Ponemon INSTITUTE

The State of Threat Feed Effectiveness in the United States and United Kingdom

Sponsored by Neustar

Independently conducted by Ponemon Institute LLC

Publication Date: March 2021

Ponemon INSTITUTE

The State of Threat Feed Effectiveness in the United States and the United Kingdom

Ponemon Institute, March 2021

Part 1. Introduction

A deterrent to mitigating and preventing threats and malicious traffic, both inbound and outbound, is not having relevant, timely and actionable data. To solve this problem, according to this research, organizations are increasingly using threat feeds with insights from DNS data.

To understand the challenges and benefits of using threat data feeds, Ponemon Institute surveyed 1,025 IT and IT security practitioners in organizations that use threat data as part of their cybersecurity program or infrastructure in the United States and the United Kingdom. All respondents are familiar with their organization's approach to using threat data. Organizations in this research use an average of 21 threat feeds.

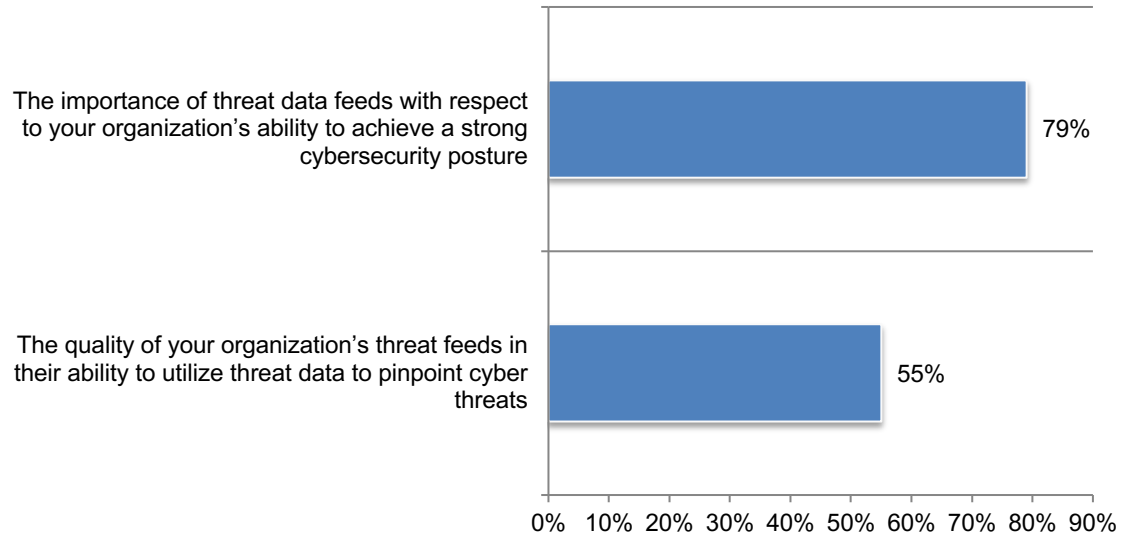
Threat intelligence feeds are the result of analysis and enrichment. The analysis and insights they provide helps security teams understand the threat landscape and focus their attention accordingly. Recent innovations in threat data feeds include collection of DNS data collected from distributed global sources, aggregating the data into easily consumable feeds and using AI and machine learning to analyze extremely large data sets. This data can be provided in near real time.

Threat feeds improve organizations' security posture. Respondents were asked to rate the importance of their threat feeds on a 10-point scale from irrelevant to essential and the quality of their threat feeds on a scale from low quality to high quality.

Figure 1 presents the 7+ responses (highly important and high quality). As shown, the overwhelming majority of respondents (79 percent) say threat data feeds are essential to achieving a strong cybersecurity posture. More than half of respondents (55 percent) are pleased with the quality of their organizations' threat feeds in the ability to use threat data to pinpoint cyber threats. Benefits of threat feeds can include timely delivery of data, threat data tailored to mitigate specific threats and flexible delivery methods.

Figure 1. The importance and quality of threat feeds

On a scale from 1 = low (irrelevant/low quality) to 10 = high (essential/ high quality), 7+ responses presented



The following findings reveal the current state of threat feed effectiveness

- Threat data feeds are important to an organization's cybersecurity strategy and more than half of respondents (55 percent) rate the quality of their threat feeds' ability to pinpoint cyber threats as very high. However, respondents also believe that the threat data they receive is too voluminous and complex to provide timely and actionable intelligence to identify potential threats before an attack is launched. Respondents believe an average of 50 percent of attacks can be stopped from intelligence threat feeds.

- SIEM integration is necessary to maximize the value of threat intelligence data. Almost half (49 percent of respondents) integrate threat data into their SIEM and 66 percent of these respondents say there is minimal or no diminishment of performance due to integration. Integration with SIEM, firewalls and WAF is considered very important for threat intelligence platforms.

- Seventy-one percent of respondents say the number one benefit of threat data feeds is the ability to add unique data to mitigate and prevent threats and malicious activity. Threat data feeds also increase preventative blocking to ensure better defense (63 percent of respondents) and reduce the mean time to detect and remediate an attack (55 percent of respondents).

- More than half of respondents (53 percent) say their organizations are very effective in leveraging unique data to better inform security, increase preventative blocking and minimize damage from cyber threats. However, only 39 percent of respondents say their organization is very effective in determining the location of a cyberattack.

- Organizations are challenged to keep up with increasingly sophisticated attacks, such as DNS tunneling and having the necessary in-house expertise to deal with these attacks. Sixty-five percent of respondents say their organizations track DNS traffic for malicious activity to obtain actionable, relevant timely threat data.

- Almost all respondents (83 percent) cite reducing the risk caused by anonymizing proxies that bypass legitimate security barriers as very difficult to mitigate. Sixty-three percent of respondents say mitigating the risk caused by phishing attacks is very difficult.

- Fifty-eight percent of respondents say their organizations deploy a threat intelligence platform and the primary benefit is that it helps pinpoint and prioritize IOCs (Indicators of Compromise) followed by the ability to streamline the collection of threat data.

Part 2. Key findings

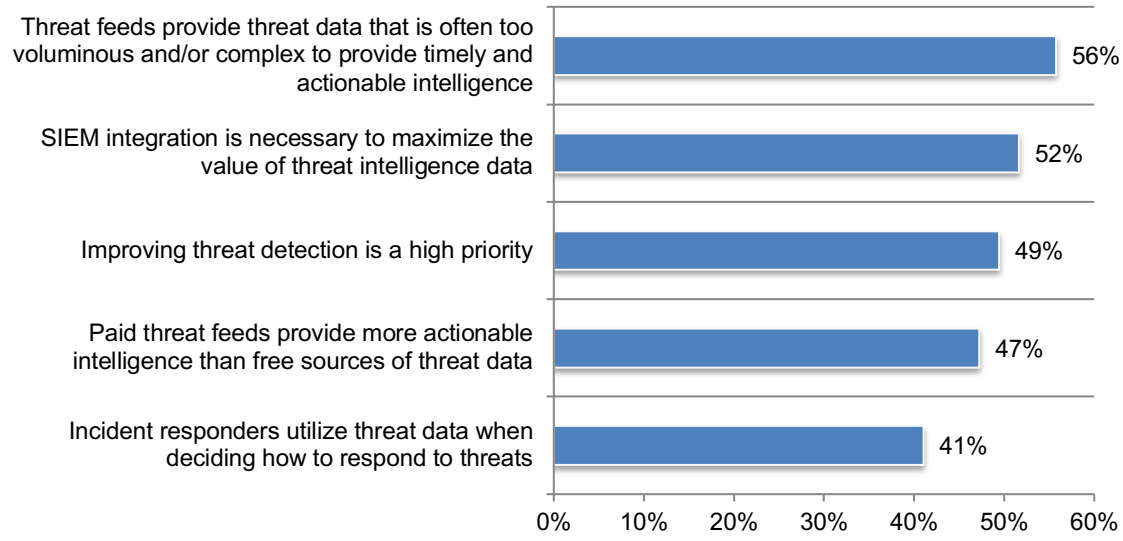
In this section, we provide an analysis of the research findings. The complete audited findings are presented in the Appendix of this report. The following topics are covered in this report.

- The use of threat feeds to improve organizations' security posture
- Threat intelligence platforms
- Industry differences
- Differences in organizational size

The use of threat feeds to improve organizations' security posture

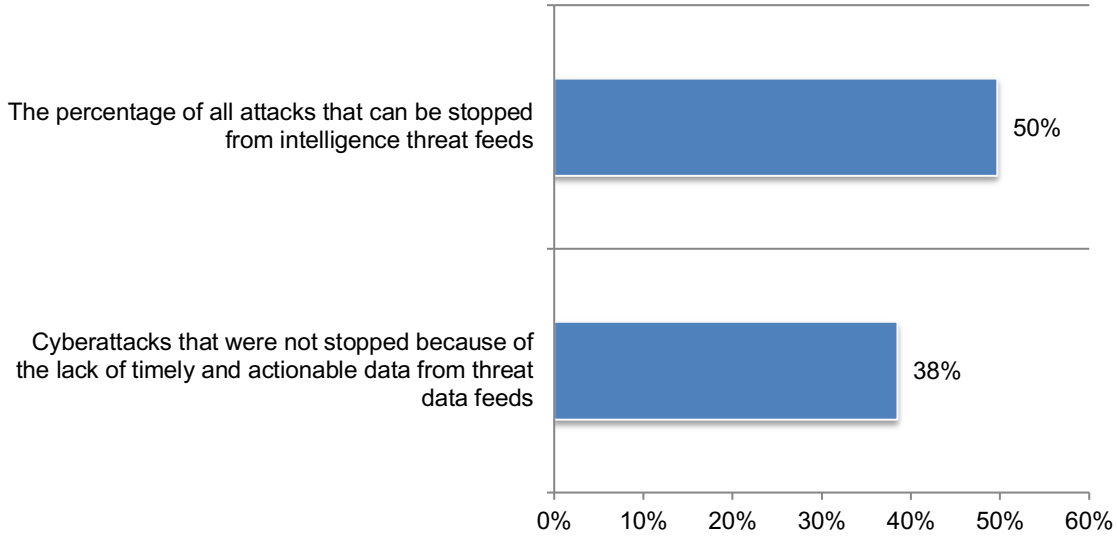
To improve an organization's security posture, threat data needs to become more actionable. As shown in Figure 2, 56 percent of respondents say a problem with threat feeds is that the threat data is often too voluminous and/or complex to provide timely and actionable intelligence. Fifty-two percent of respondents say SIEM integration is necessary to maximize the value of threat intelligence data. About half of respondents (49 percent) say their organizations are making threat detection a high priority.

Figure 2. Perceptions about threat data feeds
Strongly agree and agree responses combined



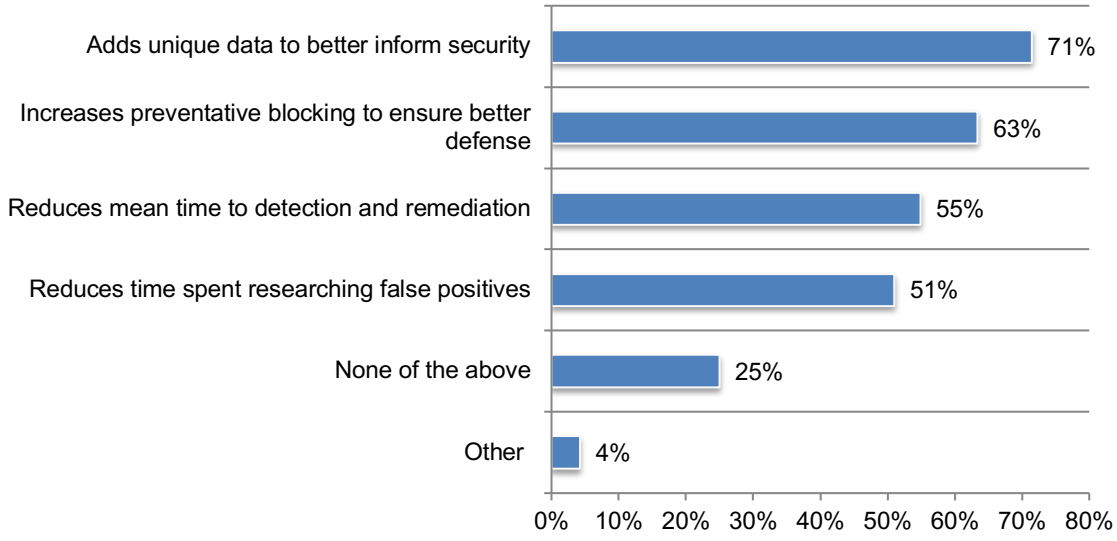
In the past two years, organizations represented in this research had an average of 28 cyberattacks. According to Figure 3, An average of 50 percent could be stopped, according to respondents, using timely and actionable intelligence from their threat feeds. However, an average of 38 percent of these cyberattacks were not stopped because of the lack of timely and actionable data from their data feeds.

