Ponemon INSTITUTE

The State of Threat Hunting and the Role of the Analyst

Sponsored by Team Cymru

Independently conducted by Ponemon Institute LLC

Publication Date: August 2021

The State of Threat Hunting and the Role of the Analyst
June 2021

Part 1. Introduction

The purpose of this research is to track the level of importance placed on analysts with regard to organizations' security programs. Another objective is to track the state of maturity organizations have achieved with regard to threat hunting and their effectiveness in leveraging their threat hunters to positively impact other areas of security programs. Sponsored by Team Cymru, Ponemon Institute surveyed 1,778 IT and IT security professionals in North America, Latin America, the UK and Europe.

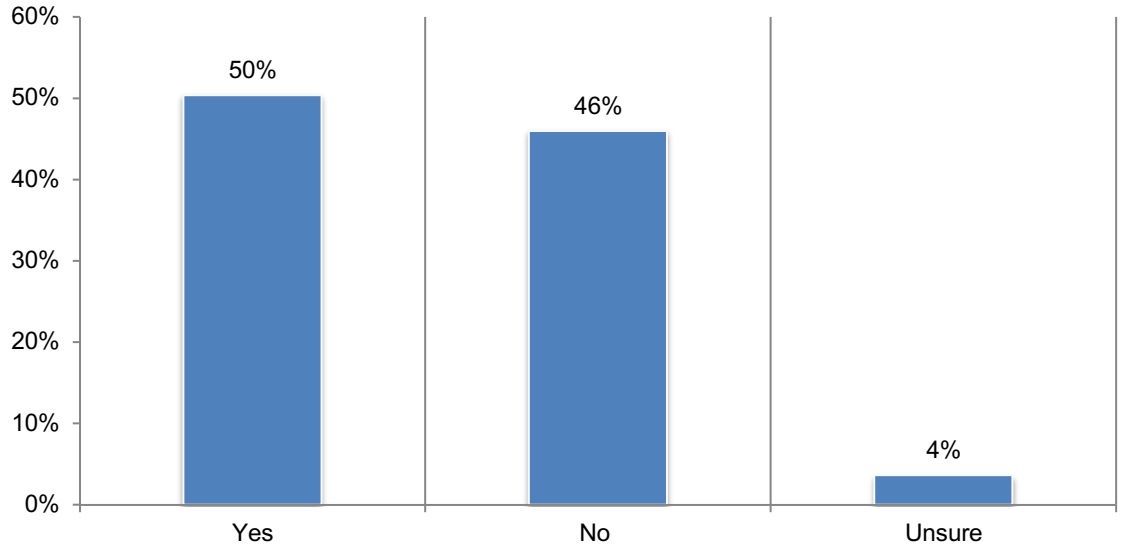
All organizations represented in this research have security/threat analysts gathering and/or using threat intelligence and engaging in threat hunting and/or threat reconnaissance. According to the research, the average 2021 budget in these organizations for IT operations is $117 million. An average of 19 percent of this is allocated to IT security and of that an average of 22 percent is allocated to analyst activities and threat intelligence—but more budget is needed. According to the findings, 68 percent of respondents say a significant investment to achieve a more mature threat hunting team can have a significant impact on the security posture of organizations.

To track the level of maturity at which analyst teams and threat hunting teams are operating, the research asks question related to the following stages of maturity: the use of threat intelligence, threat hunting as defined below and the introduction of cyber reconnaissance (a.k.a threat reconnaissance or external threat hunting).

Many companies are having recurring attacks from the same threat actor. Fifty percent of respondents say their organization had a cybersecurity incident that resulted in a significant disruption to its IT and business processes in the past two years.

As shown in Figure 1, 50 percent of these respondents say it was the result of an inability to prevent the recurrence of an attack from the same threat actor. Of these respondents, 61 percent say they did not remediate the compromises. As a result, these organizations are unable to gain long lasting network defense benefits from one incident to the next.

Figure 1. Were any cybersecurity incidents the result of an inability to prevent the recurrence of an attack from the same threat actor?



In the context of this research, threat hunting involves searching for signs of anything malicious inside a network, to close detection gaps that exist when relying solely on automated threat detection solutions. Its purpose is to reduce dwell time. The objective is to reduce the operational disruption and financial impact of cyberattacks that defenses have failed to detect or protect against.

However, more advanced threat hunters are using their existing intelligence sources along with Internet traffic telemetry to hunt outside their organizations' borders to carry out tasks, such as identifying and blocking impending attacks, monitoring their organizations' supply chains and blocking new malicious infrastructure as it is being stood up by various threat actors. For the purposes of this research, we refer to this as cyber reconnaissance a.k.a threat reconnaissance.

Following are key takeaways from the research.

- The threat intelligence market is still immature as the findings within this report demonstrate. While on one hand respondents say their organizations have high capabilities, the challenges associated with threat preventions, detection and incident response indicate that organizations do not fully grasp the strategic value external threat hunting can deliver across different teams and processes. Only 24 percent of respondents consider threat hunting to be looking outside the network perimeter to track threat actors and spot impending attacks.

- To fully realize the value of threat reconnaissance or external threat hunting, security teams need to reduce reliance on traditional threat intelligence feeds and automated tools to analyst-driven threat hunting with non-curated and unencumbered access to Internet infrastructure analysis data.

- Threat reconnaissance/external threat hunting is challenged as a concept because at best it sits among the "art of the possible" from those who have a desire to elevate their threat hunting and incident response team to gain more value, and at worst, is in a known/unknown quadrant to be encountered.

- Those with resources and budget to start a threat hunting program are not realizing its full value because the teams are underfunded, do not have the best tools for the job and the data being used is stale. Only 35 percent of respondents say their organizations value and effectively leverage the expertise of threat hunting teams.

Part 2. Key findings

In this section, we provide an analysis of the global research findings. The complete audited findings are presented in the Appendix of this report. The following topics are covered in this report.

- The role of threat analysts in creating a strong security posture
- The use of threat intelligence
- The effectiveness of threat hunting and cyber reconnaissance
- The need to improve threat hunting in the Cyber Kill Chain
- Differences among regions and countries

The role of threat analysts in creating a strong security posture

Most threat analysts in this study are users or managers in charge of threat intelligence. According to Figure 2, 52 percent of respondents say they are users of threat intelligence and another 52 percent are executives or managers in charge of threat intelligence activities. This is followed by gatherers of threat intelligence (47 percent of respondents) and analyzers of threat intelligence (41 percent of respondents).

Figure 2. How are you involved in your company's cyber threat intelligence activities or process?
More than one response permitted

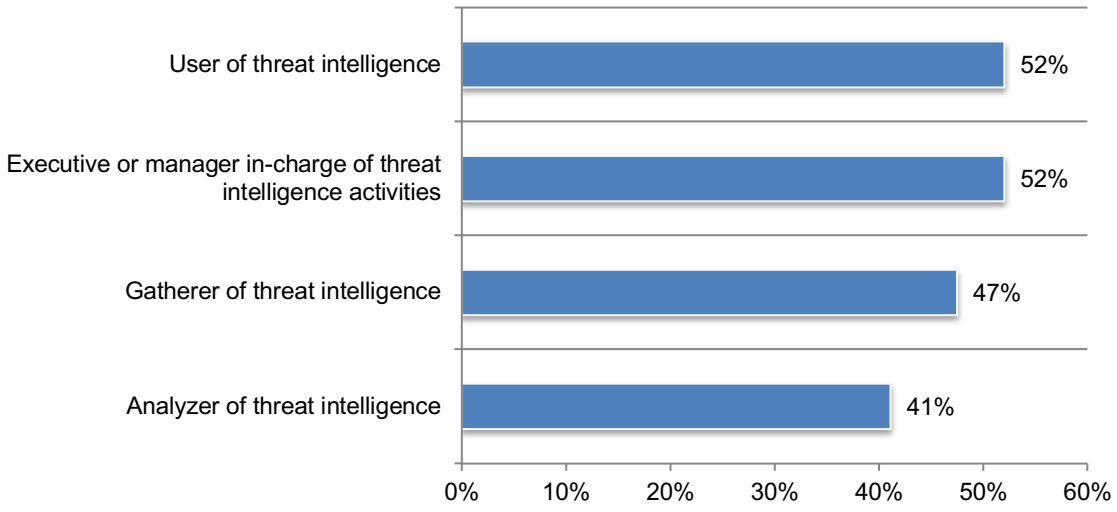
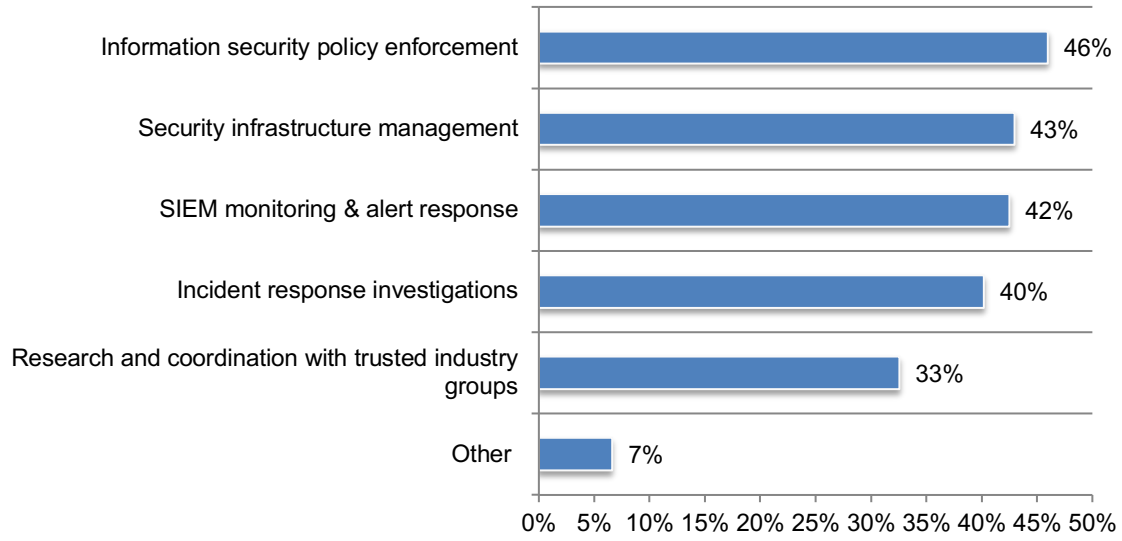


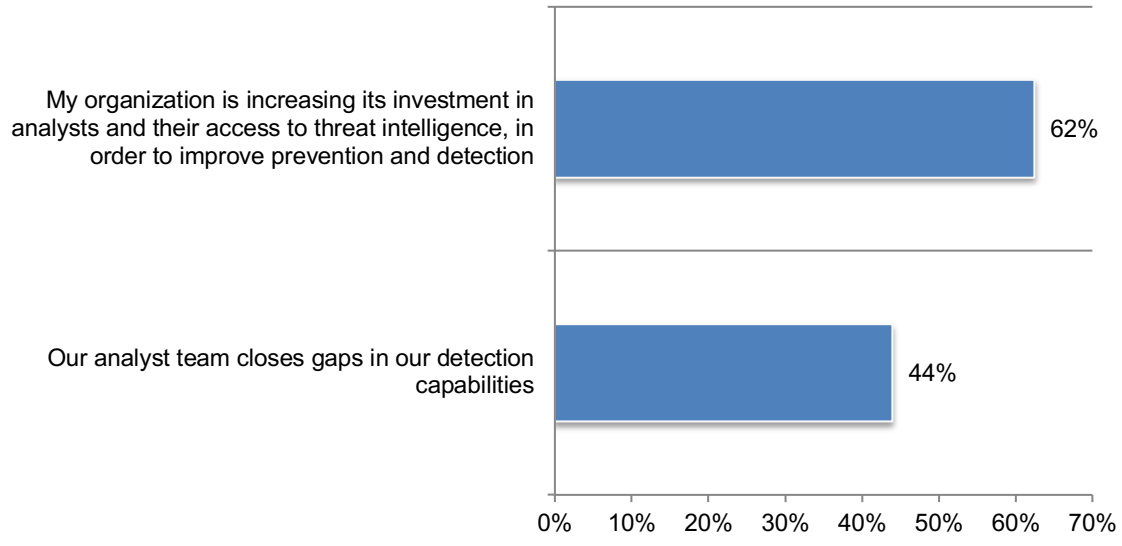
Figure 3 presents the tasks performed by security and threat analysts. The top three are information security policy enforcement (46 percent of respondents), security infrastructure management (43 percent of respondents) and SIEM monitoring and alert response (42 percent of respondents).

