 400 IT security professionals in the United States, Canada, the United Kingdom, Germany, France, Australia, and Japan in August 2023. The global margin of error for this research study (at a standard 95% confidence level) is 5%. All results pertaining to individual countries and industries should be viewed as anecdotal, as their sample sizes are much smaller. CyberEdge recommends making actionable decisions based on global data only.

All respondents had to meet two filter criteria: (1) they had to have a cybersecurity role; and (2) they had to be employed by a commercial or government organization with a minimum of 1,000 global employees.

At CyberEdge, survey data quality is paramount. CyberEdge goes to extraordinary lengths to ensure its survey data is of the highest caliber by following these industry best practices:

- Ensuring that the right people are being surveyed by (politely) exiting respondents from the survey who don't meet the respondent filter criteria of the survey (e.g., job role, company size, industry)
- Ensuring that disqualified respondents (who do not meet respondent filter criteria) cannot restart the survey from the same IP address in an attempt to obtain the survey incentive
- Constructing survey questions in a way that eliminates survey bias and minimizes the potential for survey fatigue
- Only accepting completed surveys after the respondent has provided answers to all of the questions
- Ensuring that respondents view the survey in their native language (i.e., English, German, French, Japanese)
- Randomizing survey responses when possible to prevent order bias
- Adding "Don't know" (or comparable) responses when possible so respondents aren't forced to guess at questions when they don't know the answer
- Eliminating responses from "speeders" who complete the survey in a fraction of the median completion time
- Eliminating responses from "cheaters" who apply consistent patterns to their responses (e.g., A,A,A,A and A,B,C,D,A,B,C,D)
- Ensuring the online survey is fully tested and easy to use on computers, tablets, and smartphones

CyberEdge would like to thank Recorded Future for making this research study possible. We'd particularly like to thank Kalpana Singh and Sam Langrock for sharing their threat intelligence knowledge and perspectives with us.

Appendix 3: About Our Sponsor

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence. Learn more at recordedfuture.com.

Appendix 4: About CyberEdge Group

Founded in 2012, CyberEdge is the largest research, marketing, and publishing firm to serve the cybersecurity vendor community, working with approximately one in every six established security vendors.

CyberEdge's highly acclaimed Cyberthreat Defense Report (CDR) and other single- and multi-sponsor survey reports have garnered numerous awards and have been featured by both business and technology publications alike, including *The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Magazine, DarkReading,* and *CISO Magazine*.

CyberEdge has cultivated a reputation for delivering the highest-quality market research data, survey reports, analyst reports, white papers, and custom books and eBooks in the cybersecurity industry. The depth of its cybersecurity subject matter expertise and the breadth of its services are second to none.

To learn more about CyberEdge, connect to www.cyber-edge.com.

CYBEREDGE
GROUP

CYBEREDGE GROUP, LLC

1997 ANNAPOLIS EXCHANGE PKWY.
SUITE 300
ANNAPOLIS, MD 21401

☎ 800.327.8711

🌐 WWW.CYBER-EDGE.COM

✉ INFO@CYBER-EDGE.COM

115.72.240[.]253
CVE-2 17-0199
Red Delta