Figure 3. The effectiveness of threat feeds in stopping cyberattacks
Extrapolated values presented



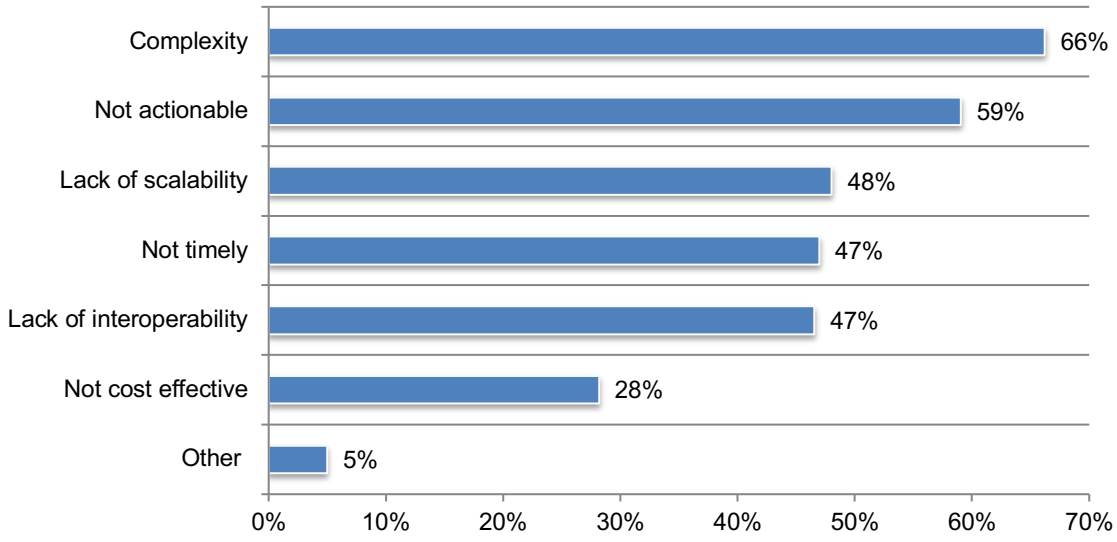
The benefit of threat data feeds is their ability to add unique data to mitigate and prevent threats and malicious activity. As discussed previously, 79 percent of respondents say threat data feeds are very important or essential to improving their organizations' security posture. According to Figure 4, the number one benefit is that threat feeds add unique data to better inform security (71 percent of respondents) followed by the increase in preventative blocking to ensure better defense (63 percent of respondents).

Figure 4. Benefits provided by organization's threat data feeds
More than one response permitted



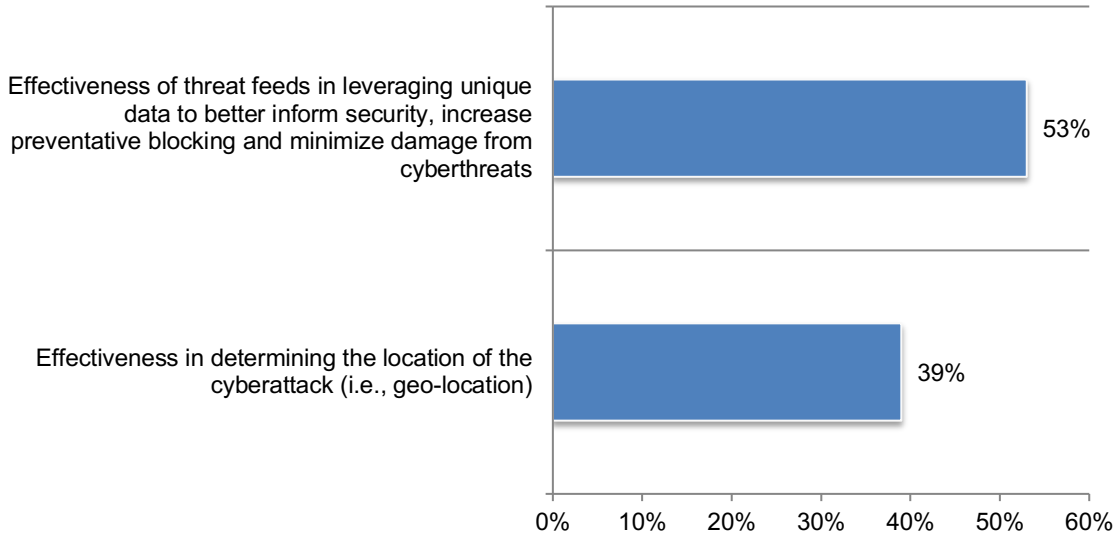
Complexity and not actionable threat data are the primary barriers of having effective threat data feeds. As shown in Figure 5, the primary barriers of having effective threat data feeds are complexity (66 percent of respondents) and intelligence from threat data feeds is not actionable (59 percent of respondents). Cost effectiveness does not seem to be so much of a barrier.

Figure 5. Barriers to having effective threat data feeds
Three responses permitted



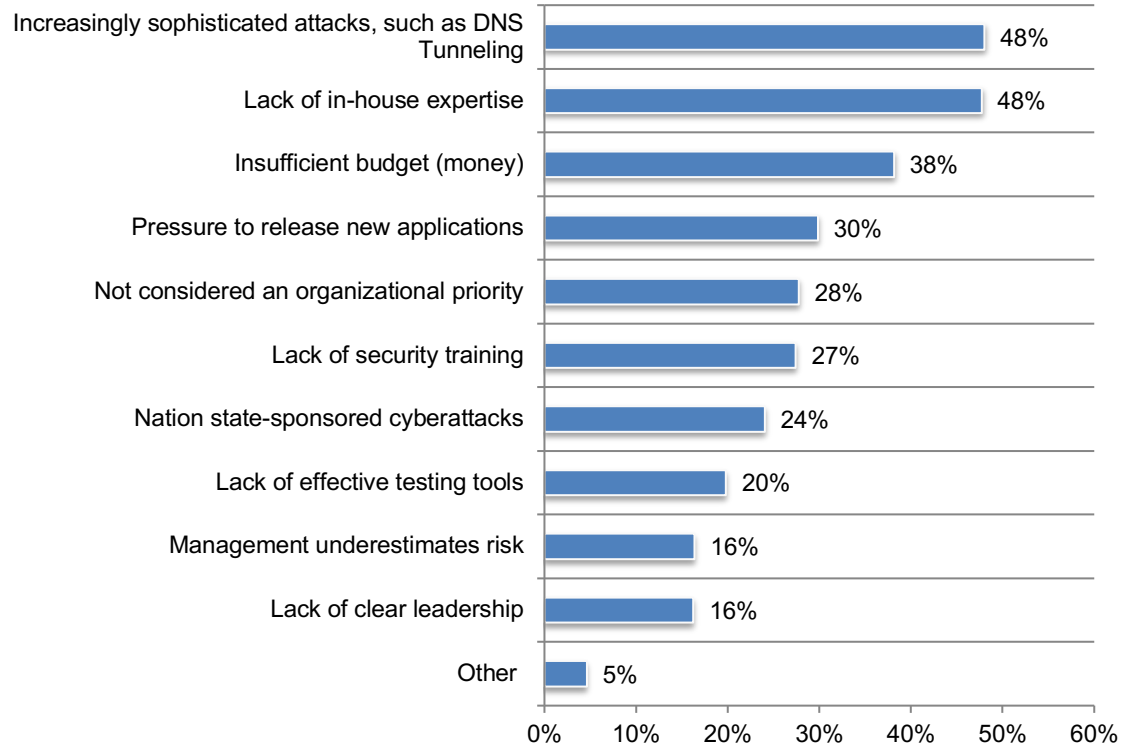
More than half of respondents (53 percent) say their organizations are effective in leveraging unique data important to improving their security posture. According to Figure 6, when asked to rate the effectiveness of the threat feeds in leveraging unique data to better inform security, increase preventative blocking and minimize damage from cyberthreats on a 10-point scale from 1= low (ineffective) to 10 = very effective. As shown in Figure 6, 53 percent of respondents say they believe their threat feeds are highly effective. However, only 39 percent of respondents say their organizations are very effective in determining the location of the cyberattack.

Figure 6. How effective are your organization's threat feeds in leveraging unique data to better inform security, increase preventative blocking and minimize damage from cyberthreats?
On a scale of 1 = low (ineffective) to 10 = high (very effective), 7+ responses presented



Increasingly sophisticated attacks and lack of in-house expertise prevent threat data feeds from being fully effective. Figure 7 presents a list of challenges that keep threat data feeds from being fully effective. Almost half of respondents (48 percent) say attacks such as DNS tunneling, which turn domain name systems (DNS) into a hacking weapon, is the number one challenge coupled with a lack of in-house expertise to address these increasingly sophisticated attacks.

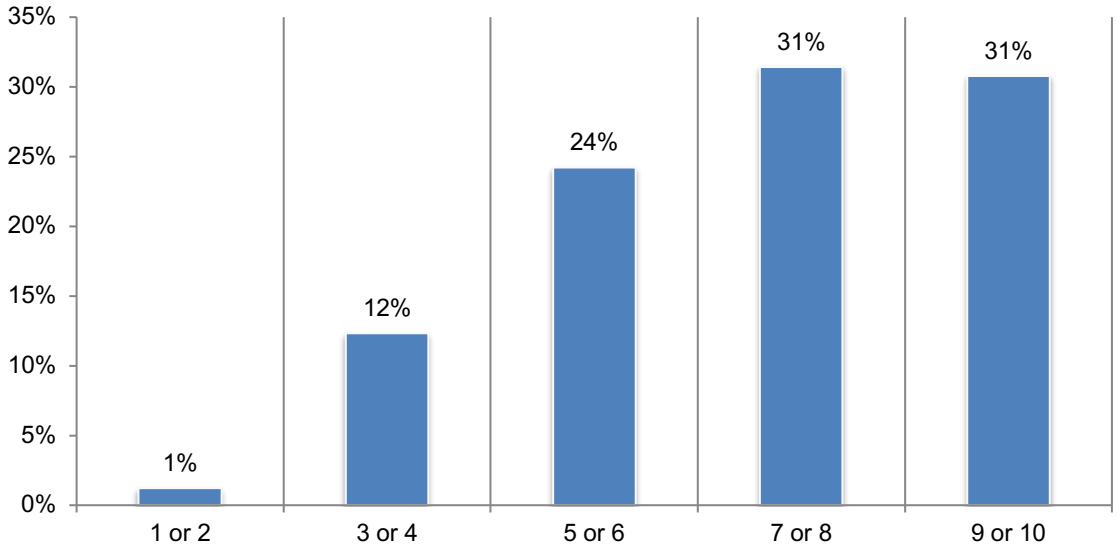
Figure 7. Challenges that keep threat data feeds from being fully effective
Three responses permitted



Security and convenience are critical to organizations' profitability. An average of 40 percent of the organizations' annual revenue represented in this study is from digital products and/or products sold online. These organizations have an average of 34 physical and virtual addresses. Because of the importance of security and convenience, we believe organizations are making these objectives a priority. As shown in Figure 8, 62 percent of respondents rate the ability to secure its online presence against risks while ensuring that customers have quality interactions as very high (31 percent + 31 percent).