Figure 3. What tasks do security/threat analysts perform in your organization?
More than one response permitted



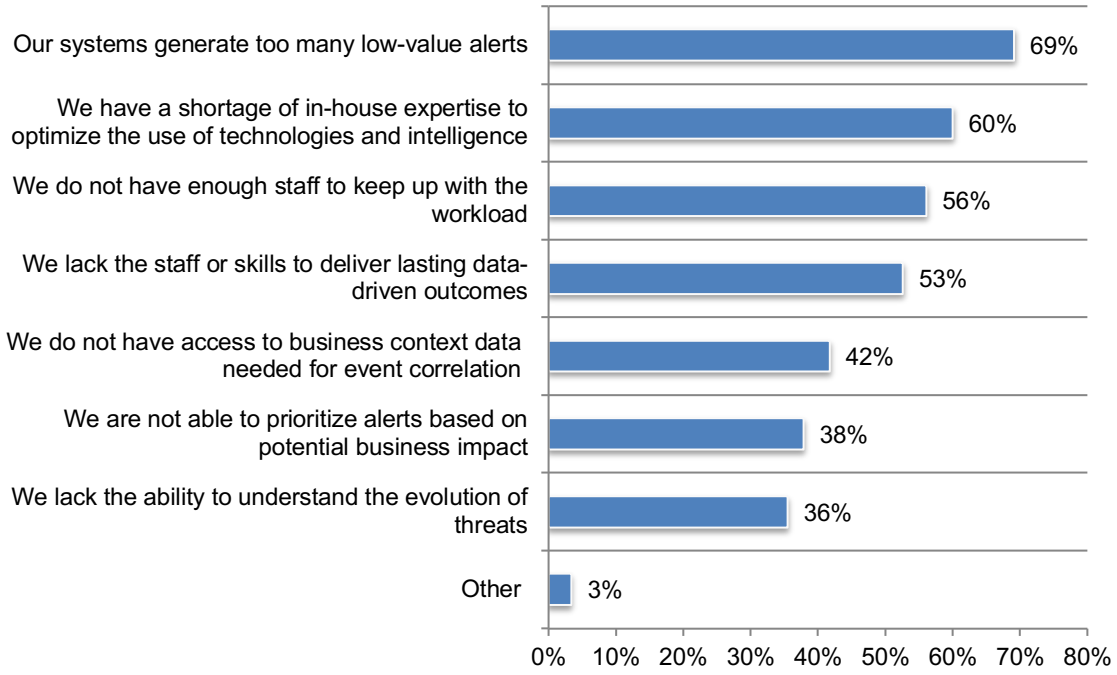
Organizations are increasing investment in analysts to improve prevention and detection of threats. As shown in Figure 4, 62 percent of respondents say their organizations are increasing their investment in analysts and their access to threat intelligence in order to improve prevention and detection. Such investment is necessary because a repeated theme in this research is not having adequate staff and in-house expertise. Further, only 44 percent say their analyst team is able to close gaps in their detection capabilities.

Figure 4. Perceptions about the role of security/threat analysts
Strongly agree and Agree responses combined



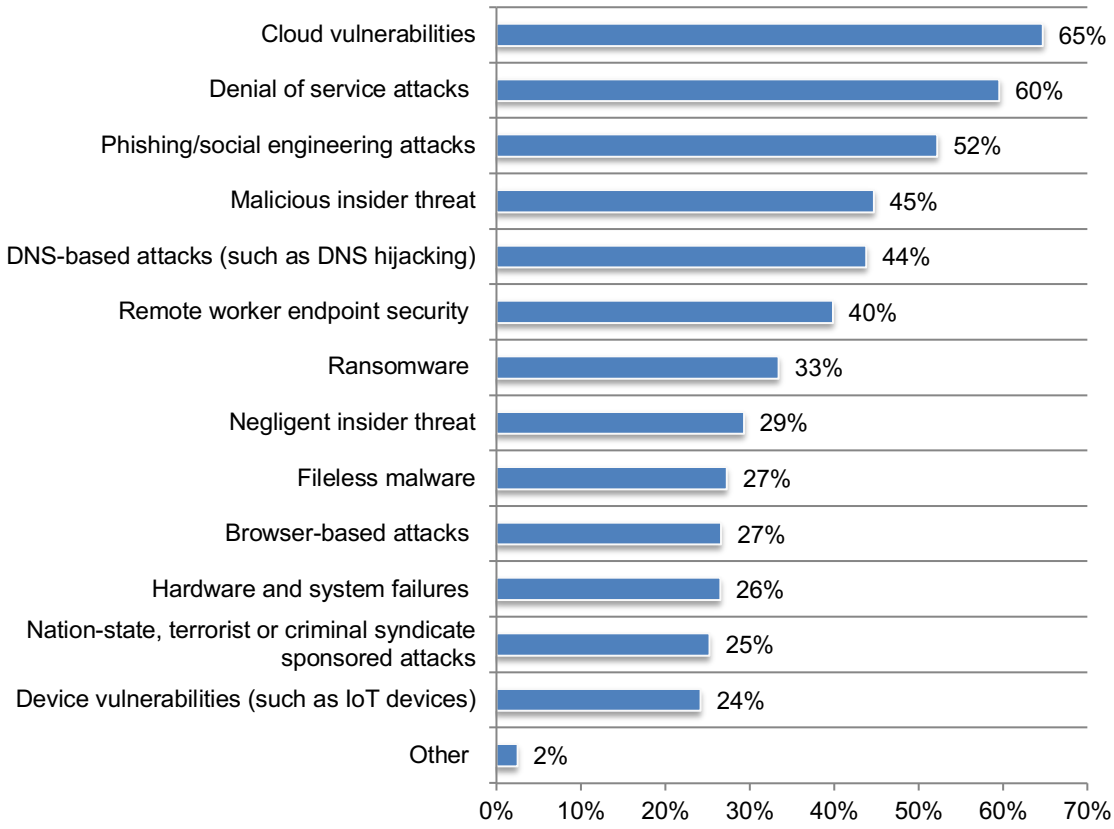
The biggest challenge for security analysts when supporting incident response processes is the need to deal with too many low-value alerts and not having adequate staffing. According to Figure 5, 69 percent of respondents say they are challenged by systems that generate too many low-value alerts followed by 60 percent of respondents who say their organizations have a shortage of in-house expertise to optimize the use of technologies and intelligence. Other challenges are not enough staff to keep up with the workload and lacking the staff or skills to deliver lasting data-driven outcomes (56 percent and 53 percent of respondents, respectively).

Figure 5. What are the biggest challenges threat analysts face when supporting incident response processes?
More than one response permitted



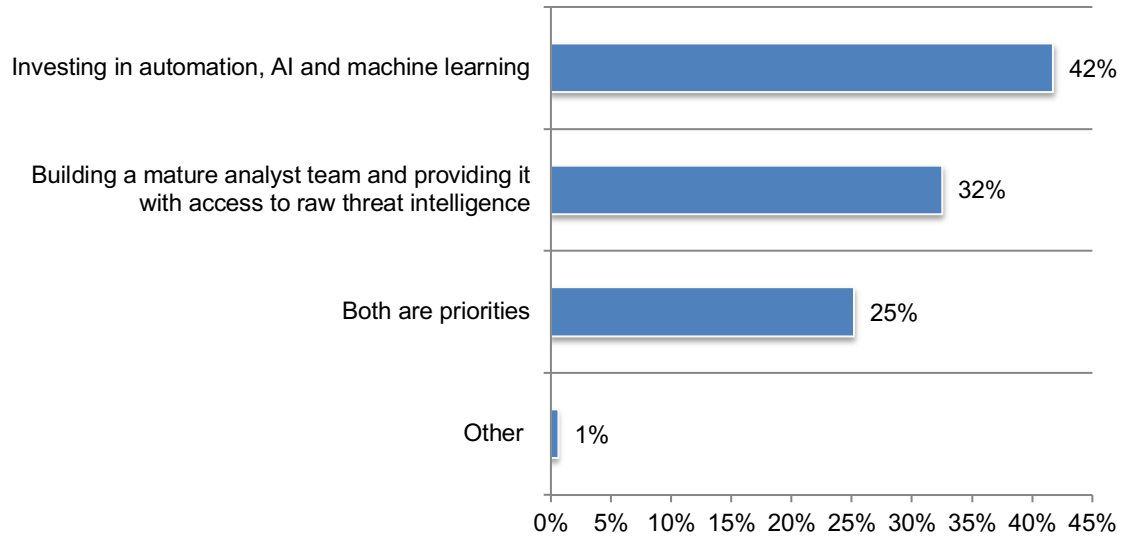
Vulnerabilities to the cloud infrastructure are considered the top security threat affecting analysts' organizations. Figure 4 presents a list of security threats. The top six risks are cloud vulnerabilities (65 percent of respondents), denial of service attacks (60 percent of respondents), phishing/social engineering attacks (52 percent of respondents), malicious insider threat (45 percent of respondents), DNS-based attacks (44 percent of respondents) and remote worker endpoint security (40 percent of respondents).

Figure 6. What are the top security threats affecting your organization?
Five responses permitted



The top step, according to respondents, to optimizing prevention, threat detection and incident response is automation, artificial intelligence and machine learning. As shown in Figure 7, 42 percent of respondents say investing in automation, AI and machine learning is the most important step to optimizing prevention, threat detection and incident response. This is followed by 32 percent of respondents who say building a mature analyst team and providing it with access to raw threat intelligence. Twenty-five percent of respondents say both are important steps to take.

Figure 7. What steps are most important to optimizing prevention, threat detection and incident response?

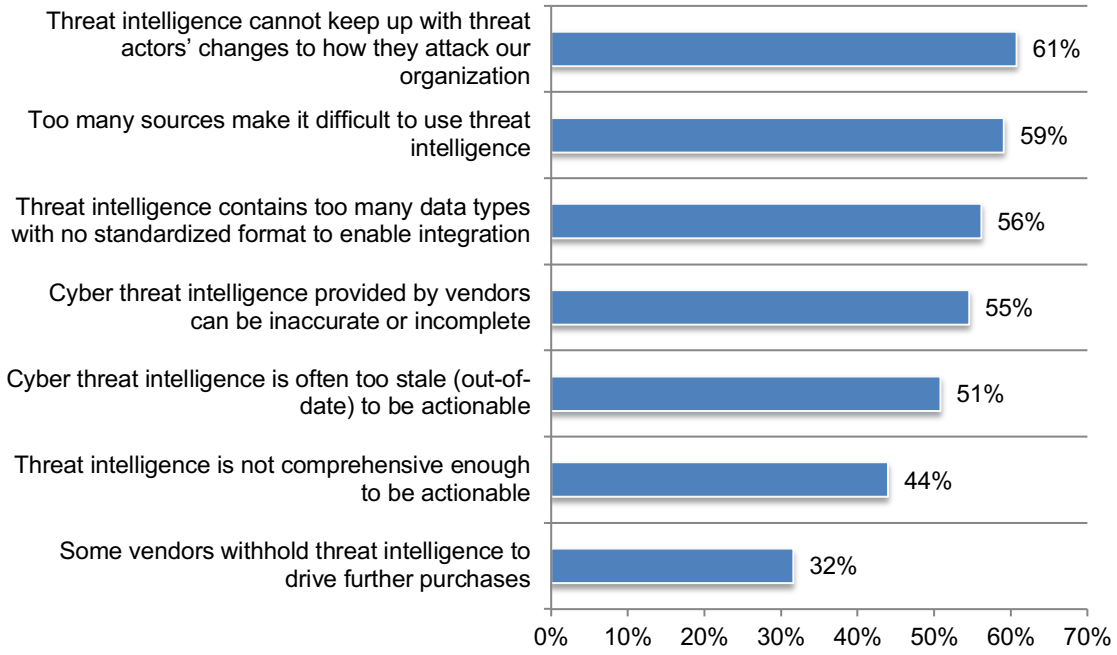


The use of threat intelligence

Threat intelligence is defined in this research as evidence-based knowledge that includes context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard.

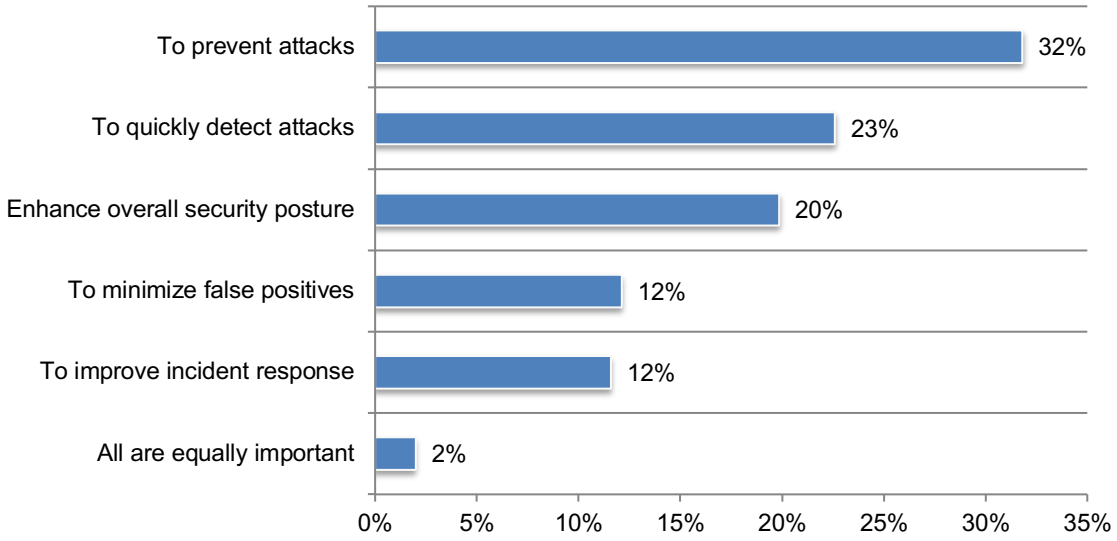
Threat intelligence cannot keep up with threat actors' changes to how they attack organizations. As shown in Figure 8, 61 percent of respondents agree that threat intelligence cannot keep up with threat actors' changes to how they attack their organizations. Respondents also strongly agree that too many sources make it difficult to use threat intelligence (59 percent), threat intelligence contains too many data types with no standardized format to enable integration (56 percent) and cyber threat intelligence provided by vendors can be inaccurate or incomplete (55 percent).