Figure 8. The ability to secure its online presence against risks while ensuring that customers have quality interactions

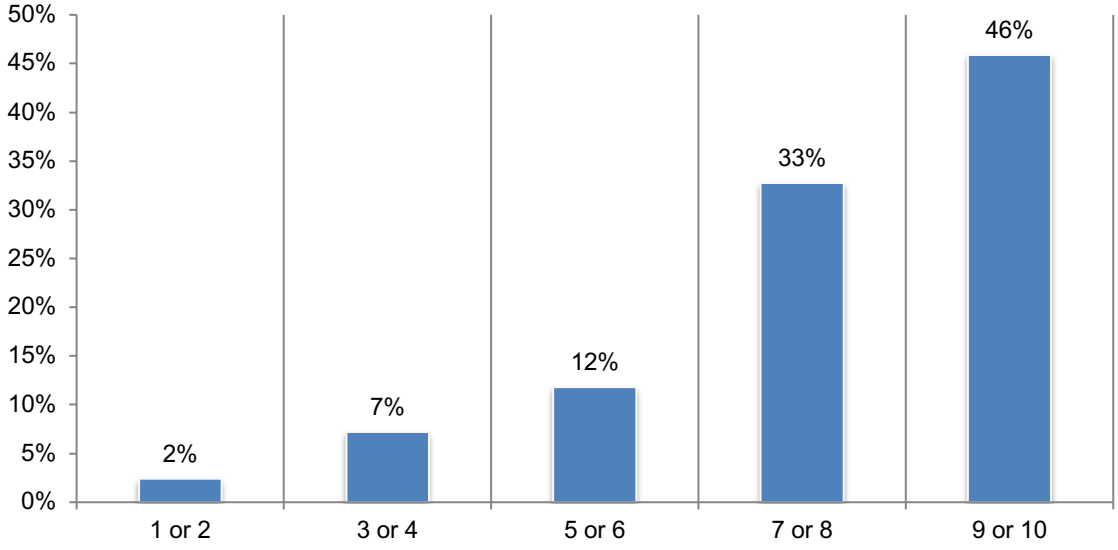
On a scale of 1 = low (ineffective) to 10 = high (very effective), extrapolated value = 7.1



Sixty-five percent of respondents say their organizations track DNS traffic for malicious traffic to obtain actionable, relevant and timely threat data. As discussed previously, attacks are getting more sophisticated making it difficult to have effective data threat feeds. According to Figure 9, 79 percent of respondents rate the difficulty in reducing risks caused by suspicious DNS Tunneling Attempts as very high (33 percent + 46 percent).

Figure 9. Difficulty in reducing risks caused by suspicious DNS Tunneling Attempts and by Domain or DNS hijacks

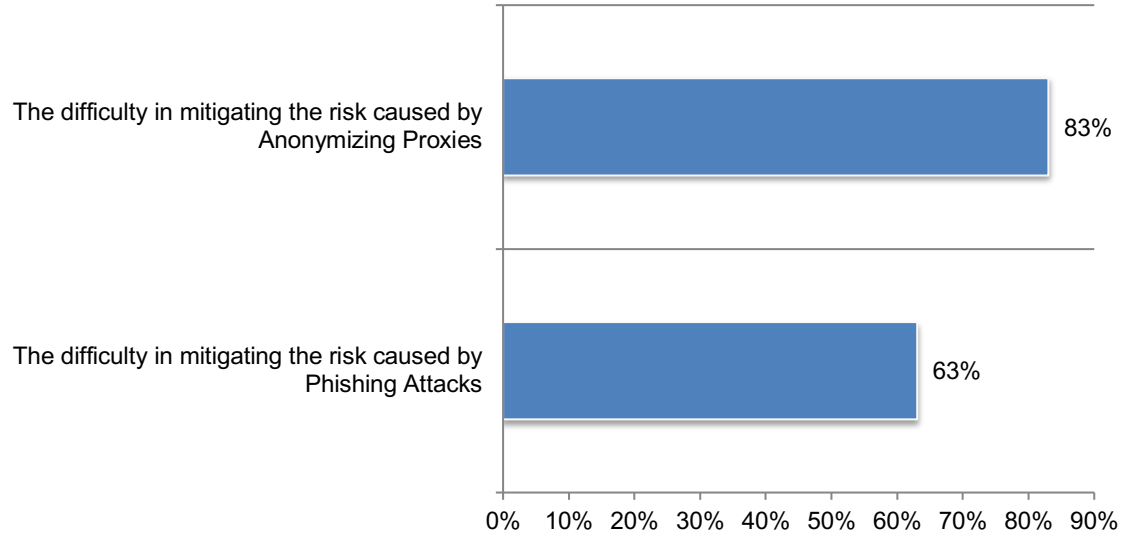
On a scale of 1 = low (not difficult) to 10 = high (very difficult), extrapolated value = 7.8



Almost all respondents cite reducing the risk caused by anonymizing proxies as very difficult to mitigate. In some cases, anonymizing proxies can be used to help minimize risk for web surfers by preventing identity theft or covering up browsing history. However, they also can be used to bypass legitimate security barriers and make it difficult to know who is operating and running anonymizing proxy servers.

Respondents were asked to rate the difficulty of reducing risks caused by anonymizing proxies on a scale of 1 = not difficult to 10 = very difficult. As shown in Figure 10, 83 percent of respondents say reducing the risk is very difficult (7+ responses). Sixty-three percent of respondents say mitigating risks caused by phishing attacks is very difficult.

Figure 10. The difficulty in mitigating the risk caused by phishing attacks and anonymizing proxies
On a scale of 1 = low (not difficult) to 10 = high (very difficult), 7+ responses presented

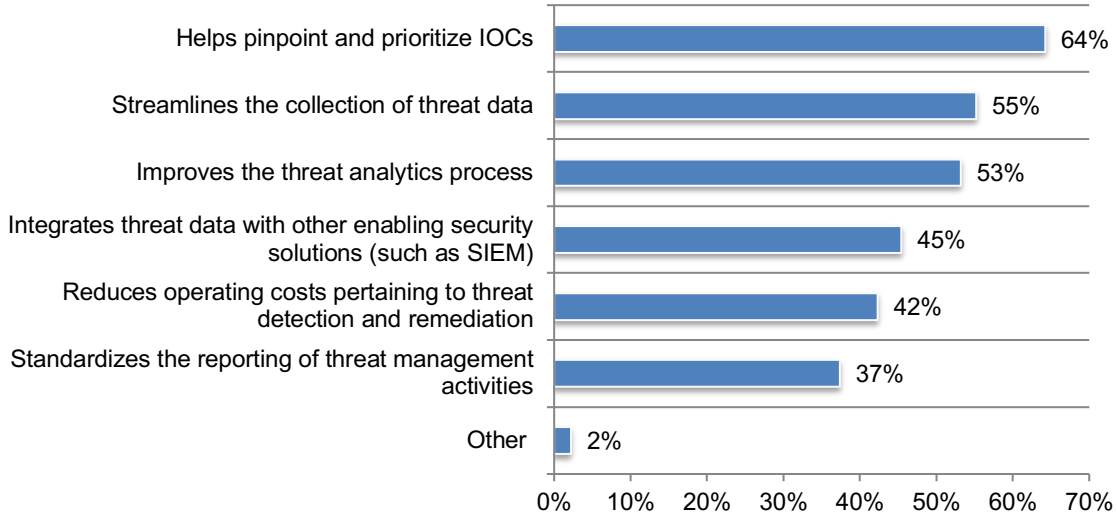


Threat intelligence platforms

Almost half (48 percent) of respondents say a threat intelligence platform is necessary to maximize the value of threat feeds. Threat intelligence platforms help organizations aggregate, correlate and analyze threat data from multiple sources in real time to support the organization's defensive actions.

Fifty-eight percent of respondents say their organizations deploy a threat intelligence platform and the primary benefit is that it helps pinpoint and prioritize IOCs (64 percent) followed by the ability to streamline the collection of threat data (55 percent) and improves the threat analytics process (53 percent), as shown in Figure 11.

Figure 11. What are the main benefits of having a threat intelligence platform?
Three responses permitted



According to Figure 12, organizations that do not deploy a threat intelligence platform say it is because of the lack of staff expertise (51 percent of respondents) and lack of technologies (47 percent of respondents).

Figure 12. Why doesn't your organization deploy a threat intelligence platform?
More than one response permitted

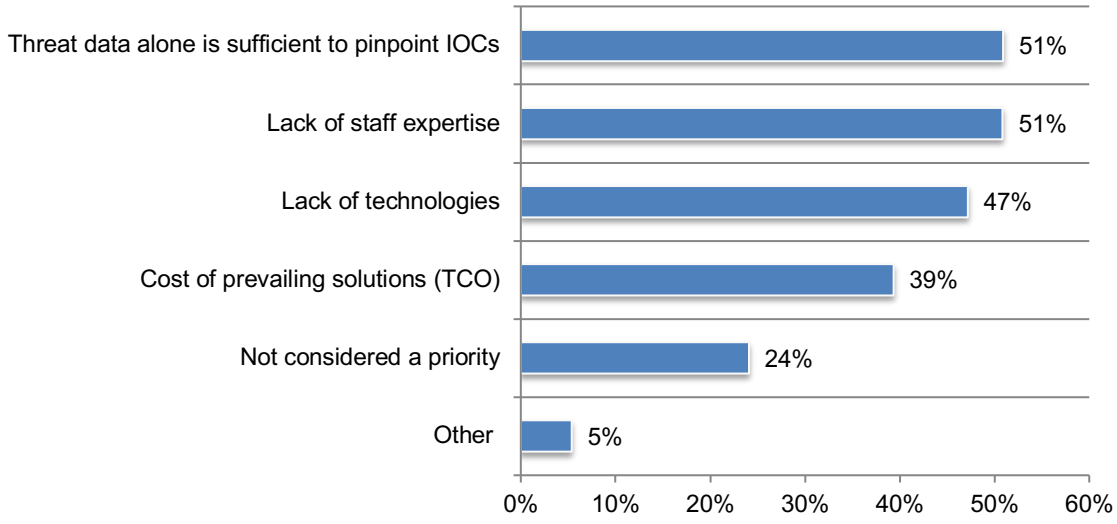
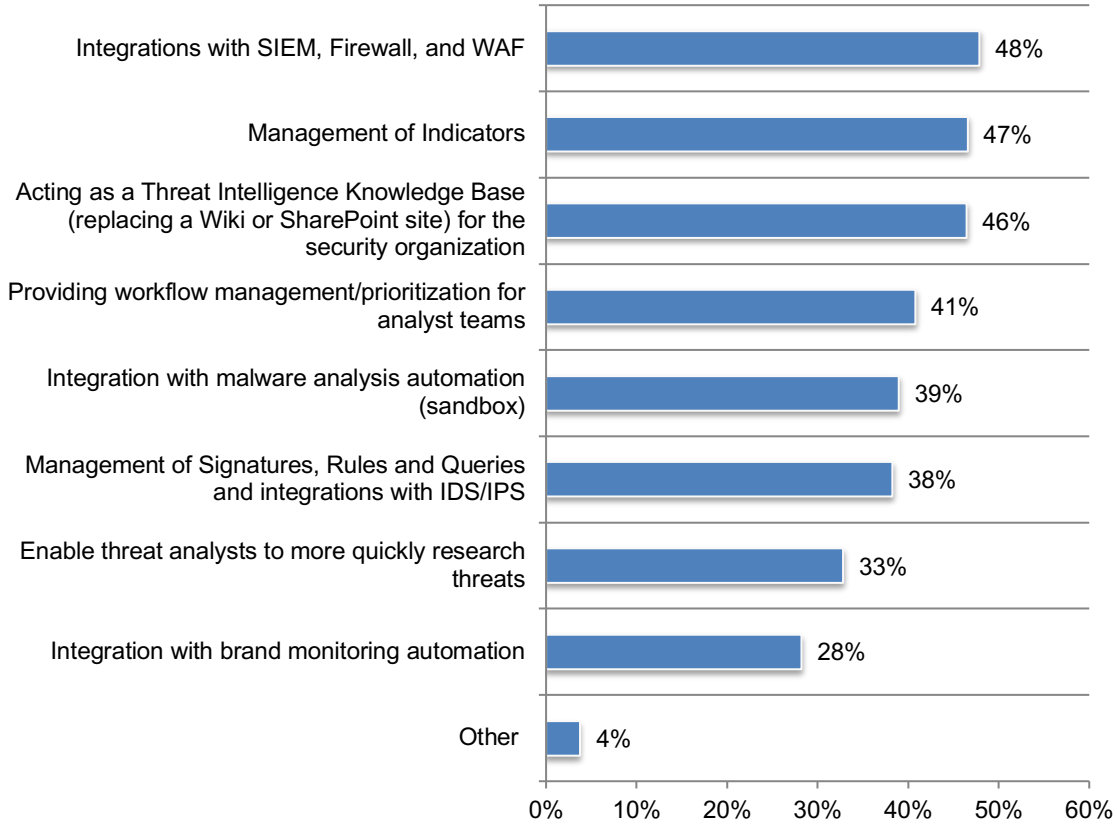


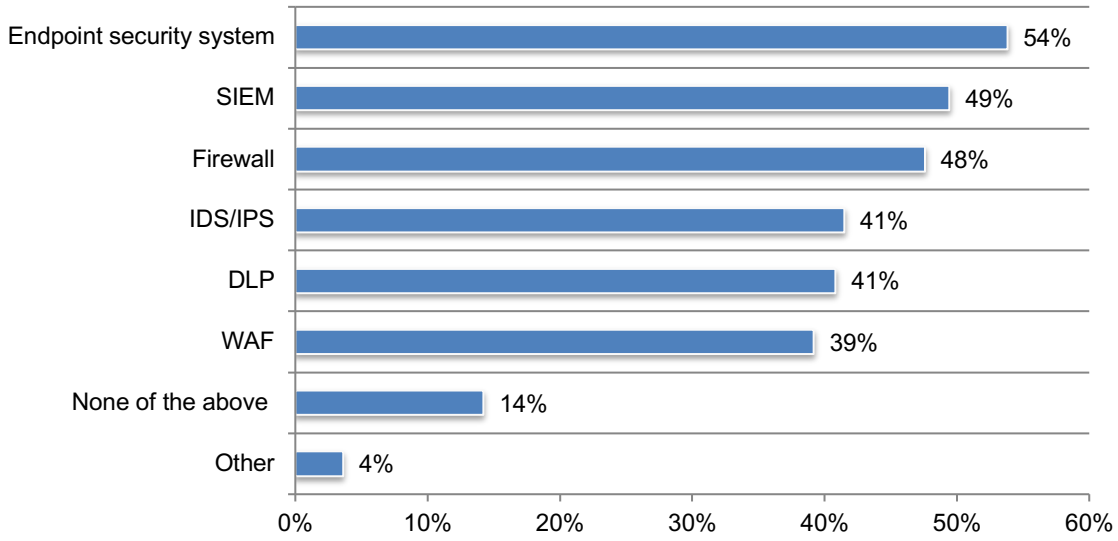
Figure 13 presents the features respondents considered most important for their threat intelligence platforms. As shown, integrations with SIEM, firewalls and WAF, management of indicators and acting as a threat intelligence knowledge base for the security organization.

Figure 13. Key functions contained in threat intelligence platforms considered most important
More than one response permitted



As shown in Figure 14, most threat data are integrated into endpoint security systems, SIEM and firewalls, according to 54 percent, 49 percent and 48 percent of respondents, respectively.

Figure 14. What parts of the security architecture does your organization integrate threat data into?
More than one response permitted



Almost half of respondents (48 percent) integrate threat data with their SIEMs. As shown in Figure 15, such integration results in only minimal diminishment (31 percent of respondents) or no diminishment (35 percent of respondents).

Figure 15. How does integration affect performance of the SIEM?

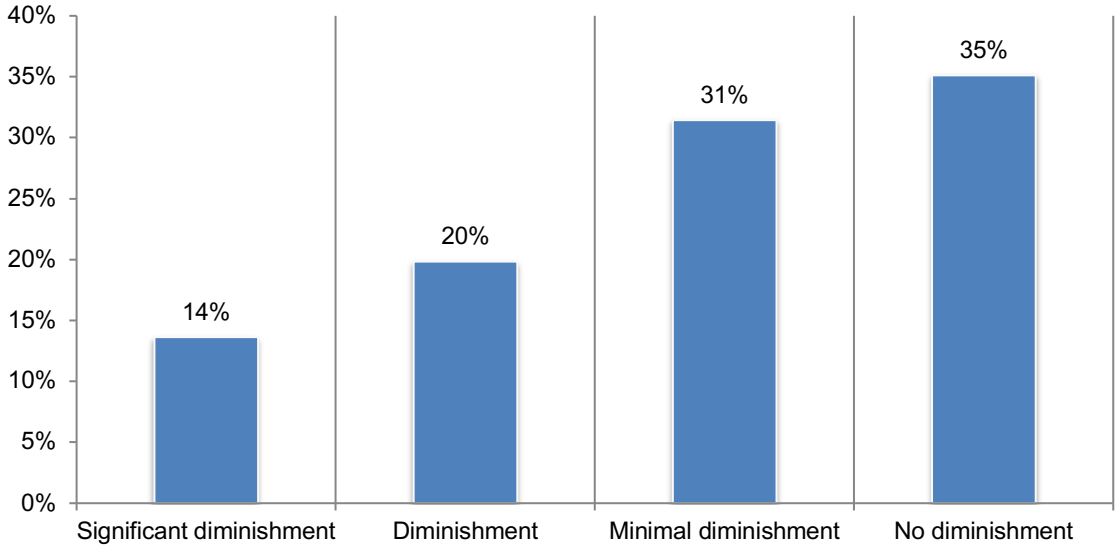
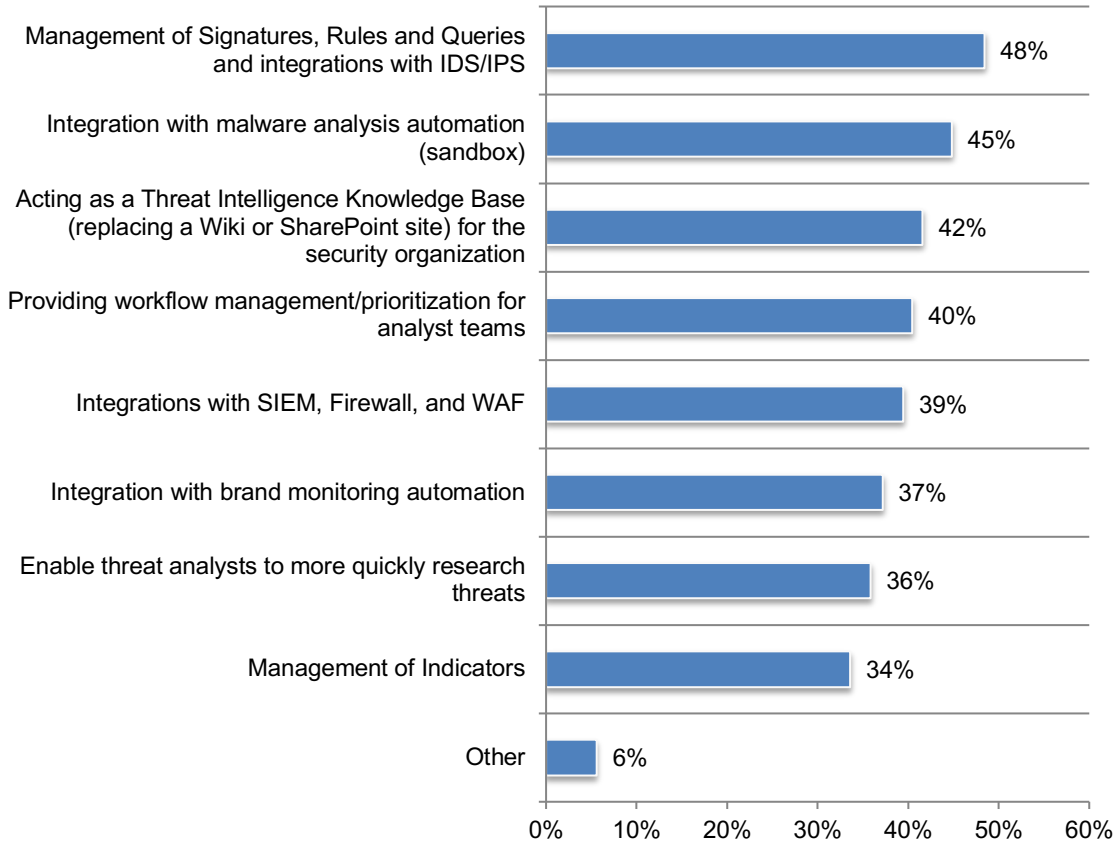


Figure 16 presents the most desirable features as part of the integration of threat data. These are: management of signatures, rules and queries and integrations with IDS/IPS; integration with malware analysis automation and acting as a threat intelligence knowledge base for the security organization, 48 percent, 45 percent and 42 percent respectively.

Figure 16. Desirable features as part of the integration of threat data
More than one response permitted



Industry differences

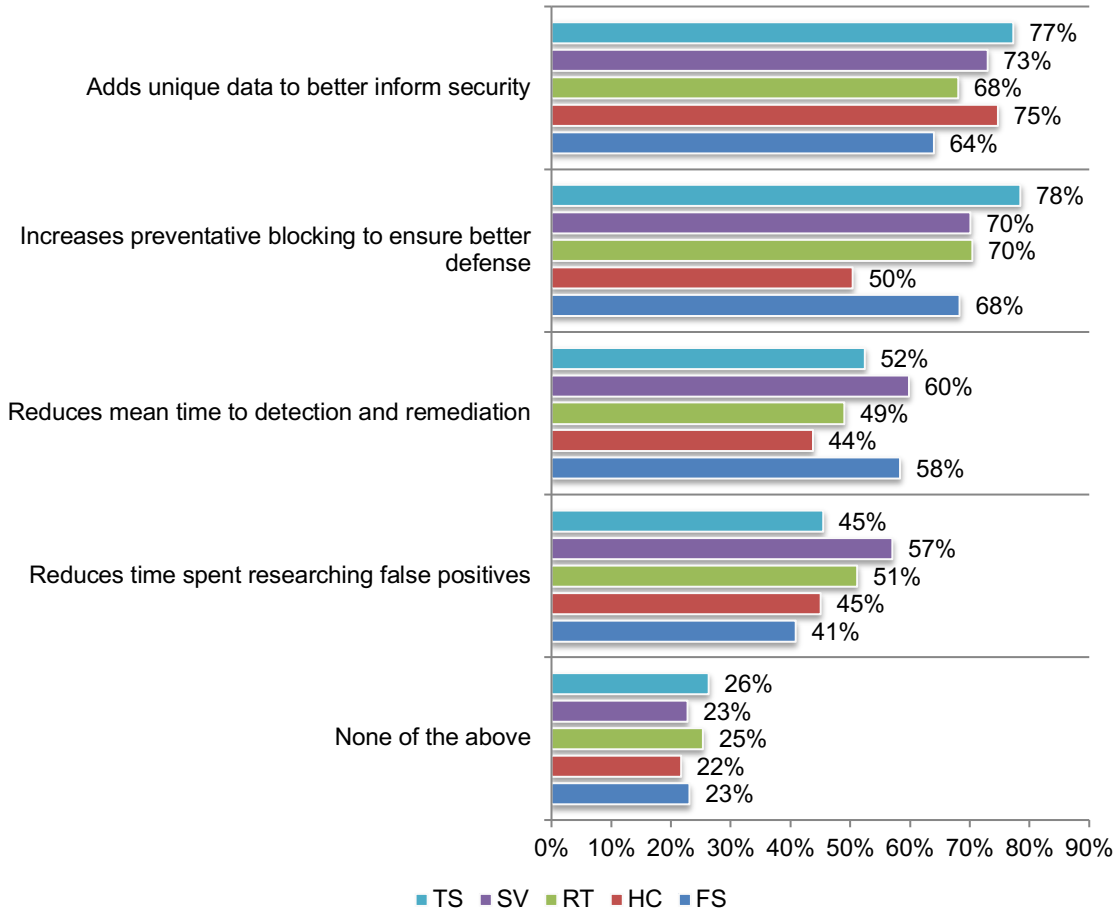
Table 1. Industry sample response	Freq
Financial Services	185
Retail	113
Healthcare and Pharma	93
Services	85
Tech and Software	82

This section presents the most salient industry differences for Financial Services (FS 185 respondents), Healthcare and Pharma (HC 93 respondents), Retail (RT 113 respondents), Services (SV 85 respondents) and Tech and Software (TS 82 respondents).