Figure 8. Perceptions about the use of threat intelligence
Strongly agree and Agree responses combined



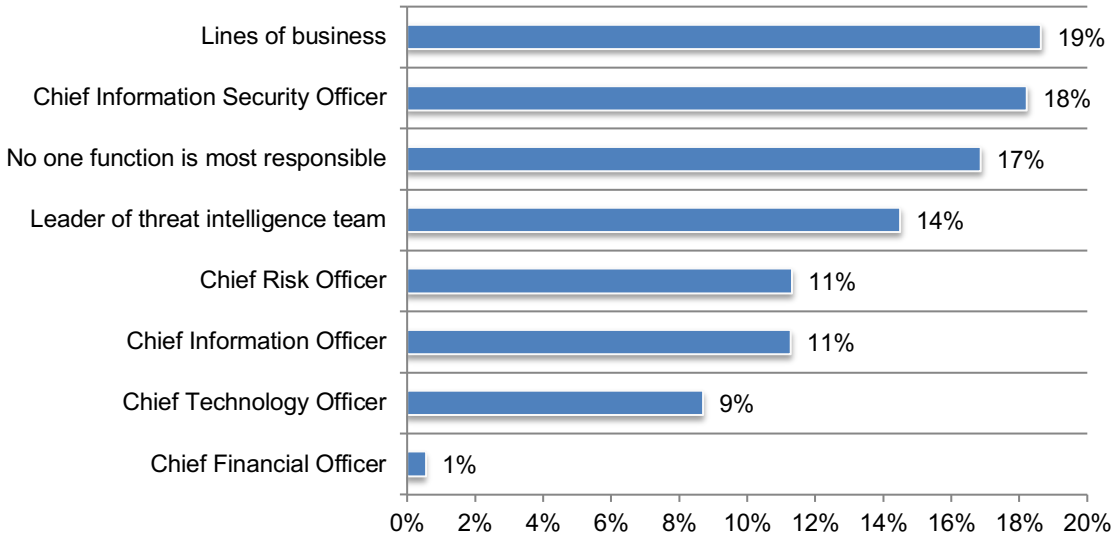
To prevent and quickly detect attacks are the two primary objectives for the use of threat intelligence. Respondents were asked to select the one primary objective for the use of threat intelligence. As shown in Figure 9, 32 percent of respondents say it is to prevent attacks followed by quickly detecting attacks (23 percent of respondents).

Figure 9. What is your organization's primary objective for the use of threat intelligence?



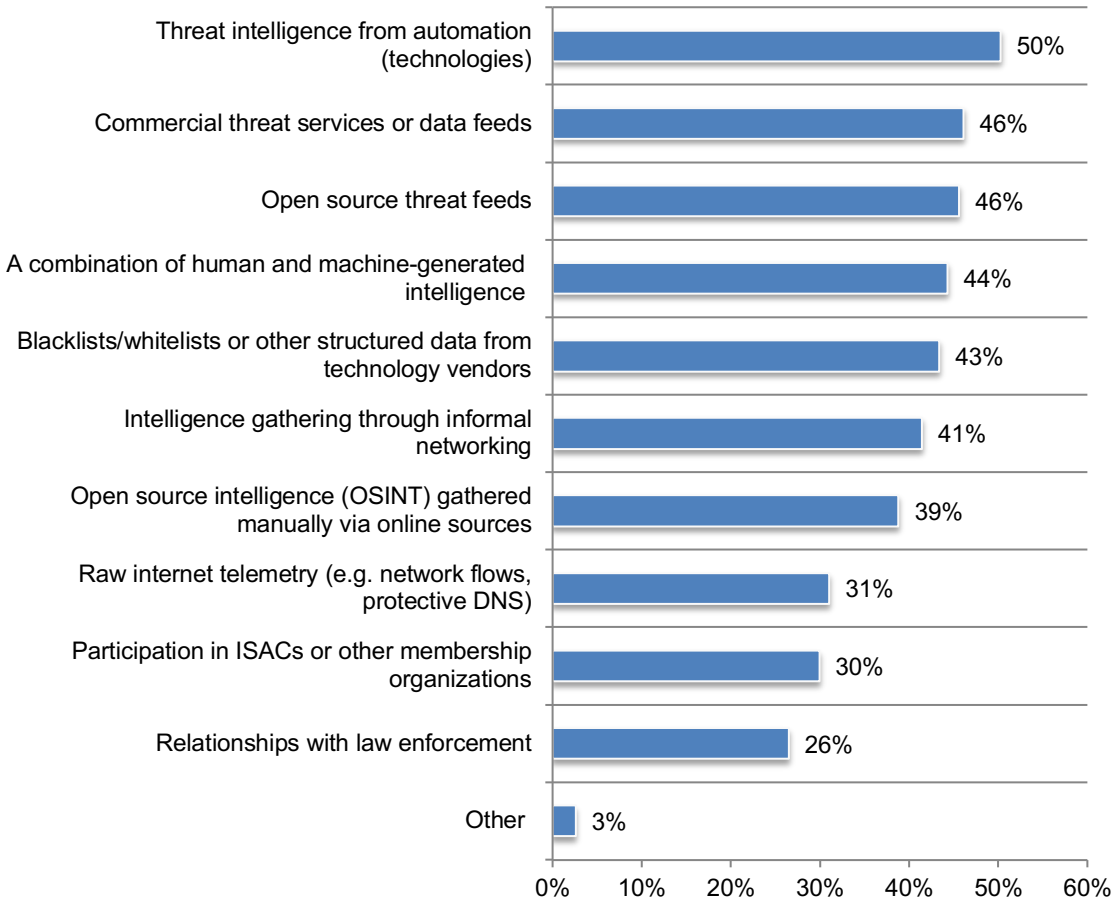
The leader of the threat intelligence team is seldom responsible for determining what threat intelligence sources are used. Responsibility for deciding what threat intelligence sources to use is dispersed throughout the organization and only 14 percent of respondents say it is the leader of the threat intelligence team, as shown in Figure 10. Twenty-nine percent of respondents say the CIO (11 percent) and the CISO (18 percent) are most responsible.

Figure 10. Who is most responsible for deciding what threat intelligence sources are used?



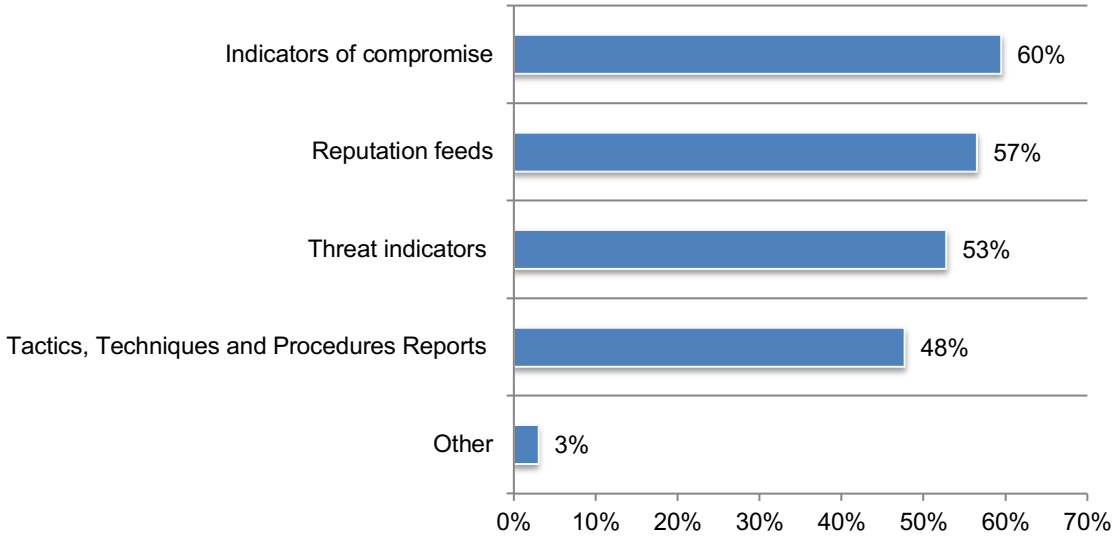
Threat intelligence from automation technologies is considered most important. As shown in Figure 11, 50 percent of respondents say threat intelligence from automation technologies is most important in their ability to plan preventative measures, detect threats and resolve security incidents followed by commercial threat services or data feeds and open source threat feeds (both 46 percent of respondents).

Figure 11. What threat intelligence activities and technologies are most important in their ability to plan preventive measures, detect threats and resolve security incidents
Four responses permitted



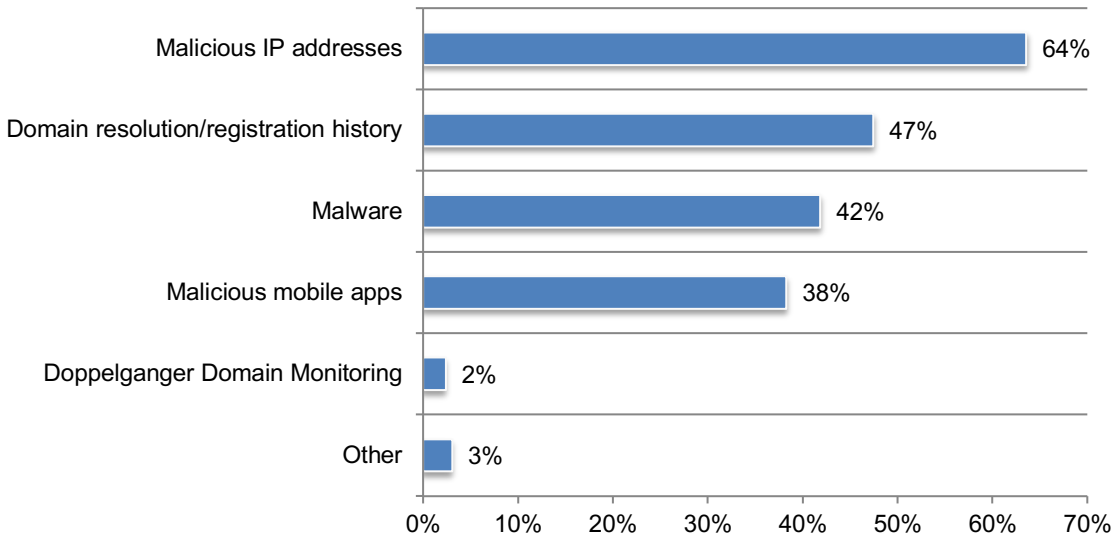
Indicators of compromise and reputation feeds are the types of threat intelligence most often used. As shown in Figure 12, 60 percent of respondents say indicators of compromise and 57 percent of respondents say reputation feeds are the types of threat intelligence their organizations use. Fifty-three percent of respondents say their organizations use threat indicators.

Figure 12. What threat intelligence sources does your company use?
More than one response permitted



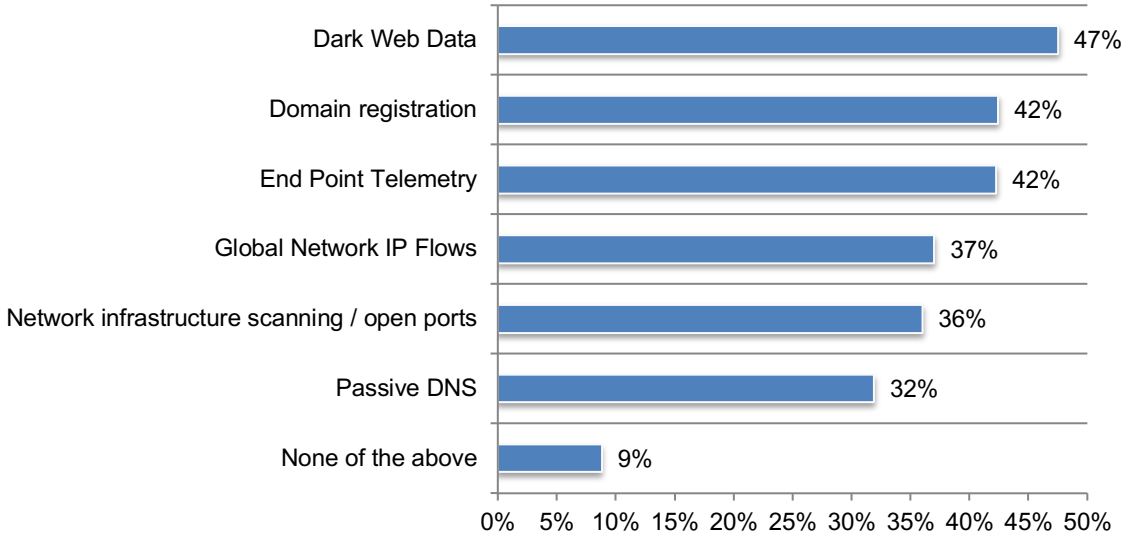
Malicious IP addresses and domain resolution/registration history are the threat indicators that provide the most valuable information, as shown in Figure 13.

Figure 13. If your organization uses threat indicators, which ones provide the most valuable information?
More than one response permitted



Organizations are most likely to have dark web data. According to Figure 14, 47 percent of respondents say the threat intelligence data they have is dark web data and 42 percent of respondents say they have end point telemetry and domain registration threat intelligence.

Figure 14. What are the threat intelligence data types you have today?
More than one response permitted

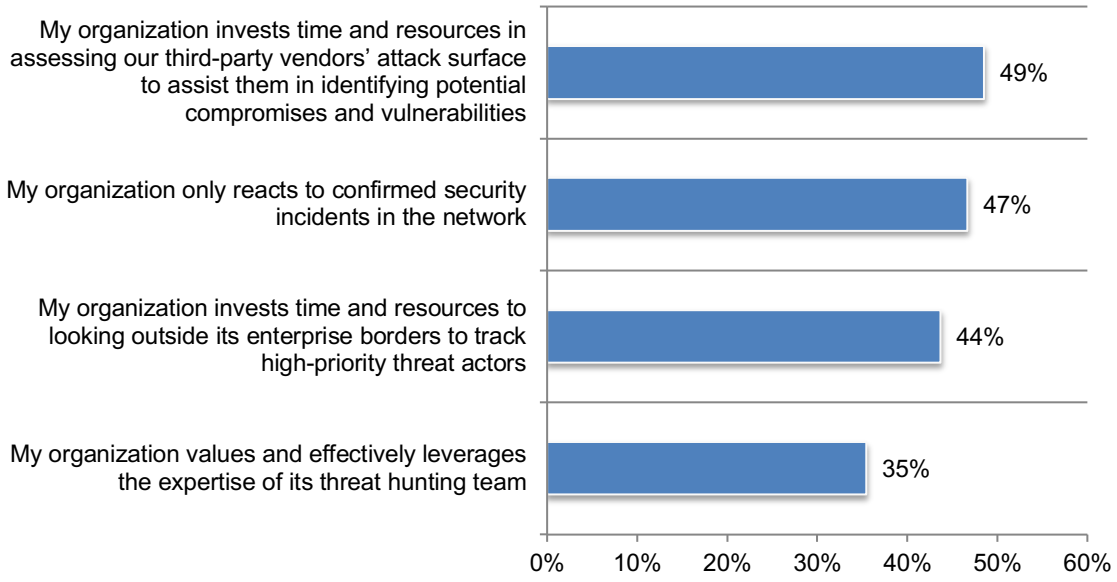


The effectiveness of threat hunters and cyber reconnaissance

Most organizations are yet to fully realize the value of and effectively leverage the expertise of their threat hunting team. As shown in Figure 15, only 35 percent of respondents say the abilities of threat hunters are valued and leveraged effectively. On average, organizations have seven people on the analyst team and of these an average of five are dedicated to threat hunting. The person most likely to lead the threat hunting team is the IT security practitioner (37 percent of respondents) or the IT practitioner (35 percent of respondents). On average, 30 percent of security incidents are uncovered by threat hunters.

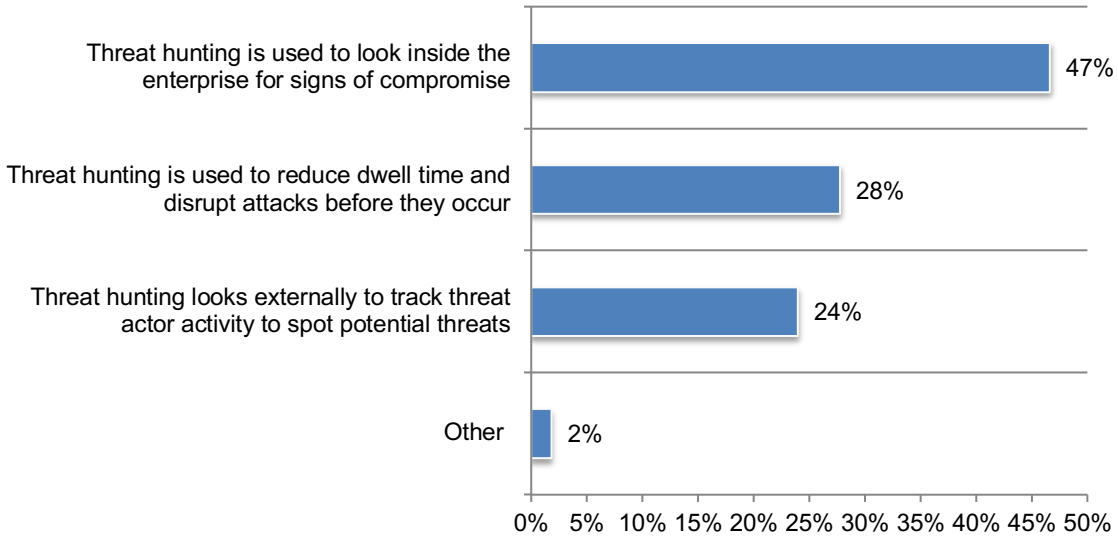
A significant barrier to a strong cybersecurity posture is that almost half (47 percent) of respondents) say their organizations only react to confirmed security incidents in the network. In addition, less than half of organizations (49 percent of respondents) are investing time and resources in assessing their third-party vendors' attack surface to assist them in identifying potential compromises and vulnerabilities and only 44 percent of respondents say their organizations invest time and resources to looking outside its enterprise borders to track high-priority threat actors.

Figure 15. Perceptions about the effectiveness of threat hunting
Strongly agree and Agree responses combined



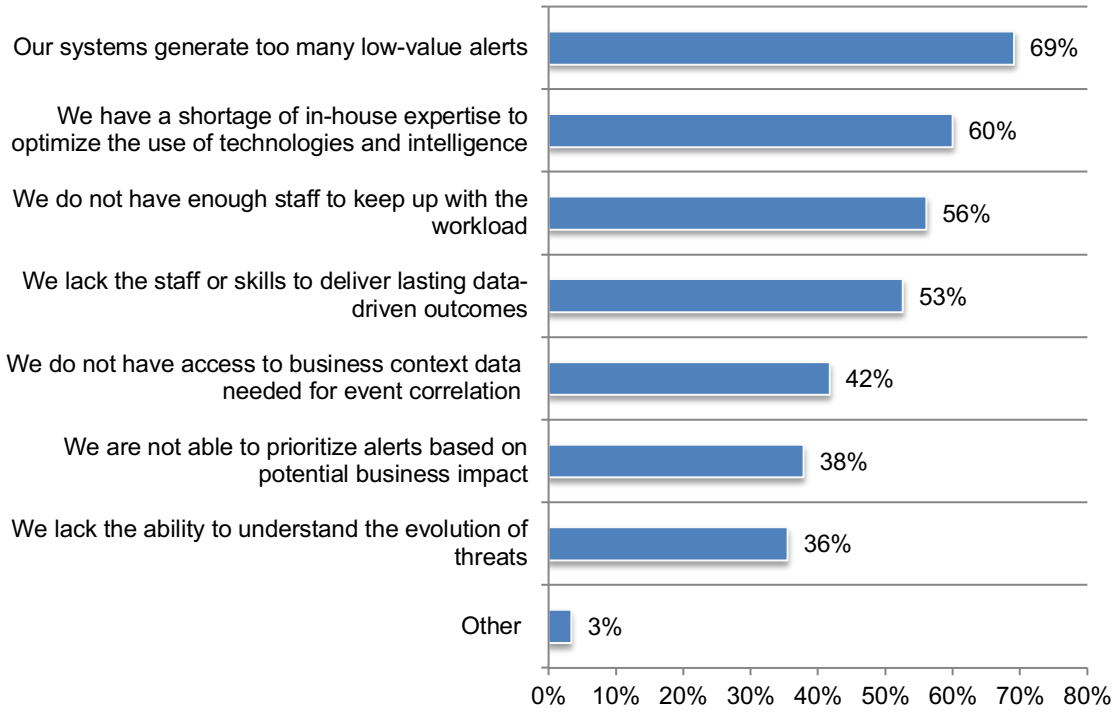
The primary reason for conducting threat hunting is to look inside the enterprise for signs of compromise. As shown in Figure 16, 47 percent of respondents say they conduct threat hunting to look inside the enterprise for signs of compromise followed by 28 percent of respondents who say threat hunting is used to reduce dwell time and disrupt attacks before they occur. Only 24 percent of respondents say threat hunting looks externally to track threat actor activity to spot potential threats.

Figure 16. Why does your organization conduct threat hunting?



The lack of staff and in-house expertise affects the cybersecurity posture of organizations. While systems generate too many low-value alerts, according to 69 percent of respondents, the other challenges are the lack of in-house expertise and skills. As shown in Figure 17, 60 percent of respondents say their organizations have a shortage of in-house expertise to optimize the use of technologies and intelligence, 56 percent of respondents say their organizations do not have enough staff to keep up with the workload and 53 percent of respondents say there is a lack of staff and skills to deliver lasting data-driven outcomes.

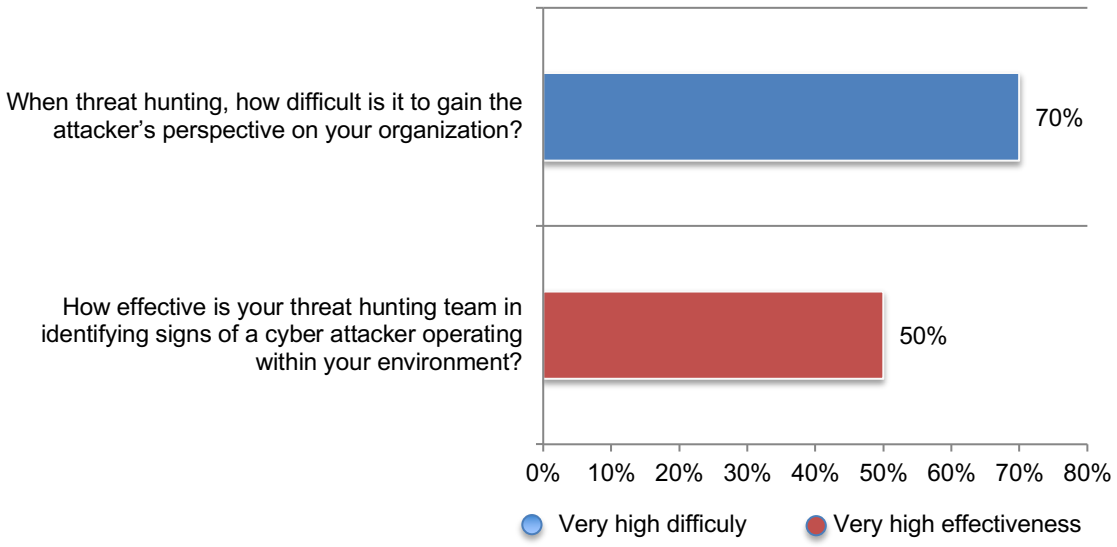
Figure 17. What are the biggest challenges security analysts face when supporting incident response processes?
More than one response permitted



Respondents were asked to rate the difficulty in gaining the attacker's perspective on the organization and the effectiveness of the threat hunting team in identifying signs of a cyber attacker operating within the environment on a scale from 1 = no difficulty/low effectiveness to 10 = high difficulty/high effectiveness. Figure 18 shows the high difficulty and high effectiveness responses (7+ on the 10-point scale).

As shown, 70 percent of respondents rate the difficulty in gaining the attacker's perspective on their organizations as very high. Only half (50 percent) of respondents rate the effectiveness of identifying signs of a cyber attacker operating within their organization as very high.