Respondents in healthcare and services rate the top benefit provided by threat data feeds as the ability to add unique data to better inform security (75 percent and 73 percent of respondents, respectively). According to Figure 18, tech and software organizations say the top benefits are the increase in preventative blocking to ensure better defense (78 percent of

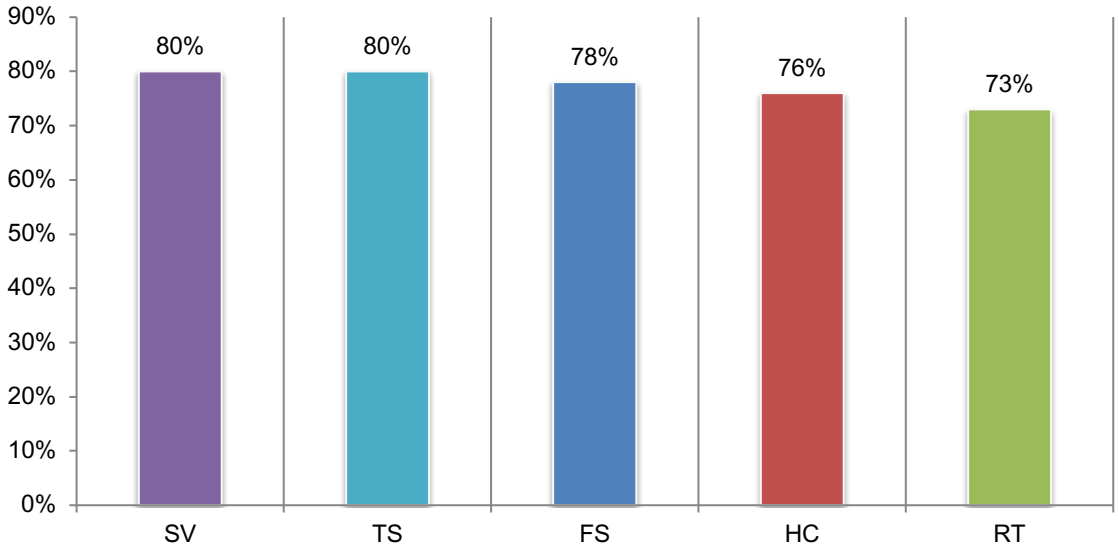
respondents) and the addition of unique data to better inform security (77 percent of respondents). Respondents in services are more likely to say the top benefits are the reduction in mean time to detection and remediation (60 percent) and the reduction in time spent researching false positives (57 percent).

Figure 18. The top two benefits provided by threat data feeds
More than one response permitted



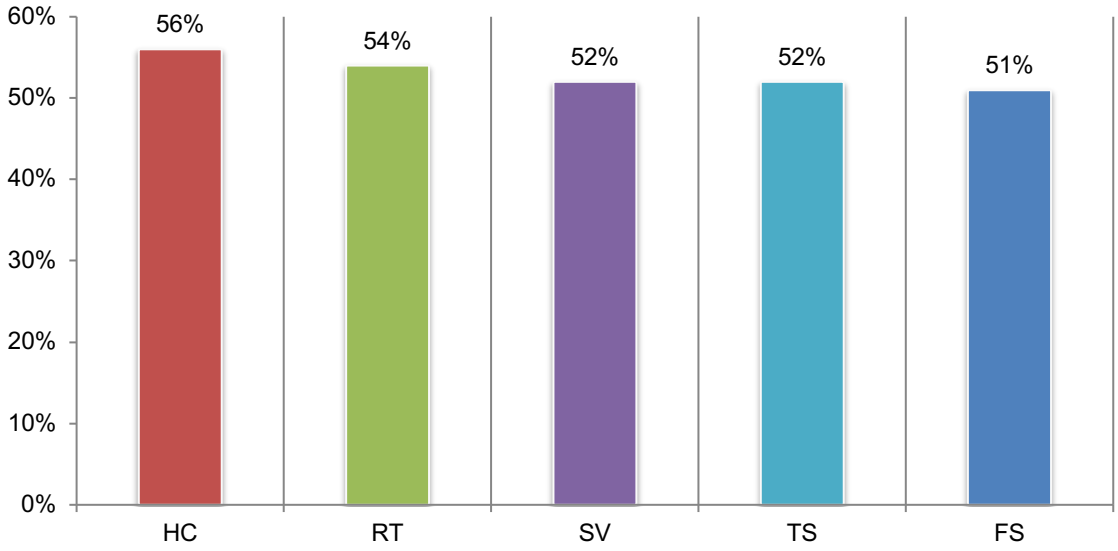
As shown in Figure 19, most respondents in all verticals believe threat data feeds are essential to achieving a strong cybersecurity posture.

Figure 19. The importance of threat data feeds in achieving a strong cybersecurity posture
On a scale from 1 = low (irrelevant) to 10 = high (essential), 7+ responses presented



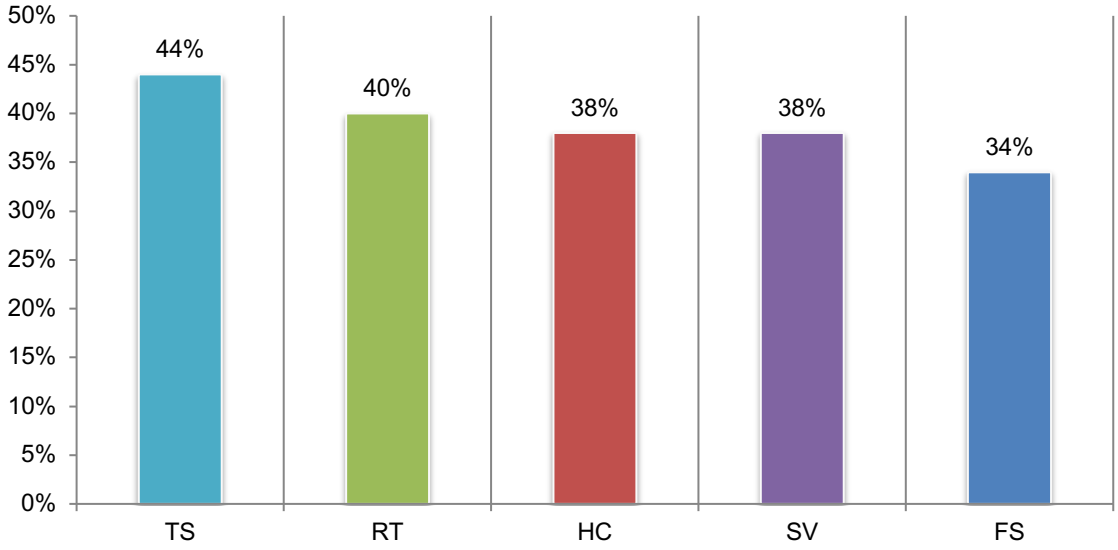
A top benefit of using threat data feeds is that they add unique data to better inform security. When asked to rate their effectiveness on a scale 1 = low to 10 = very effective, the majority of respondents in all industries say the effectiveness of threat feeds to leverage unique data to better inform security, increase preventative blocking and minimize danger from cyberthreats is very high, according to Figure 20.

Figure 20. The effectiveness of threat feeds in leveraging unique data to better inform security, increase preventative blocking and minimize danger from cyberthreats
On a scale from 1 = low (ineffective) to 10 = high (very effective), 7+ response presented



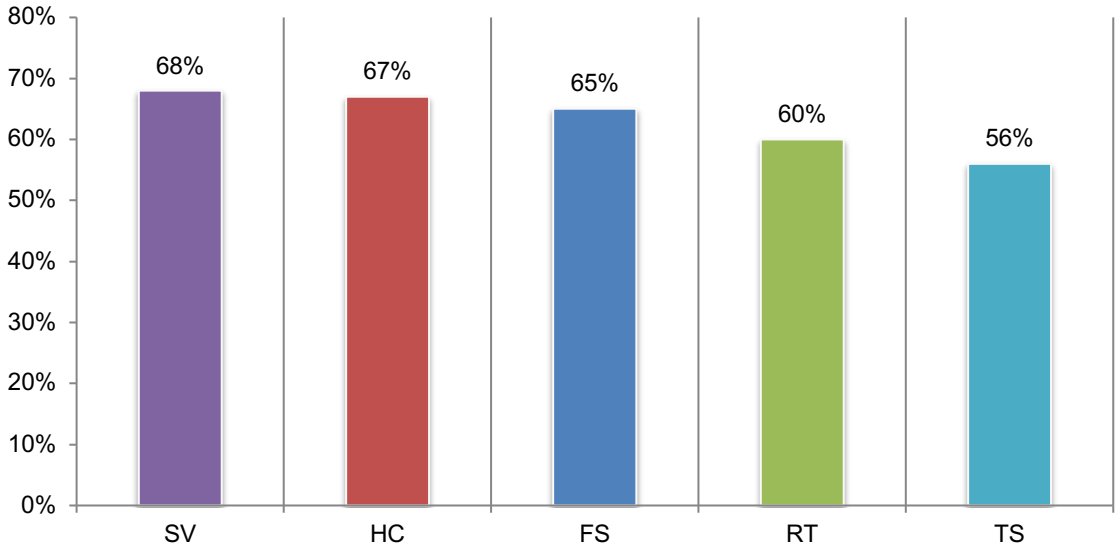
The effectiveness of threat feeds in determining the location of the cyberattack needs to improve. As shown in Figure 21, only 34 percent of respondents in financial services say the effectiveness in determining the location of the cyberattack is very high.

Figure 21. Effectiveness in determining the location of the cyberattack
On a scale from 1 = low (ineffective) to 10 = high (very effective), 7+ response presented



Services (68 percent of respondents), healthcare (67 percent of respondents) and financial services (65 percent of respondents) rate the difficulty of reducing the risk caused by phishing attacks as very difficult.

Figure 22. The difficulty in mitigating the risk caused by phishing attacks
On a scale from 1 = low (not difficult) to 10 = high (very difficult), 7+ response presented

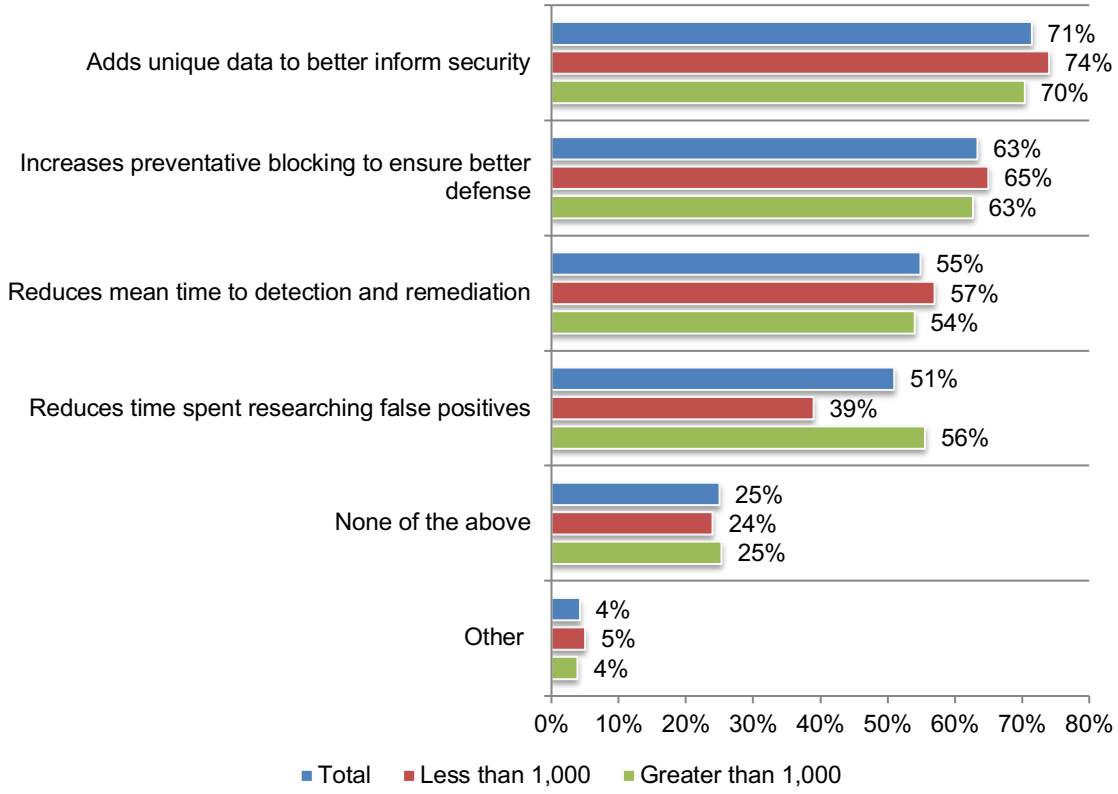


Differences by organizational size

In this section, the most salient differences between organizations that are small and with a headcount of 1,000 or less (28 percent of the total sample) and organizations that are mid-sized or large with a headcount of more than 1,000 (72 percent of the total sample).