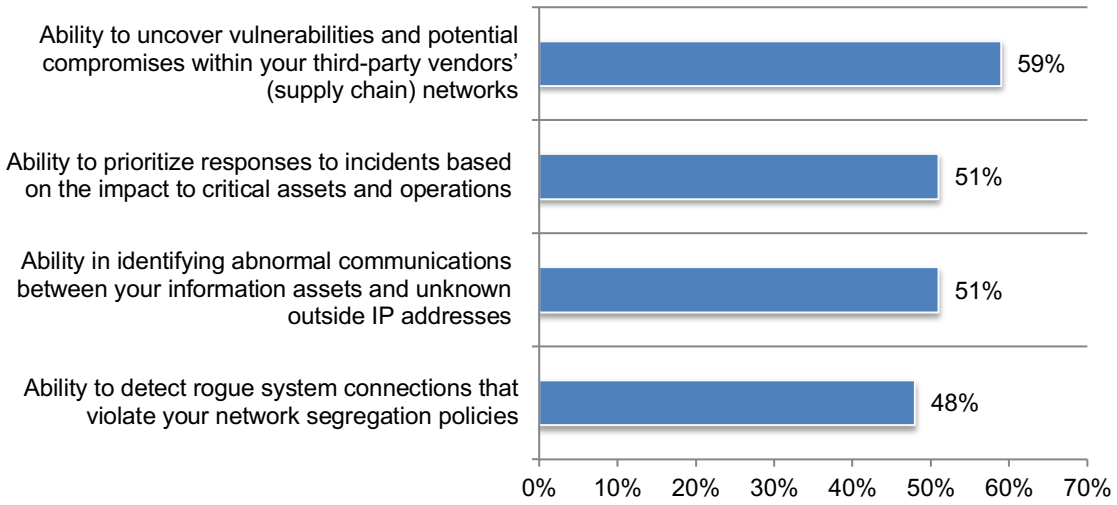
Figure 18. Challenges facing the threat hunting team
On a scale from 1 = not difficult/not effective to 10 = extremely difficult/highly effective, 7+ responses presented



Threat hunting teams are most confident in their ability to uncover vulnerabilities and potential compromises within their third-party vendors' networks. Respondents were asked to rate their threat team's ability to accomplish certain security objectives on a scale from 1 = no ability to 10 = high ability. Figure 19 shows the high ability responses (7+ on the 10-point scale).

Fifty-nine percent of respondents rate the ability to uncover vulnerabilities and potential compromises in third-parties' networks. Slightly more than half (51 percent) of respondents rate the ability to identify abnormal communications between their information assets and unknown outside IP addresses as high. The same percentage of respondents rate the ability to prioritize responses to incidents based on the impact to critical assets and operations as high. Less than half (48 percent) of respondents rate the ability to detect rogue system connections that violate network segregation policies as high.

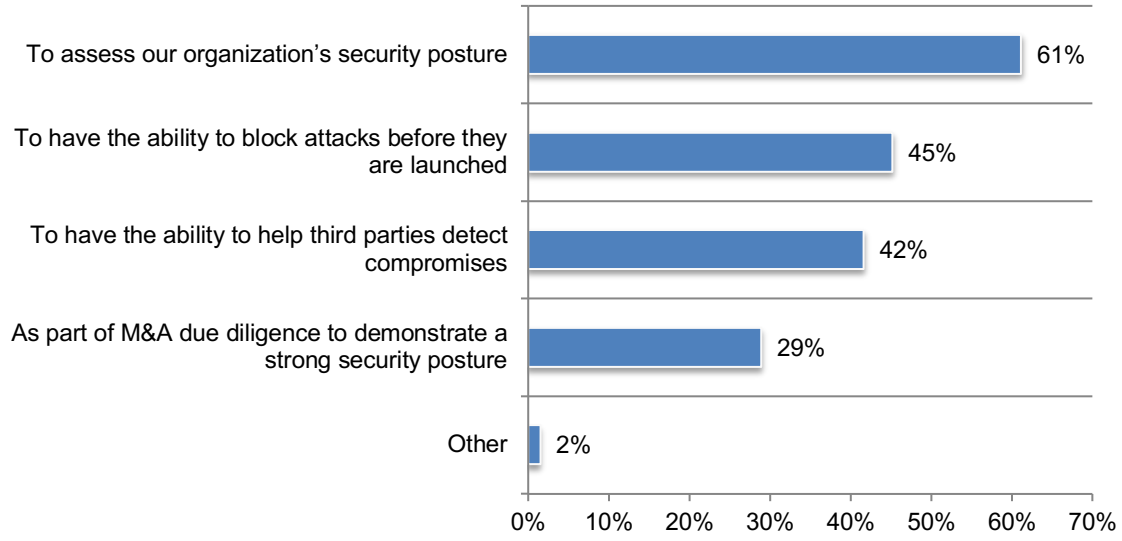
Figure 19. Perspectives of the threat hunting team's abilities
On a scale from 1 = no ability to 10 = high ability, 7+ responses permitted



Threat reconnaissance (external threat hunting) in this research is defined as the use of seeds of intelligence such as IP addresses or domain names to trace, map and monitor adversary infrastructures beyond the organization's perimeter. Its purpose is to view an organization and its connected third parties from the perspective of external threat actors, while directly observing their malicious activity to extract greater context around threats and to be in a position to identify signs of impending attacks. The objective is to optimize risk management and adapt an organization's defense against highly sophisticated threat actors.

According to Figure 20, the most significant benefit from cyber reconnaissance is the ability to assess their organization's security posture, according to 61 percent of respondents. This is followed by the ability to block attacks before they are launched (45 percent of respondents) and to have the ability to help third parties detect compromises (42 percent of respondents).

Figure 20. How would your organization benefit from greater visibility into malicious infrastructure referred to as cyber reconnaissance as defined above?
More than one response permitted



The importance of the Cyber Kill Chain in creating a strong security posture

The term **Cyber Kill Chain** refers to a cyberattack life cycle that allows information security professionals to align to a common method to proactively remediate and mitigate advanced threats as part of the organization's intelligence-driven defense process. This process is organized into seven discrete phases, summarized as follows:

1. Reconnaissance: The research, identification and selection of targets and vulnerabilities via scanning and other methods.

2. Weaponization: The attacker creates an attack that takes advantage of the vulnerabilities discovered during the reconnaissance phase.

3. Delivery: The transmission of the weapon to the targeted environment, often via email, websites, or USBs.

4. Exploitation: The attack is "detonated", exploiting vulnerabilities, such as an application, operating system or even a user.

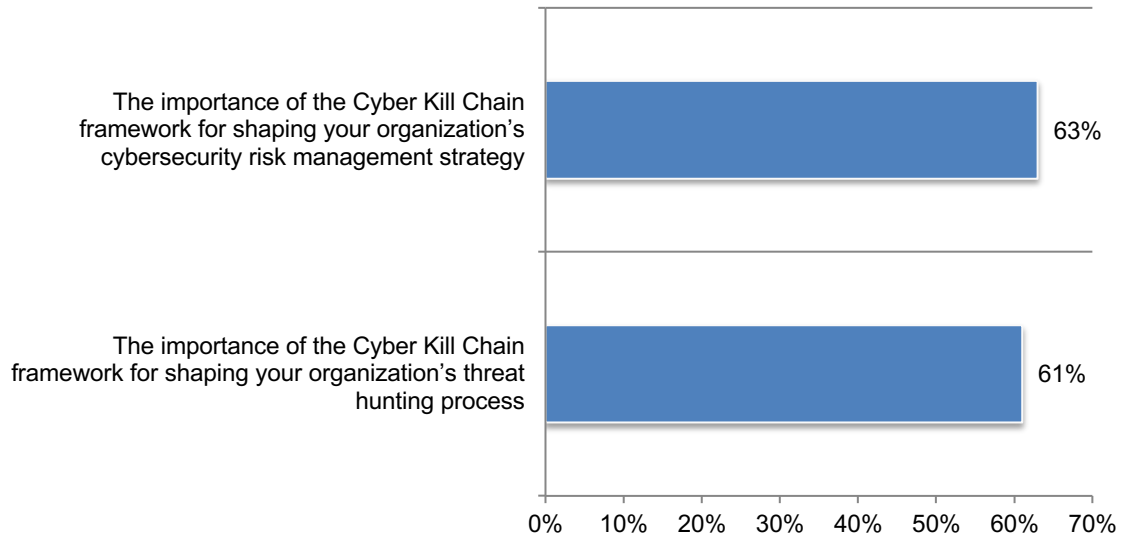
5. Installation: The point at which malicious code is installed.

6. Command and Control (C2): Establishing communication between the attacker and victim network. Often communications are routed through several proxies obfuscating the origin of the malicious communications.

7. Actions on Objectives: Once communication is established the attacker sends commands to achieve the original objectives (e.g. data exfiltration).

Forty-four percent of respondents say their organizations use the Cyber Kill Chain as part of their cybersecurity risk management strategy. Of these respondents, 63 percent of respondents say the Cyber Kill Chain is considered essential, very important or important in shaping their organizations' cybersecurity risk management strategy. Sixty-one percent of respondents say it is essential, very important or important to shaping their organizations' threat hunting process.

Figure 21. The importance of the Cyber Kill Chain to cyber risk management strategies and threat hunting
Essential, Very important and Important responses combined

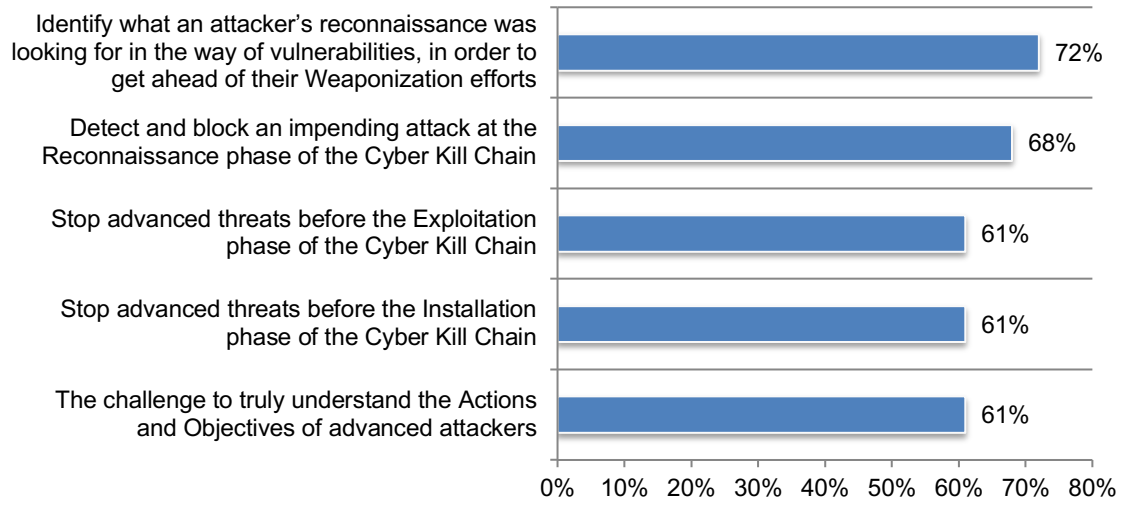


While the Cyber Kill Chain is considered important to organizations' cybersecurity posture, most respondents find it challenging to stop attacks in the 8 phases. Figure 22 presents the impossible and very difficult responses combined.

Following are the 5 phases that most respondents consider impossible and difficult to address.

- Seventy-two percent of respondents say it is impossible or very difficult to identify what vulnerabilities an attacker's reconnaissance was looking for in order to get ahead of their **Weaponization** efforts.
- Sixty-eight percent of respondents say it is impossible or very difficult to detect and block an impending attack at the **Reconnaissance** phase.
- Sixty-one percent of respondents say it is impossible or very difficult to stop advanced threats before the **Exploitation** phase.
- Sixty-one percent of respondents say it is impossible or very difficult to stop advanced threats before the **Installation** phase.
- Sixty-one percent of respondents say it is impossible or very difficult to understand the **Actions and Objectives** of **advanced attackers**?

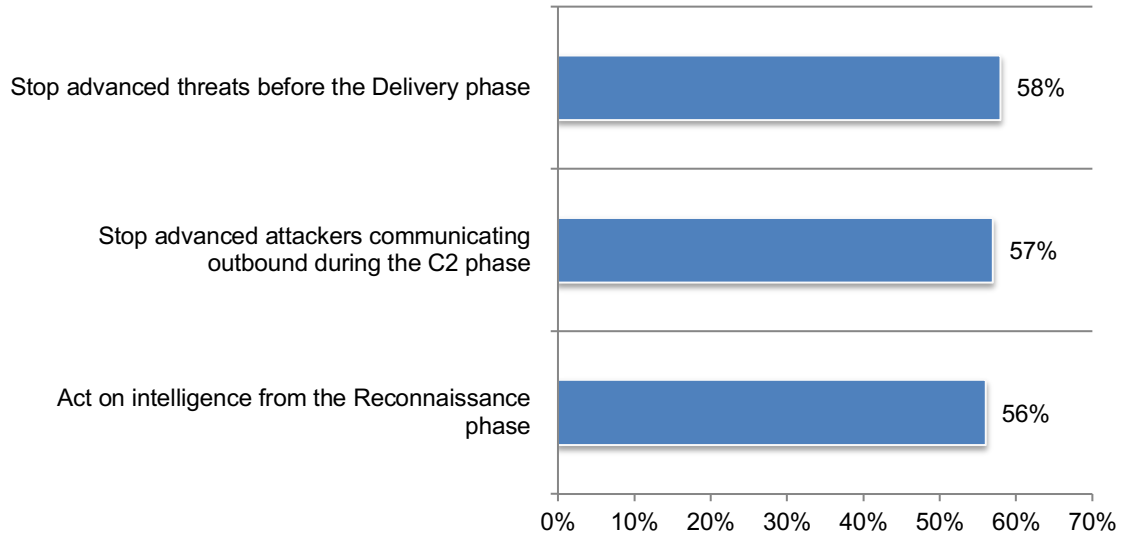
Figure 22. The 5 most difficult phases in the 7 phases of the Cyber Kill Chain
Impossible and Very difficult responses combined



Following are the 3 phases that more than half of respondents consider impossible and difficult to address.

- Fifty-eight percent of respondents say it is impossible or very difficult to stop advanced threats before the **Delivery** phase.
- Fifty-six percent of respondents say it is impossible or very difficult to act upon intelligence from the **Reconnaissance** phase.
- Fifty-seven percent of respondents say it is impossible or very difficult to stop **advanced attackers** communicating outbound during the **C2** phase.

Figure 23. The level of difficulty in the other 3 phases of the Cyber Kill Chain
Impossible and Very difficult responses combined



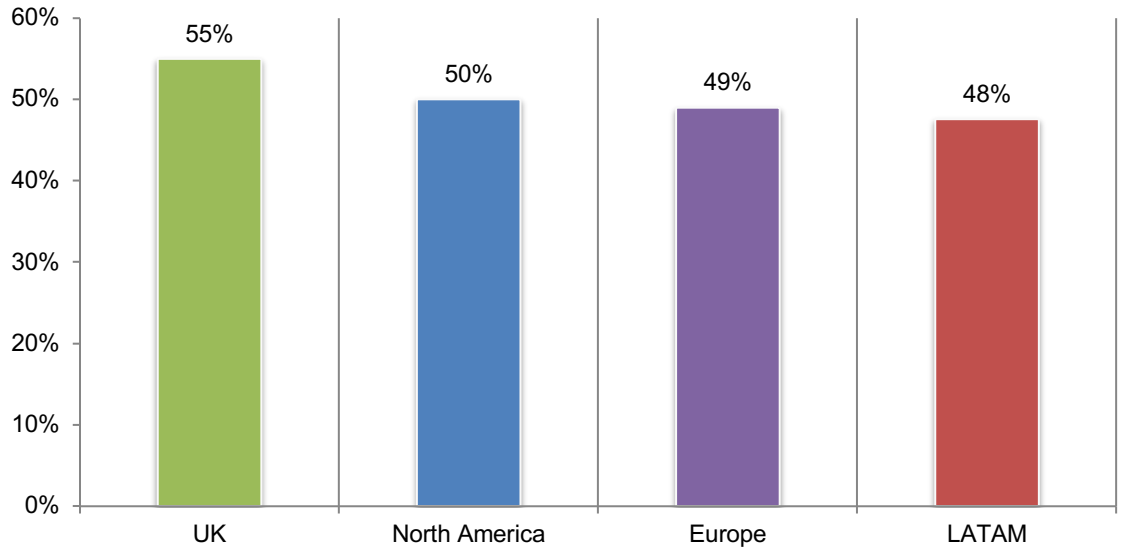
Differences among North America (NA), Latin America (LATAM), United Kingdom (UK) and Europe

In this section, we present differences in findings from organizations represented in North America (612 respondents), Latin America (347 respondents), United Kingdom (393 respondents) and Europe (426 respondents).

Many organizations globally are having recurring attacks from the same threat actor. Respondents were asked if their organization had a cybersecurity incident that resulted in a significant disruption to the IT and business processes in the past two years. Following is the percentage of organizations that had such an attack: NA (53 percent), LATAM (49 percent), UK (51 percent) and Europe (46 percent).

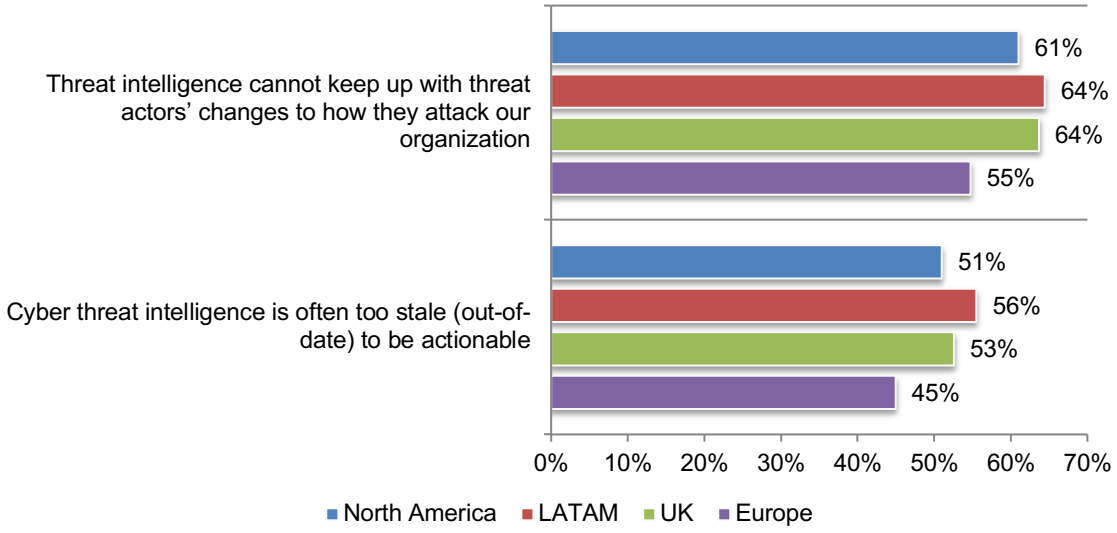
As shown in Figure 24, of these respondents in the UK, 55 percent say it was the result of an inability to prevent the recurrence of an attack from the same threat actor. Fifty percent of NA respondents, 49 percent of European respondents and 48 percent of LATAM respondents say this was the case.

Figure 24. Were any cybersecurity incidents the result of an inability to prevent the recurrence of an attack from the same threat actor?
Yes responses presented



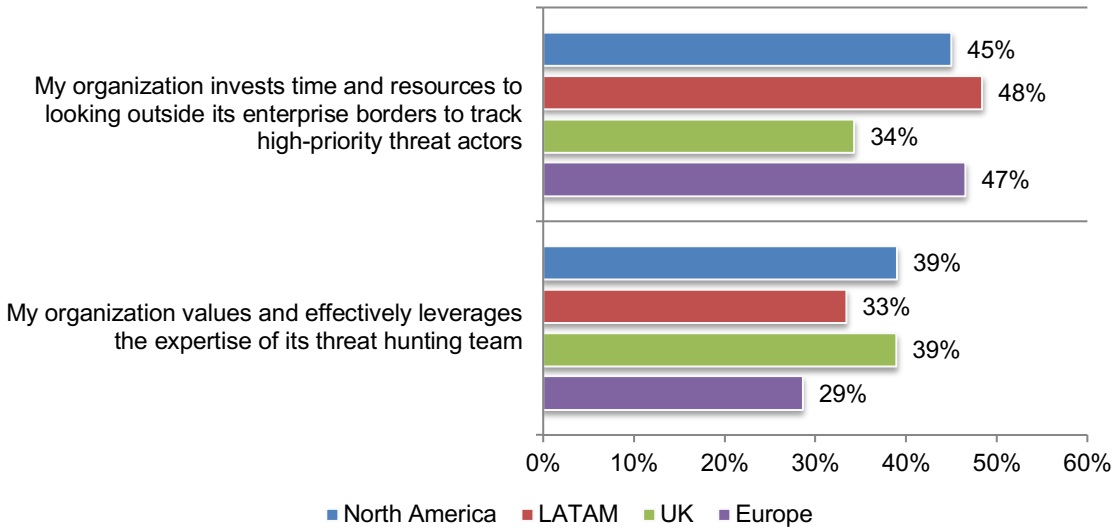
Globally, analysts cannot keep up with threat actors' changes to how they attack their organizations. According to Figure 25, 64 percent of respondents in LATAM and the UK say their threat intelligence cannot keep up with threat actors' changes to how they attack their organization. Fifty-six percent of respondents in LATAM say cyber threat intelligence is often too stale to be actionable.

Figure 25. Perceptions about threat intelligence
Strongly agree and Agree responses combined



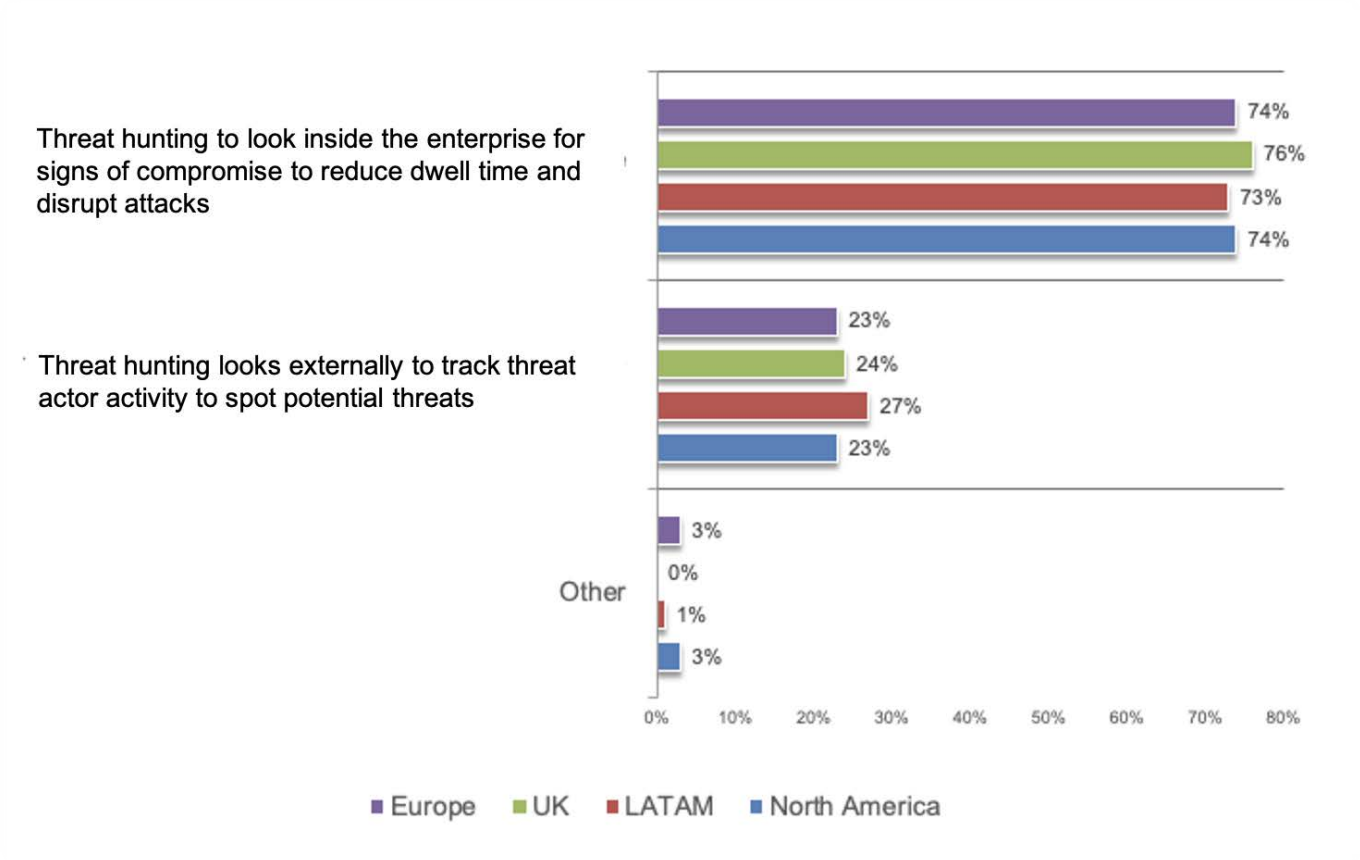
Globally, organizations are not valuing and leveraging the expertise of its threat hunting team. As shown in Figure 26, only 29 percent of respondents in Europe are say their organizations are valuing and using their threat hunting team as effectively as possible. Only 34 percent of respondents in the UK say their organization invests time and resources to looking outside its borders to track high-priority threat actors.

Figure 26. Perceptions about threat hunting
Strongly agree and Agree responses combined



Globally, organizations are mainly conducting threat hunting to look inside the enterprise for signs of compromise. As shown in Figure 27, most global organizations focus on looking inside the enterprise for signs of compromise. Very few are using external threat hunting to track threat actor activity, a method employed to interdict malicious infrastructure and predict attacks.