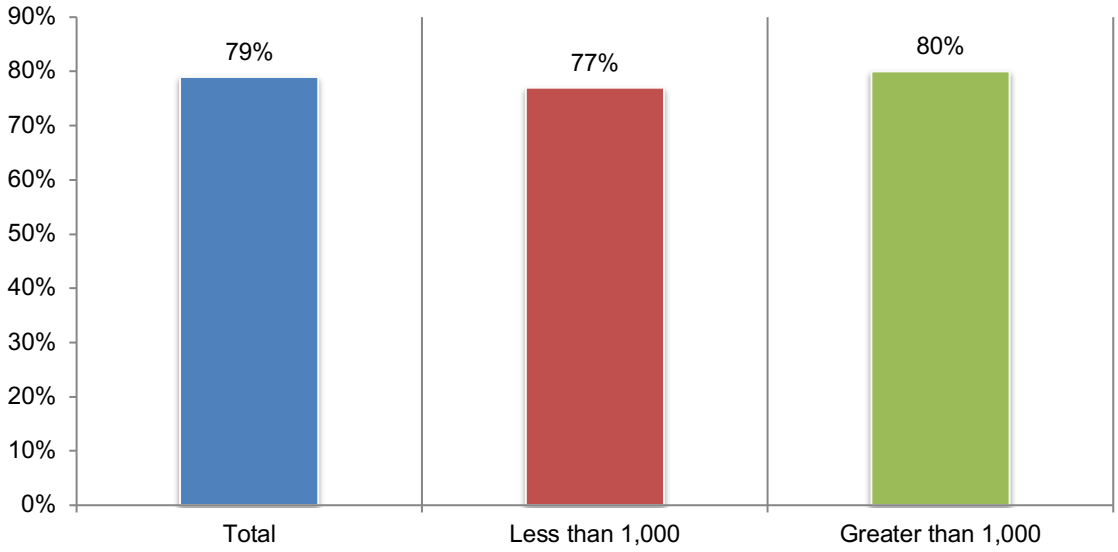
Both large and small organizations rate the top benefit of threat data feeds is the ability to add unique data to better inform security. Large organizations are more likely than small organizations to say the benefit of threat data feeds is the reduction of time spent researching false positives (56 percent vs. 39 percent of small organizations), as shown in Figure 23.

Figure 23. The top two benefits provided by threat data feeds
More than one response permitted



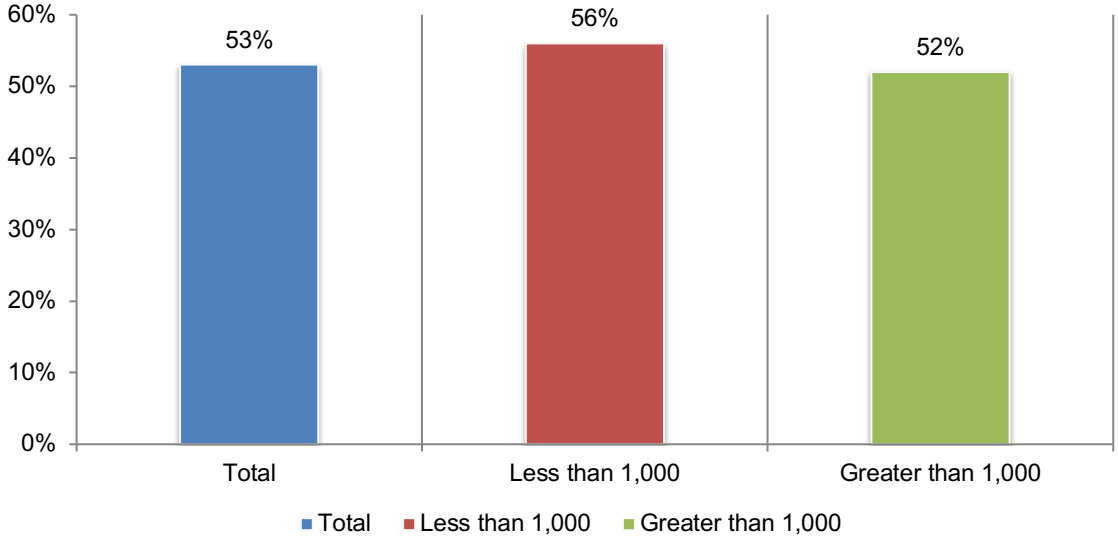
Both respondents in large (80 percent) and small organizations (77 percent) value the ability of threat data feeds to create a strong cybersecurity posture, as shown in Figure 24.

Figure 24. The importance of threat data feeds in achieving a strong cybersecurity posture
On a scale from 1 = low (irrelevant) to 10 = high (essential), 7+ responses presented



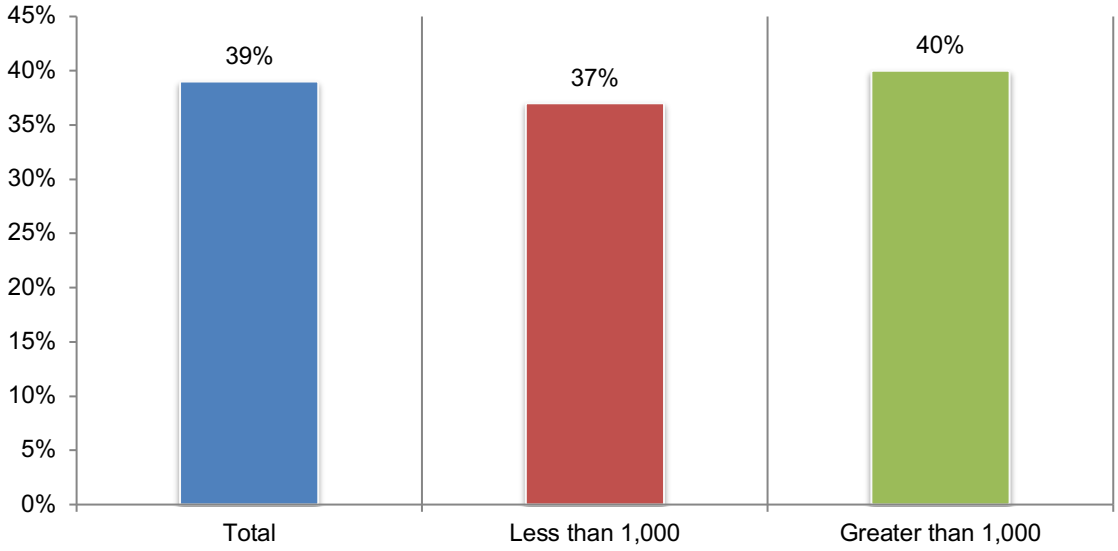
As discussed, the top benefit of threat data feeds according to both large and small organizations is the ability to add unique data to better inform security. According to Figure 25, 56 percent of respondents in small organizations and 52 percent of large organizations rate the effectiveness of threat feeds in leveraging unique data to better inform security, increase preventative blocking and minimize danger from cyberthreats as very high.

Figure 25. The effectiveness of threat feeds in leveraging unique data to better inform security, increase preventative blocking and minimize danger from cyberthreats
On a scale from 1 = low (ineffective) to 10 = high (very effective), 7+ response presented



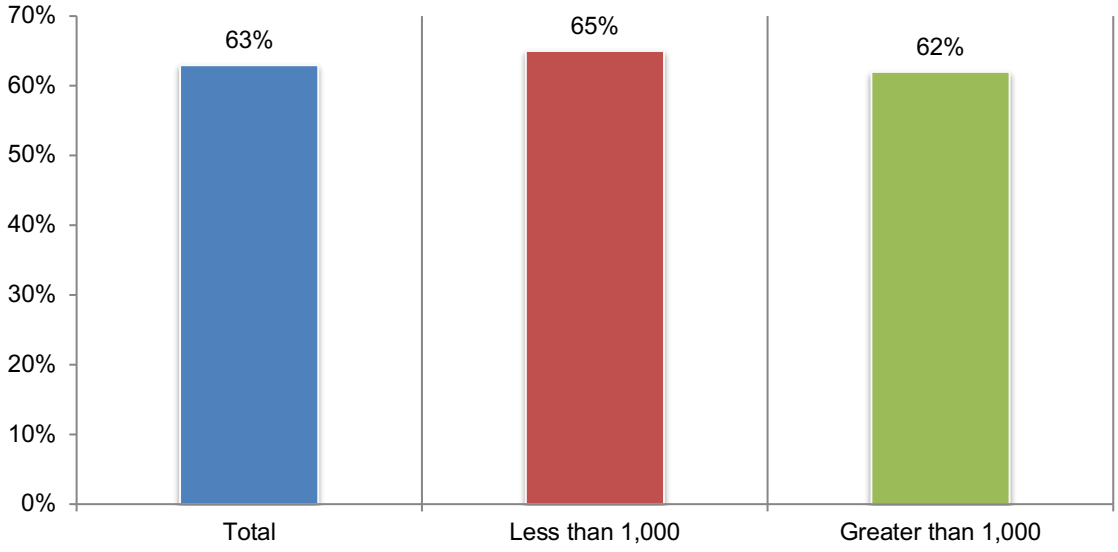
Both large and small organizations need to improve the effectiveness of the ability to determine the location of the cyberattack. As shown in Figure 26, only 37 percent of respondents in small organizations and 41 percent of respondents in large organizations say their threat feeds are highly effective in determining the location of the cyberattack.

Figure 26. Effectiveness in determining the location of the cyberattack
On a scale from 1 = low (ineffective) to 10 = high (very effective), 7+ response presented



Mitigating the risk caused by phishing attacks is very difficult for both small (65 percent of respondents) and large organizations (60 percent of respondents).

Figure 27. The difficulty in mitigating the risk caused by phishing attacks
On a scale from 1 = low (not difficult) to 10 = high (very difficult), 7+ response presented



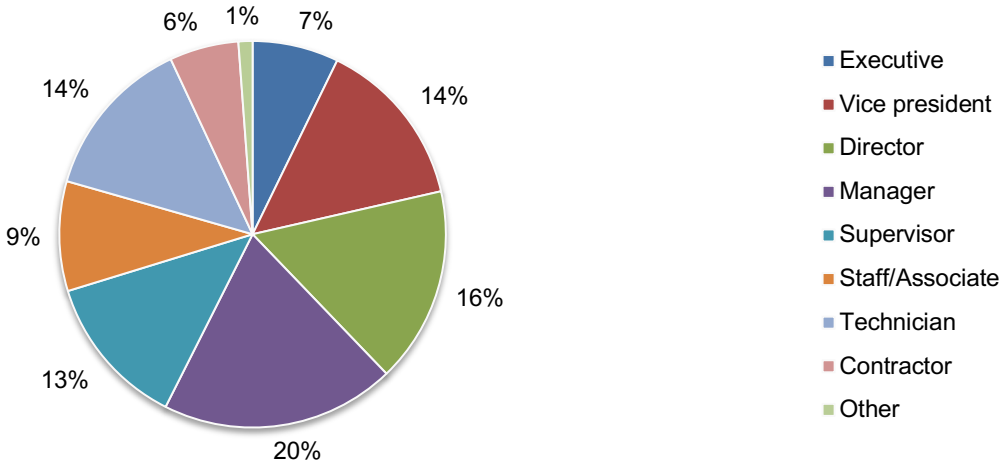
Part 3. Methods

A sampling frame of 27,002 IT security practitioners in the United States and the United Kingdom and in organizations that use threat data as part of its cybersecurity program or infrastructure were selected as participants to this survey. Table 2 shows 1,146 total returns. Screening and reliability checks required the removal of 121 surveys. Our final sample consisted of 1,025 surveys or a 3.8 percent response.

Table 12 Sample response	Freq	Pct%
Sampling frame	27,002	100.0%
Total returns	1,146	4.2%
Rejected or screened surveys	121	0.4%
Final sample	1,025	3.8%

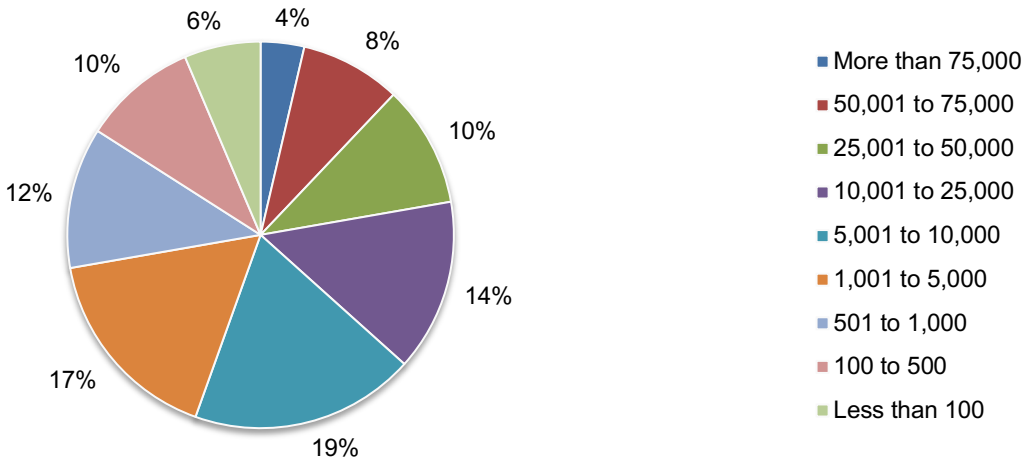
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (70 percent) of respondents are at or above the supervisory levels. The largest category at 20 percent of respondents is manager.

Pie Chart 1. Current position within the organization



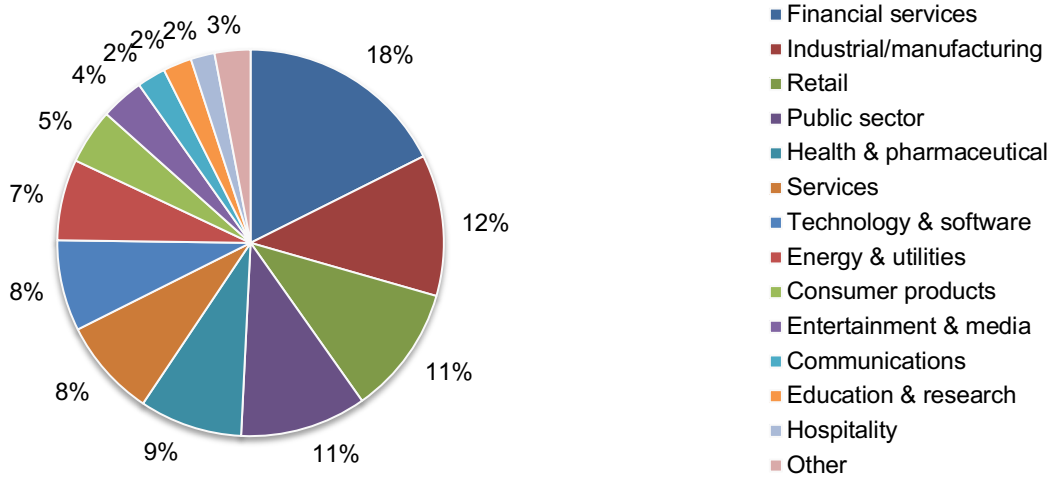
As shown in Pie Chart 2, 55 percent of respondents are from organizations with a global headcount of more than 5,000 employees.

Pie Chart 2. Global employee headcount



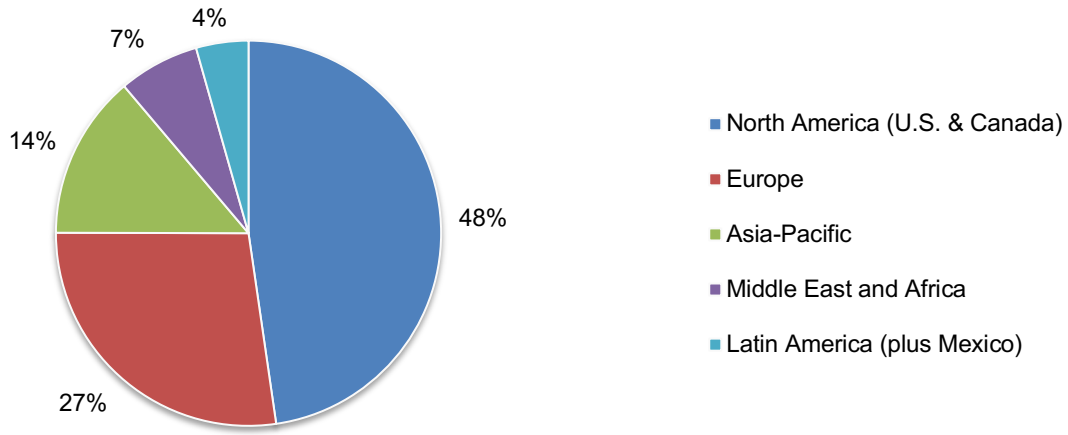
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by industrial and manufacturing (12 percent of respondents), retail (11 percent of respondents), public sector (11 percent of respondents) and health and pharmaceuticals (9 percent of respondents).

Pie Chart 3. Primary industry focus



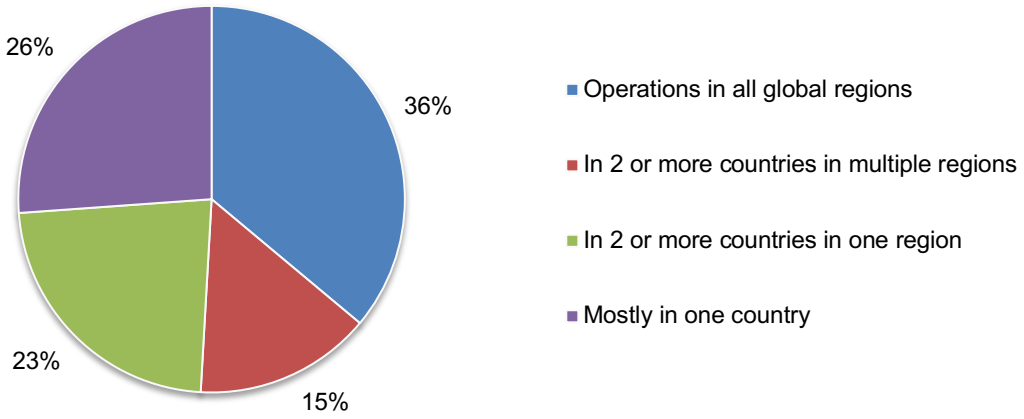
Pie Chart 4 reports the headquarter location of respondents organizations. Almost half (48 percent) of respondents reported their headquarters are located in North America, 27 percent of respondents reported Europe, 14 percent of respondents reported Asia-Pacific, 7 percent of respondents reported Middle East and Africa and 4 percent of respondents reported Latin America.

Pie Chart 4. Headquarter locations of respondents organizations



Pie Chart 5 reports the respondents organization's global footprint. Thirty-six percent of respondents reported their organization has operations in all global regions, 26 percent of respondents are from organizations with operations in mostly one country, 23 percent of respondents are from organizations with operations in 2 or more countries in one region and 15 percent of respondents are from organizations with operations in 2 or more countries in multiple regions.

Pie Chart 5. Respondents organization's global footprint



Part 4. Caveats to this study

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 security practitioners located in the United States and the United Kingdom. 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 all survey questions contained in this study. All survey responses were captured in November 2020.

Survey response	Total
Total sampling frame	27,002
Total survey returns	1,146
Rejected surveys	121
Final sample	1,025
Response rate	3.8%

Part 1. Screening questions

S1a. Does your organization utilize threat data as part of its cybersecurity program or infrastructure?	Total
Yes	100%
No (stop)	0%
Total	100%

S1b. If no, why not?	Total
Not considered a priority	29%
Lack of staff expertise	44%
Lack of technologies	43%
Cost of prevailing solutions (TCO)	31%
Threat data is insufficient to pinpoint IOCs	46%
Other (please specify)	3%
None of the above (Stop)	0%
Total	197%

S2. What best describes your familiarity with your organization's approach(es) to using threat data?	Total
Very familiar	41%
Familiar	36%
Somewhat familiar	23%
Not familiar (stop)	0%
Total	100%

Part 2. Organizational characteristics

D1. What best defines your position level within the organization?	Total
Executive	7%
Vice president	14%
Director	16%
Manager	20%
Supervisor	13%
Staff/Associate	9%
Technician	14%
Contractor	6%
Other (please specify)	1%
Total	100%

D2. What best defines the global employee headcount of your organization?	Total
Less than 100	6%
100 to 500	10%
501 to 1,000	12%
1,001 to 5,000	17%
5,001 to 10,000	19%
10,001 to 25,000	14%
25,001 to 50,000	10%
50,001 to 75,000	8%
More than 75,000	4%
Total	100%

D3. What best defines your organization's primary industry segment?	Total
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	7%
Entertainment & media	4%
Financial services	18%
Health & pharmaceutical	9%
Hospitality	2%
Industrial/manufacturing	12%
Public sector	11%
Retail	11%
Services	8%
Technology & software	8%
Transportation	1%
Other	0%
Total	100%

D4. Where is your organization headquartered? Please choose only one region.	Total
North America (U.S. & Canada)	48%
Europe	27%
Middle East and Africa	7%
Asia-Pacific	14%
Latin America (plus Mexico)	4%
Total	100%

D5. What best defines your organization's global footprint	Total
Operations mostly in one country	26%
Operations in 2 or more countries in one region	23%
Operations in 2 or more countries in multiple regions	15%
Operations in all global regions	36%
Total	100%

Part 3. Background questions

Q1. What percentage of your organization's annual revenue is through digital products and/or products sold online?	Total
Less than 25 percent	42%
26 percent to 40 percent	19%
41 percent to 60 percent	18%
60 percent to 75 percent	10%
76 percent to 100 percent	12%
Total	100%
Extrapolated value	40%

Q2. How many physical and virtual addresses does your organization have?	Total
One	0%
2 to 5	5%
6 to 10	9%
11 to 20	12%
21 to 40	29%
More than 40	45%
Total	100%
Extrapolated value	34.0

Q3. What is the primary source of threat data used by your organization?	Total
Open source (free)	31%
Paid feeds	44%
Combination of open source and paid feeds	25%
Total	100%

Part 4. Organizations' perceptions about their use of threat feeds

Q4. Approximately, how many threat data feeds are used by your organization today?	Total
One	6%
2 to 5	16%
6 to 10	18%
11 to 20	19%
21 to 40	22%
More than 40	20%
Total	100%
Extrapolated value	21.2

Q5a. How many cyberattacks has your organization had in the past two years?	Total
Less than 10	28%
11 to 25	26%
26 to 50	28%
More than 50	18%
Total	100%
Extrapolated value	27.5