Figure 27. Why does your organization conduct threat hunting?
Only one choice permitted



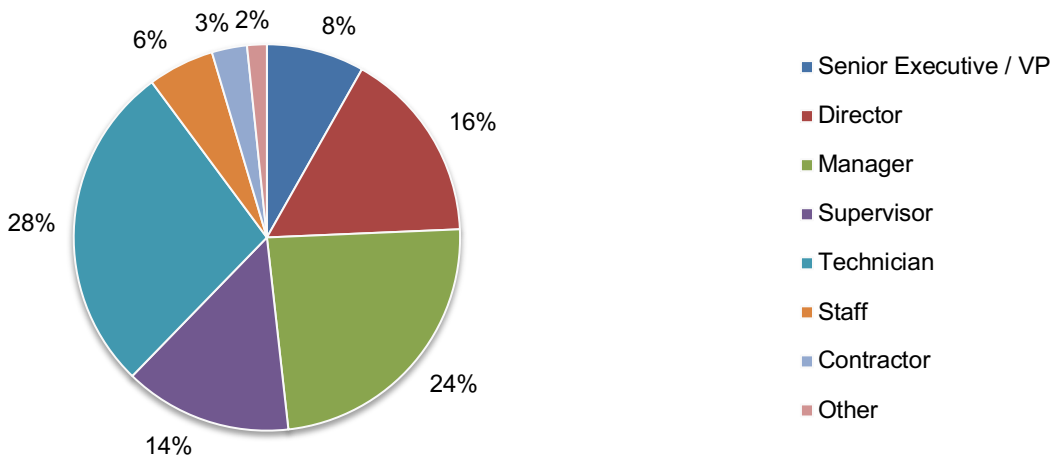
Part 3. Methodology

A sampling frame of 49,169 IT and IT security practitioners located in North America, Latin America, the United Kingdom, and Europe were selected as participants to this survey. Table 1 shows 1,987 total returns. Screening and reliability checks required the removal of 209 surveys. Our final sample consisted of 1,778 surveys (3.6 percent response rate). All organizations represented in this research have security/threat analysts gathering and/or using threat intelligence and engaging in threat hunting and/or cyber reconnaissance.

Table 1. Sample response	North America	LATAM	UK	Europe	Global
Total sampling frame	16,525	9,855	10,898	11,891	49,169
Total returns	681	394	436	476	1,987
Rejected or screened surveys	69	47	43	50	209
Final sample	612	347	393	426	1,778
Response rate	3.7%	3.5%	3.6%	3.6%	3.6%

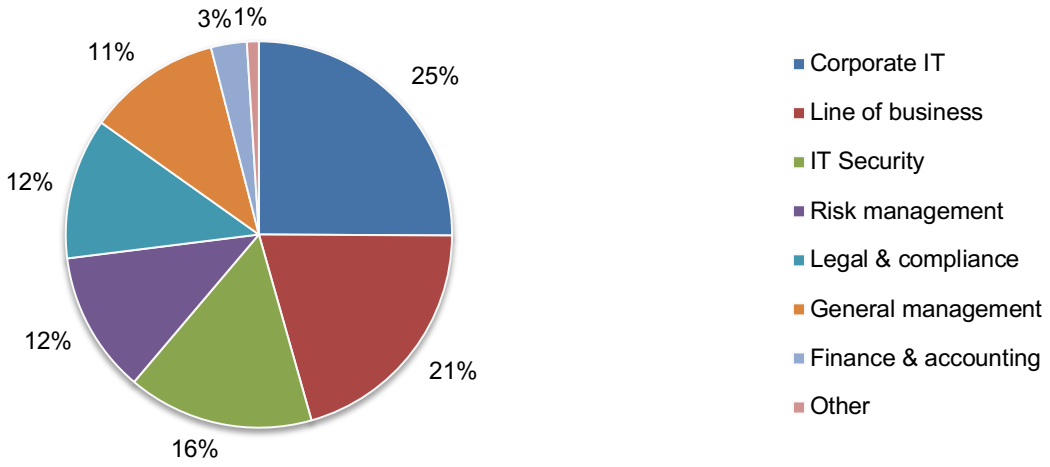
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (62 percent) of respondents are at or above the supervisory levels. Technician represents the largest segment at 28 percent of respondents.

Pie Chart 1. Current position within the organization



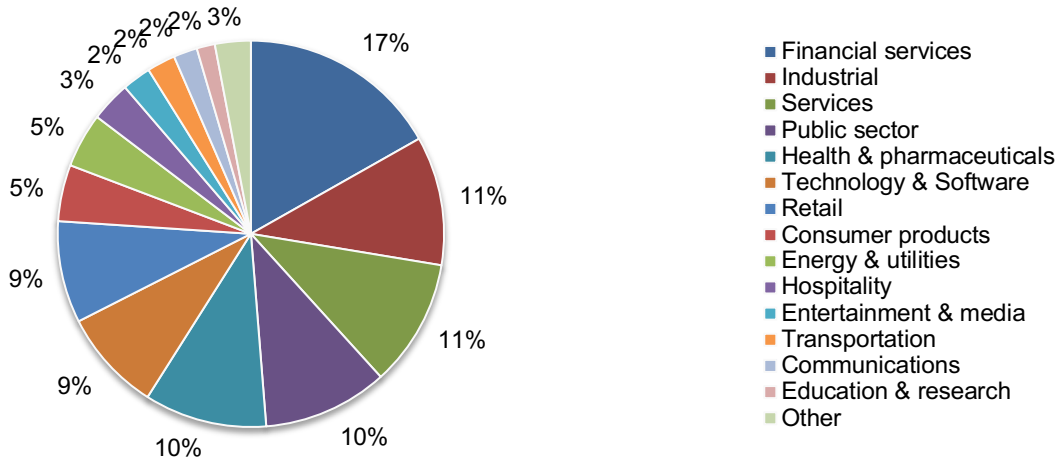
Pie Chart 2 reports that 25 percent of respondents reported their job function is located within corporate IT. Twenty-one percent of respondents are located within the line of business followed by 16 percent of respondents that are located in IT security.

Pie Chart 2. Department or function that best describes where respondents are located



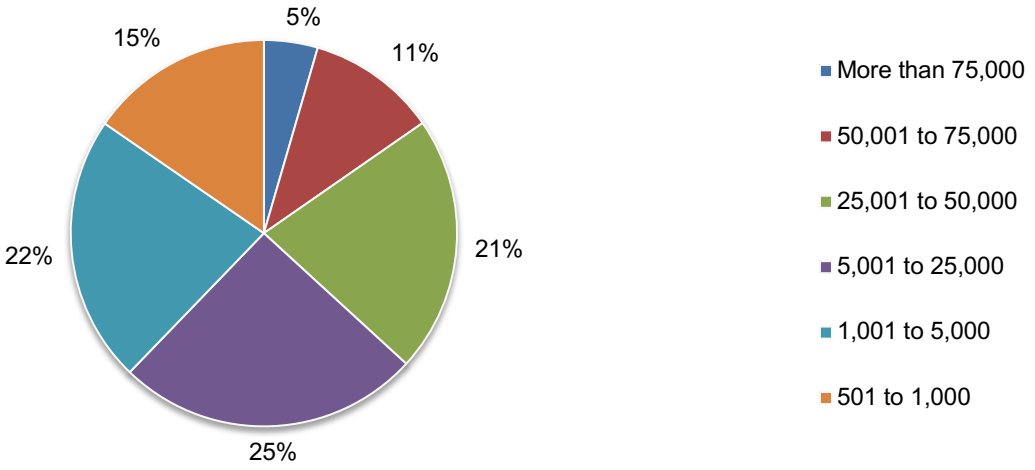
Pie Chart 3 reports the industry focus of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by followed by industrial (11 percent of respondents), services (11 percent of respondents), public sector (10 percent of respondents), and health and pharmaceuticals (10 percent of respondents).

Pie Chart 3. Industry focus of respondents' organizations



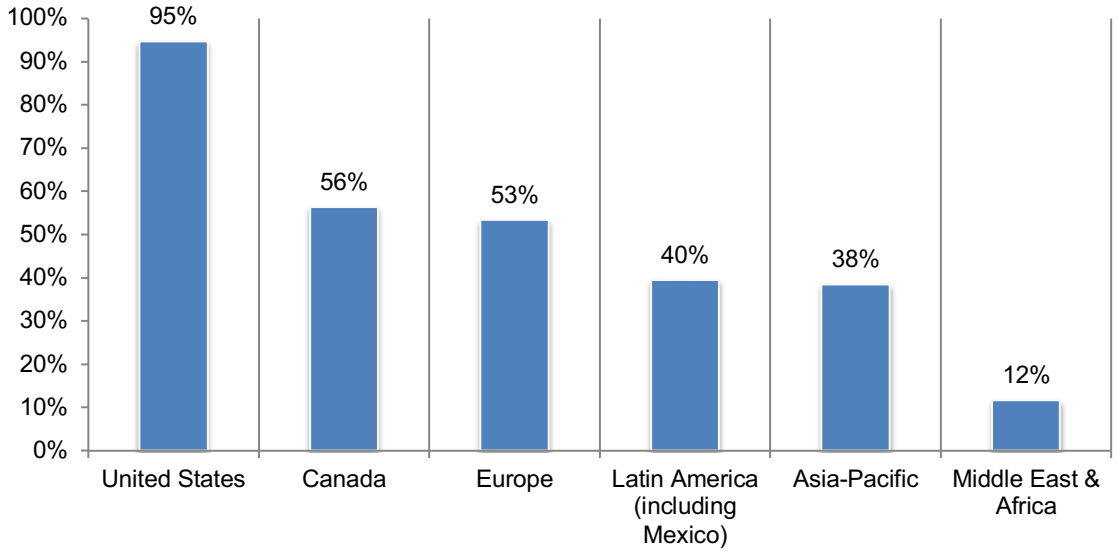
Sixty-two percent of respondents are from organizations with a global headcount of more than 5,000 employees, as shown in Pie Chart 4.

Pie Chart 4. Worldwide headcount of the organization



When asked where the employees are located, 95 percent of respondents indicated the United States, 56 percent of respondents identified Canada, 53 percent of respondents identified Europe, 40 percent of respondents said Latin America, 38 percent of respondents said Asia-Pacific and 12 percent of respondents said Middle East and Africa, as shown in Figure 28.

Figure 28. Location of employees
More than one response permitted



Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to al survey questions. All survey responses were captured in January 2021.

Survey response	Global
Total sampling frame	49,169
Total returns	1,987
Rejected or screened surveys	209
Final sample	1,778
Response rate	3.6%

Part 1. Screening

S1. Does your organization have security/threat analysts gathering and/or using threat intelligence?	Global
Yes	100%
No	0%
Total	100%

S2. Does your organization engage in threat hunting and/or cyber reconnaissance?	Global
Yes	100%
No	0%
Total	100%

S3. How familiar are you with how security analysts are used in your organization?	Global
Very familiar	41%
Familiar	33%
Somewhat familiar	16%
Not familiar (stop)	10%
Total	100%

S4. How are you involved in your company's cyber threat intelligence activities or process? Please select all that apply.	Global
User of threat intelligence	52%
Gatherer of threat intelligence	47%
Analyzer of threat intelligence	41%
Executive or manager in-charge of threat intelligence activities	52%
We do not use threat intelligence (stop)	25%
Total	218%

Part 2. Background

Q1. What best describes the maturity level of your organization's cybersecurity program or activities?	Global
Early stage – many cybersecurity program activities have not as yet been planned or deployed	14%
Middle stage – cybersecurity program activities are planned but only partially deployed	22%
Late-middle stage – many cybersecurity program activities are mostly deployed across the organization	31%
Mature stage – most cybersecurity program activities are successfully deployed, maintained and/or refined across the organization.	33%
Total	100%

Q2. What are the top security threats affecting your organization? Please select your top five choices.	Global
Phishing/social engineering attacks	52%
Hardware and system failures	26%
Remote worker endpoint security	40%
Browser-based attacks	27%
Ransomware	33%
Fileless malware	27%
Device vulnerabilities (such as IoT devices)	24%
Negligent insider threat	29%
Malicious insider threat	45%
Cloud vulnerabilities	65%
DNS-based attacks (such as DNS hijacking)	44%
Denial of service attacks	60%
Nation-state, terrorist or criminal syndicate sponsored attacks	25%
Other	2%
Total	500%

Q3. What tasks do security/threat analysts perform at your organization? Please select all that apply.	Global
Incident response investigations	40%
SIEM monitoring & alert response	42%
Information security policy enforcement	46%
Research and coordination with trusted industry groups	33%
Security infrastructure management	43%
Other	7%
Total	211%

Q4. Did your organization have a cybersecurity incident that resulted in a significant disruption to your organization's IT and business processes in the past two years?	Global
Yes	50%
No	48%
Unsure	2%
Total	100%

Q5a. If yes, were any of these incidents the result of an inability to prevent the recurrence of an attack from the same threat actor?	Global
Yes	50%
No	46%
Unsure	4%
Total	100%

Q5b. If yes, has your organization remediated the/those compromise(s)?	Global
Yes	39%
No	61%
Total	100%

Q6. In the next 12 to 24 months, what steps are most important to optimizing prevention, threat detection and incident response? Please select only one choice.	Global
Building a mature analyst team and providing it with access to raw threat intelligence	32%
Investing in automation, AI and machine learning	42%
Both are priorities	25%
Other	1%
Total	100%

Part 3. Threat intelligence

Q7. What is your organization's primary objective for the use of threat intelligence? Please select only one choice.	Global
To prevent attacks	32%
To quickly detect attacks	23%
To improve incident response	12%
To minimize false positives	12%
Enhance overall security posture	20%
All are equally important	2%
Total	100%

Q8a. Typically, what threat intelligence sources does your company use? Please select all that apply.	Global
Threat indicators (proceed to 8b)	53%
Indicators of compromise	60%
Reputation feeds	57%
Tactics, Techniques and Procedures Reports (TTPs)	48%
Other	3%
Total	220%

Q8b. If you are using threat indicators, which threat indicators provide the most valuable information? Please select all that apply.	Global
Malicious IP addresses	64%
Domain resolution/registration history	47%
Malware	42%
Malicious mobile apps	38%
Doppelganger Domain Monitoring	2%
Other	3%
Total	197%

Q9. Who is **most** responsible for deciding what threat intelligence sources are used? Please select only one choice.	Global
Chief Information Officer	11%
Chief Technology Officer	9%
Chief Financial Officer	1%
Chief Information Security Officer	18%
Chief Risk Officer	11%
Lines of business	19%
Leader of threat intelligence team	14%
No one function is most responsible	17%
Other	0%
Total	100%

Q10. What threat intelligence activities and technologies are most important in your ability to plan preventive measures, detect threats, and resolve security incidents? Please select the top four.	Global
Open source intelligence (OSINT) gathered manually via online sources	39%
Raw internet telemetry (e.g. network flows, passive DNS)	31%
Intelligence gathering through informal networking	41%
Relationships with law enforcement	26%
Participation in ISACs or other membership organizations	30%
Blacklists/whitelists or other structured data from technology vendors	43%
Commercial threat services or data feeds	46%
Open source threat feeds	46%
Threat intelligence from automation (technologies)	50%
A combination of human and machine-generated intelligence	44%
Other	3%
Total	400%

Q11. What are the threat intelligence data types that you have today? Please select all that apply.	Global
End Point Telemetry	42%
Domain registration	42%
Network infrastructure scanning / open ports	36%
Global Network IP Flows	37%
Passive DNS	32%
Dark Web Data	47%
None of the above	9%
Total	246%

Attributions about threat intelligence

Strongly Agree and Agree response combined	Global
Q12a. My organization's cyber threat intelligence is often too stale (out-of-date) to be actionable.	51%
Q12b. Cyber threat intelligence provided by vendors can be inaccurate or incomplete.	55%
Q12c. Threat intelligence cannot keep up with threat actors' changes to how they attack our organization.	61%
Q12d. Threat intelligence is not comprehensive enough to be actionable.	44%
Q12e. Threat intelligence contains too many data types with no standardized format to enable integration.	56%
Q12f. Some vendors withhold threat intelligence to drive further purchases.	32%
Q12g. Too many sources make it difficult to use threat intelligence.	59%

Part 4. Threat hunting

Strongly Agree and Agree resonse combined	Global
Q13a. My organization only reacts to confirmed security incidents in the network.	47%
Q13b. Proactive identification of impending cyber threats is critical to our security strategy.	55%
Q13c. Our analyst team closes gaps in our detection capabilities.	44%
Q13d. To achieve a strong cybersecurity posture, my organization believes it is important to invest in both automation and threat hunter in-house expertise.	59%
Q13e. My organization values and effectively leverages the expertise of its threat hunting team.	35%
Q13f. My organization invests time and resources to looking outside its enterprise borders to track high-priority threat actors.	44%
Q13g. Our cybersecurity team believes that persistent insider and external malicious actors may already be dwelling within the network.	37%
Q13h. My organization invests time and resources in assessing our third-party vendors' attack surface to assist them in identifying potential compromises and vulnerabilities.	49%
Q13i. My organization is increasing its investment in analysts and their access to threat intelligence, in order to improve prevention and detection.	62%

Part 5. The effectiveness of threat hunting and cyber reconnaissance

Q14a. What describes how threat hunting is conducted in your organization? Please select only one choice.	Global
Threat hunting is conducted in-house	40%
Threat hunting is outsourced to a third party	35%
Threat hunting is conducted in-house and partially outsourced	25%
Total	100%

Q15. Based on the survey definition, how would your organization benefit from greater visibility into malicious infrastructures ("cyber reconnaissance")? Please select all that apply.	Global
To assess our organization's security posture	61%
To have the ability to block attacks before they are launched	45%
To have the ability to help third parties detect compromises	42%
As part of M&A due diligence to demonstrate a strong security posture	29%
Other	2%
Total	178%

Q16. Why does your organization conduct threat hunting?	Global
Threat hunting is used to look inside the enterprise for signs of compromise	47%
Threat hunting looks externally to track threat actor activity to spot potential threats	24%
Threat hunting is used to reduce dwell time and disrupt attacks before they occur	28%
Other	2%
Total	100%

Q17. Does your organization have gaps in visibility across the following? Please check all that apply.	Global
Network segments	66%
Supply chain	56%
Acquired companies	21%
Cloud infrastructure	43%
Total	186%

Q18. What are the biggest challenges security analysts face when supporting incident response processes? Please select all that apply.	Global
Our systems generate too many low-value alerts	69%
We are not able to prioritize alerts based on potential business impact	38%
We do not have access to business context data needed for event correlation	42%
We lack the staff or skills to deliver lasting data-driven outcomes	53%
We do not have enough staff to keep up with the workload	56%
We have a shortage of in-house expertise to optimize the use of technologies and intelligence	60%
We lack the ability to understand the evolution of threats	36%
Other	3%
Total	356%

Q19a. How many people are on your analyst team?	Global
1 to 3	19%
4 to 5	26%
6 to 10	34%
More than 10	21%
Total	100%
Extrapolated value	6.72

Q19b. How many are fully dedicated to threat hunting?	Global
1 to 3	42%
4 to 5	30%
6 to 10	17%
More than 10	12%
Total	100%
Extrapolated value	4.70

Q20. Who leads the threat hunting team? Please select only one choice	Global
IT security analyst	26%
IT security practitioner	37%
IT practitioner	35%
Other	2%
Total	100%

Q21. What percentage of security incidents are uncovered by threat hunters? Please select all that apply	Global
Less than 5%	5%
5% to 10%	17%
11% to 25%	32%
26% to 50%	22%
More than 50%	24%
Total	100%
Extrapolated value	30%

Q22. When threat hunting, how difficult is it to gain the attacker's perspective on your organization on a scale from 1 = not difficult to 10 = extremely difficult.	Global
1 to 2	3%
3 to 4	9%
5 to 6	18%
7 to 8	36%
9 to 10	34%
Total	100%
Extrapolated value	7.28

Q23. What impact would a significant increase in the investment in a mature threat hunting team have on your organization's security posture on a scale from 1 = no impact to 10 = high impact?	Global
1 to 2	5%
3 to 4	12%
5 to 6	15%
7 to 8	31%
9 to 10	37%
Total	100%
Extrapolated value	7.21

Q24. How effective is your organization's threat hunting team in uncovering threats that have infiltrated the network and systems on a scale from 1 = not effective to 10 = highly effective?	Global
1 to 2	6%
3 to 4	9%
5 to 6	14%
7 to 8	37%
9 to 10	33%
Total	100%
Extrapolated value	7.13

Q25. How effective is your threat hunting team in identifying signs of a cyber attacker operating within your environment 1 = not effective to 10 = highly effective?	Global
1 to 2	6%
3 to 4	21%
5 to 6	23%
7 to 8	28%
9 to 10	22%
Total	100%
Extrapolated value	6.27

Following are questions about your organization's threat hunting ability

Q26. The ability of the threat hunting team in identifying abnormal communications between your information assets and unknown outside IP addresses on a scale from 1 = no ability to 10 = high ability.	Global
1 to 2	4%
3 to 4	18%
5 to 6	28%
7 to 8	26%
9 to 10	25%
Total	100%
Extrapolated value	6.49

Q27. The ability of the threat hunting team to prioritize responses to incidents based on the impact to critical assets and operations on a scale from 1 = no ability to 10 = high ability.	Global
1 to 2	6%
3 to 4	19%
5 to 6	24%
7 to 8	28%
9 to 10	23%
Total	100%
Extrapolated value	6.39

Q28. The ability to detect rogue system connections that violate your network segregation policies 1 = no ability to 10 = high ability.	Global
1 to 2	11%
3 to 4	19%
5 to 6	22%
7 to 8	26%
9 to 10	22%
Total	100%
Extrapolated value	6.13

Q29. The ability to uncover vulnerabilities and potential compromises within your third-party vendors' (supply chain) networks on a scale from 1 = no ability to 10 = high ability?	Global
1 to 2	11%
3 to 4	17%
5 to 6	13%
7 to 8	24%
9 to 10	35%
Total	100%
Extrapolated value	6.59

Part 6. Cyber Kill Chain

Q30. Does your organization use the Cyber Kill Chain as part of its cybersecurity risk management strategy?	Global
Yes	44%
No	56%
Total	100%

Q31. How important is the Cyber Kill Chain framework for shaping your organization's cybersecurity risk management strategy?	Global
Essential	21%
Very important	28%
Important	14%
Somewhat important	17%
Not important	20%
Total	100%

Q32. How important is the Cyber Kill Chain framework for shaping your organization's threat hunting process?	Global
Essential	19%
Very important	26%
Important	16%
Somewhat important	20%
Not important	19%
Total	100%

Q33. In your opinion, how difficult is it detect and block an impending attack at the **Reconnaissance** phase of the Cyber Kill Chain?	Global
Impossible	34%
Very difficult	34%
Difficult	22%
Not difficult	9%
Easy	2%
Total	100%

Q34. In your opinion, how difficult is it to identify what an attacker's reconnaissance was looking for in the way of vulnerabilities, in order to get ahead of their **Weaponization** efforts?	Global
Impossible	34%
Very difficult	38%
Difficult	16%
Not difficult	9%
Easy	4%
Total	100%

Q35. Using the 10-point scale, how difficult would it be for your organization to act on intelligence from the **Reconnaissance** phase of the Cyber Kill Chain?	Global
Impossible	35%
Very difficult	21%
Difficult	25%
Not difficult	15%
Easy	5%
Total	100%

Q36. In your opinion, how difficult is it to stop **advanced threats** before the **Delivery** phase of the Cyber Kill Chain?	Global
Impossible	30%
Very difficult	28%
Difficult	18%
Not difficult	21%
Easy	4%
Total	100%

Q37. In your opinion, how difficult is it to stop **advanced threats** before the **Exploitation** phase of the Cyber Kill Chain?	Global
Impossible	36%
Very difficult	25%
Difficult	25%
Not difficult	12%
Easy	2%
Total	100%

Q38. In your opinion, how difficult is it to stop **advanced threats** before the **Installation** phase of the Cyber Kill Chain?	Global
Impossible	28%
Very difficult	33%
Difficult	16%
Not difficult	17%
Easy	6%
Total	100%

Q39. In your opinion, how difficult is it to stop **advanced attackers communicating outbound** during the **C2 phase** of the Cyber Kill Chain?	Global
Impossible	38%
Very difficult	19%
Difficult	21%
Not difficult	16%
Easy	6%
Total	100%

Q40. In your opinion, how challenging is it to truly understand the **Actions and Objectives** of **advanced attackers**?	Global
Impossible	37%
Very difficult	24%
Difficult	19%
Not difficult	18%
Easy	3%
Total	100%

Part 7. Budget

Q41. Approximately, what range best defines your organization's 2021 IT budget? **US$ millions**	Global
< $1 million	3%
$1 to 5 million	9%
$6 to $10 million	15%
$11 to $50 million	17%
$51 to $100 million	25%
$101 to $250 million	16%
$251 to $500 million	10%
> $500 million	4%
Total	100%
Extrapolated value	$ 117

Q42. Approximately, what percentage of the 2021 IT budget will be allocated to IT security activities?	Global
< 1%	3%
1% to 2%	5%
3% to 5%	10%
6% to 10%	12%
11% to 15%	14%
16% to 20%	18%
21% to 30%	17%
31% to 40%	9%
41% to 50%	6%
> 50%	4%
Total	100%
Extrapolated value	19%

Q43. Approximately, what percentage of the IT security budget will be allocated to analyst activities and threat intelligence?	Global
< 1%	3%
1% to 2%	5%
3% to 5%	9%
6% to 10%	8%
11% to 15%	14%
16% to 20%	20%
21% to 30%	14%
31% to 40%	11%
41% to 50%	9%
> 50%	7%
Total	100%
Extrapolated value	22%

Part 6. Role and organizational characteristics

D1. What organizational level best describes your current position?	Global
Senior Executive / VP	8%
Director	16%
Manager	24%
Supervisor	14%
Technician	28%
Staff	6%
Contractor	3%
Other	2%
Total	100%

D2. Check the department or function that best describes where you are located in your organization.	Global
General management	11%
Finance & accounting	3%
Legal & compliance	12%
Corporate IT	25%
Line of business	21%
Risk management	12%
IT Security	16%
Other	1%
Total	100%

D3. What industry best describes your organization's industry focus?	Global
Agriculture & food service	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	2%
Financial services	17%
Health & pharmaceuticals	10%
Hospitality	3%
Industrial	11%
Public sector	10%
Retail	9%
Services	11%
Technology & Software	9%
Transportation	2%
Other	1%
Total	100%

D4. Where are your employees located? Please choose all that apply.	Global
United States	95%
Canada	56%
Europe	53%
Middle east & Africa	12%
Asia-Pacific	38%
Latin America (including Mexico)	40%

D5. What is the worldwide headcount of your organization?	Global
501 to 1,000	15%
1,001 to 5,000	22%
5,001 to 25,000	25%
25,001 to 50,000	21%
50,001 to 75,000	11%
More than 75,000	5%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Insights Association,** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.