Q5b. On average, what percentage of these cyberattacks were not stopped because of the lack of timely and actionable data from your organization's threat data feeds?	Total
Zero	0%
Less than 5 percent	1%
5 percent to 10 percent	7%
11 percent to 15 percent	7%
16 percent to 20 percent	8%
21 percent to 30 percent	12%
31 percent to 40 percent	7%
41 percent to 50 percent	30%
More than 50 percent	27%
Total	100%
Extrapolated value	38%

Q6. In your opinion, what percentage of all attacks can intelligence from your organization's threat feeds stop?	Total
Zero	0%
Less than 5 percent	1%
5 percent to 10 percent	2%
11 percent to 15 percent	1%
16 percent to 20 percent	3%
21 percent to 30 percent	8%
31 percent to 40 percent	4%
41 percent to 50 percent	21%
More than 50 percent	60%
Total	100%
Extrapolated value	50%

Q7. Which of the following are barriers to having effective threat data feeds? Please select the top three barriers.	Total
Lack of scalability	48%
Not actionable	59%
Lack of interoperability	47%
Not timely	47%
Complexity	66%
Not cost effective	28%
Other (Please specify)	5%
Total	300%

Q8.Which of the following benefits are provided by your organization's threat data feeds? Please select all that apply.	Total
Adds unique data to better inform security	71%
Increases preventative blocking to ensure better defense	63%
Reduces time spent researching false positives	51%
Reduces mean time to detection and remediation	55%
None of the above	25%
Other (Please specify)	4%
Total	270%

Q9. What challenges keep your organization's threat data feeds from being fully effective? Please select your top three challenges.	Total
Increasingly sophisticated attacks, such as DNS Tunneling	48%
Nation state-sponsored cyberattacks	24%
Insufficient budget (money)	38%
Lack of clear leadership	16%
Lack of effective testing tools	20%
Lack of in-house expertise	48%
Lack of security training	27%
Management underestimates risk	16%
Not considered an organizational priority	28%
Other (please specify)	5%
Pressure to release new applications	30%
Total	300%

Q10. Does your organization track DNS traffic for malicious activity?	Total
Yes	65%
No	35%
Total	100%

Q11a. Does your organization have a cloud-based DNS service?	Total
Yes	55%
No	45%
Total	100%

Q11b. If yes, using the following 10-point scale, please rate the effectiveness of your organization's DNS service in its ability to securely deliver fast and accurate query responses to websites and other vital online assets. 1 = low (ineffective) to 10 = high (very effective).	Total
1 or 2	6%
3 or 4	12%
5 or 6	20%
7 or 8	29%
9 or 10	32%
Total	100%
Extrapolated value	6.89

Q12. How many years of DNS data does your organization have?	Total
1 year	12%
2 to 5 years	36%
6 to 10 years	24%
11 to 20 years	17%
21 to 40 years	9%
More than 40 years	1%
Total	100%
Extrapolated value	9.22

Q13. Using the following 10-point scale, please rate the importance of threat data feeds with respect to your organization's ability to achieve a strong cybersecurity posture. 1 = low (irrelevant) to 10 = high (essential).	Total
1 or 2	2%
3 or 4	7%
5 or 6	11%
7 or 8	26%
9 or 10	53%
Total	100%
Extrapolated value	7.91

Q14. Using the following 10-point scale, please rate the quality of your organization's threat feeds in their ability to utilize threat data to pinpoint cyber threats. 1 = low (quality) to 10 = high (quality).	Total
1 or 2	9%
3 or 4	13%
5 or 6	23%
7 or 8	27%
9 or 10	28%
Total	100%
Extrapolated value	6.52

Q15. Using the following 10-point scale, please rate the effectiveness of your organization's ability to secure its online presence against risks and downtime while ensuring customers have consistent, uninterrupted quality interactions. 1 = low (ineffective) to 10 = high (very effective).	Total
1 or 2	1%
3 or 4	12%
5 or 6	24%
7 or 8	31%
9 or 10	31%
Total	100%
Extrapolated value	7.06

Q16. Using the following 10-point scale, please rate the effectiveness of your organization's threat feeds in leveraging unique data to better inform security, increase preventative blocking and minimize damage from cyberthreats. 1 = low (ineffective) to 10 = high (very effective).	Total
1 or 2	4%
3 or 4	9%
5 or 6	33%
7 or 8	27%
9 or 10	26%
Total	100%
Extrapolated value	6.74

Q17. Using the following 10-point scale, please rate your organization's effectiveness in determining the location of the cyberattack (i.e. geo-location). 1 = low (ineffective) to 10 = high (very effective).	Total
1 or 2	18%
3 or 4	19%
5 or 6	24%
7 or 8	19%
9 or 10	20%
Total	100%
Extrapolated value	5.57

Q18. Using the following 10-point scale, please rate the difficulty in mitigating the risks created by Malicious DGAs. 1 = low (not difficult to 10 = high (very difficult).	Total
1 or 2	0%
3 or 4	7%
5 or 6	17%
7 or 8	25%
9 or 10	51%
Total	100%
Extrapolated value	7.90

Q19. Using the following 10-point scale, please rate the difficulty in mitigating the risk caused by suspicious DNS Tunneling Attempts. 1 = low (not difficult) to 10 = high (very difficult).	Total
1 or 2	2%
3 or 4	10%
5 or 6	16%
7 or 8	24%
9 or 10	48%
Total	100%
Extrapolated value	7.63

Q20. Using the following 10-point scale, please rate the difficulty in mitigating the risks created by Domain or DNS hijacks . 1 = low (not difficult to 10 = high (very difficult).	Total
1 or 2	2%
3 or 4	7%
5 or 6	12%
7 or 8	33%
9 or 10	46%
Total	100%
Extrapolated value	7.75

Q21. Using the following 10-point scale, please rate the difficulty in mitigating the risk caused by Phishing Attacks. 1 = low (not difficult) to 10 = high (very difficult).	Total
1 or 2	2%
3 or 4	11%
5 or 6	24%
7 or 8	28%
9 or 10	35%
Total	100%
Extrapolated value	7.13

Q22. Using the following 10-point scale, please rate the difficulty in mitigating the risk caused by Anonymizing Proxies 1 = low (not difficult) to 10 = high (very difficult).	Total
1 or 2	1%
3 or 4	4%
5 or 6	12%
7 or 8	36%
9 or 10	47%
Total	100%
Extrapolated value	7.99

Part 5. Threat intelligence platforms

Q23a. Does your organization deploy a threat intelligence platform?	Total
Yes (Please skip to Q24)	58%
No, but planning to deploy within the next 12 months	8%
No, but planning to deploy more than 12 months from now	8%
No plan to deploy	26%
Total	100%

Q23b. If no, why doesn't your organization deploy a threat intelligence platform?	Total
Not considered a priority	24%
Lack of staff expertise	51%
Lack of technologies	47%
Cost of prevailing solutions (TCO)	39%
Threat data alone is sufficient to pinpoint IOCs	51%
Other (please specify)	5%
Total	218%

Q23c. If no, how difficult is the process of prioritizing threat data (without a platform)?	Total

Very difficult	29%
Difficult	34%
Somewhat difficult	25%
Not difficult	9%
Easy	3%
Total	100%

Q24. What are the main benefits of having a threat intelligence platform? Please select your top three choices.	Total
Helps pinpoint and prioritize IOCs	64%
Streamlines the collection of threat data	55%
Improves the threat analytics process	53%
Standardizes the reporting of threat management activities	37%
Reduces operating costs pertaining to threat detection and remediation	42%
Integrates threat data with other enabling security solutions (such as SIEM)	45%
Other (please specify)	2%
Total	300%

Q25. Is the threat intelligence platform deployed consistently across the organization?	Total
Yes	40%
No	60%
Total	100%

Q26. How difficult is the process of prioritizing threat data (with a platform)?	Total
Very difficult	30%
Difficult	36%
Somewhat difficult	18%
Not difficult	12%
Easy	4%
Total	100%

Q27a. What parts of your security architecture do you integrate threat data into? Please select all that apply.	Total
Firewall	48%
SIEM	49%
Endpoint security system	54%
IDS / IPS	41%
WAF	39%
DLP	41%
None of the above (Please skip to Q28)	14%
Other (please specify)	4%
Total	290%

Q27b. What features would you like to see as part of the integration that you don't already have? Please select all that apply.	Total
Management of Indicators	34%
Integrations with SIEM, Firewall, and WAF	39%
Management of Signatures, Rules and Queries and integrations with IDS/IPS	48%
Acting as a Threat Intelligence Knowledge Base (replacing a Wiki or SharePoint site) for the security organization	42%
Enable threat analysts to more quickly research threats	36%
Providing workflow management / prioritization for analyst teams	40%
Integration with malware analysis automation (sandbox)	45%
Integration with brand monitoring automation	37%
Other (please specify)	6%
Total	327%

Q27c. How difficult was the integration process?	Total
Very difficult	35%
Difficult	37%
Somewhat difficult	16%
Not difficult	8%
Easy	3%
Total	100%

Q27d. How does integration affect performance of the SIEM?	Total
Significant diminishment	14%
Diminishment	20%
Minimal diminishment	31%
No diminishment	35%
Total	100%

Q28. How many days of log data does your organization keep live and online in your SIEM?	Total
Less than 1 day	5%
1 to 7 days	7%
1 to 4 weeks	7%
1 to 3 months	15%
4 to 6 months	19%
7 to 12 months	15%
1 to 2 years	19%
More than 2 years	12%
Total	100%
Extrapolated value	271

Q29. Following is a list of key functions contained in most threat intelligence platforms. Please select the functions that are (or would be) considered most important to your organization?	Total
Management of Indicators	47%
Integrations with SIEM, Firewall, and WAF	48%
Management of Signatures, Rules and Queries and integrations with IDS/IPS	38%
Acting as a Threat Intelligence Knowledge Base (replacing a Wiki or SharePoint site) for the security organization	46%
Enable threat analysts to more quickly research threats	33%
Providing workflow management / prioritization for analyst teams	41%
Integration with malware analysis automation (sandbox)	39%
Integration with brand monitoring automation	28%
Other (please specify)	4%
Total	324%

Part 6. Attributions about threat data feeds

Please rate each statement using the agreement scale provided below each item. **Strongly agree and Agree response combined.**	Total
Q30. Paid threat feeds provide more actionable intelligence than free sources of threat data.	47%
Q31. In my organization, improving threat detection is a high priority	49%
Q32. In my organization, incident responders utilize threat data when deciding how to respond to threats.	41%
Q33. SIEM integration is necessary to maximize the value of threat intelligence data.	52%
Q34. Our organization's threat feeds provide threat data that is often too voluminous and/or complex to provide timely and actionable intelligence.	56%
Q35. A threat intelligence platform is necessary to maximize the value of threat feeds.	48%

Part 7. Budget & investment

Q36. What is your organization's total IT budget?	Total
Less than $100,000	0%
$100,000 to $500,000	2%
$500,001 to $1,000,000	4%
$1,000,001 to $5,000,000	8%
$5,000,001 to $10,000,000	8%
$10,000,001 to $50,000,000	20%
$50,000,001 to $100,000,000	19%
$100,000,001 to $250,000,000	20%
$250,000,001 to $500,000,000	16%
More than $500,000,000	3%
Total	100%
Extrapolated value	##########

Q37. Approximately, what percentage of the current year's IT budget is allocated to IT security budget?	Total
< 1 percent	0%
1 percent to 2 percent	0%
3 percent to 5 percent	2%
6 percent to 10 percent	4%
11 percent to 15 percent	6%
16 percent to 20 percent	18%
21 percent to 30 percent	25%
31 percent to 40 percent	22%
41 percent to 50 percent	17%
> 50 percent	5%
Total	100%
Extrapolated value	29%

Q38. Approximately, what percentage of the current year's IT security budget will go to threat intelligence activities?	Total
< 1 percent	0%
1 percent to 2 percent	0%
3 percent to 5 percent	1%
6 percent to 10 percent	10%
11 percent to 15 percent	11%
16 percent to 20 percent	19%
21 percent to 30 percent	23%
31 percent to 40 percent	22%
41 percent to 50 percent	14%
> 50 percent	1%
Total	100%
Extrapolated value	26%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

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.

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.