Ponemon INSTITUTE

The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies

Sponsored by Anomali

Independently conducted by Ponemon Institute LLC

Publication Date: February 2019

The Value of Threat Intelligence:
Annual Study of North American and United Kingdom Companies

Presented by Ponemon Institute, February 2019

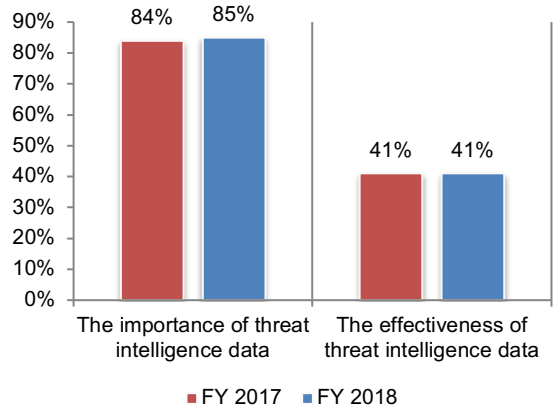
Part 1. Introduction

Ponemon Institute is pleased to present *The Value of Threat Intelligence: Annual Study of North American and United Kingdom Companies*, sponsored by Anomali. The purpose of this research is to examine trends in the benefits of threat intelligence and the challenges companies face when integrating threat intelligence with existing security platforms and technologies.

Only respondents who report their organization uses threat intelligence as part of their cybersecurity program completed the survey. A total of 1,098 IT and IT security practitioners in North America and the United Kingdom participated in this research. According to the findings, these participants strongly believe in the importance and value of threat intelligence data but are struggling to maximize its effectiveness in detecting cyber threats.

Participants in this research were asked to rate the importance and effectiveness of threat intelligence with respect to having a strong security posture on a scale from 1 = low to 10 = high. As shown in Figure 1, respondents continue to say threat intelligence is important, but have not made progress in improving its effectiveness. We refer to this as the threat intelligence gap.

Figure 1. The threat intelligence effectiveness gap
1 = low to 10 = high, 7+ responses



Closing the threat intelligence effectiveness gap

The importance of threat intelligence as part of an IT security mission should encourage organizations to take steps to improve how it is used. Following are recommendations to close the threat intelligence effectiveness gap.

- Establish a formal and dedicated team to manage threat intelligence activities.
- Allocate adequate budget to threat intelligence, including threat hunting and advanced attacker investigations.
- Participate in threat intelligence sharing.
- Participate in an ISAC/ISAO or other industry sharing group.
- Increase the security team's knowledge about adversaries including their motivations, infrastructure and methods.
- Improve ability to integrate threat intelligence with their tools.
- Improve ability to integrate threat intelligence data with SIEM and IDS/IPS.

Best practices in threat intelligence

In this section of the report, we outline eight best practices for threat intelligence. These best practices are extrapolated from 198 respondents who self-reported their organizations as highly effective in detecting external threats.

The eight best practices of high performing organizations

1. **Adequate budget.** Forty-one percent of high performing organizations have resources that focus on threat detection vs. only 33 percent of respondents in the overall sample.

2. **Focused on improving the use of threat intelligence to detect threats.** Seventy-two percent of respondents in high performing organizations rate their organizations' use of threat intelligence data as part of its threat detection efforts as highly effective. In contrast, 41 percent of respondents in the overall sample rate their effectiveness as very high.

3. **Understand their adversaries**. Virtually all high performing organizations want to understand the motivations, infrastructure and methods of attackers.

4. **Pay for threat intelligence.** Sixty percent of respondents say the primary source of threat intelligence is paid threat intelligence feeds. Twenty-three percent of respondents in the overall sample are more likely than high performing organizations to use open source threat intelligence feeds.

5. **Implement a dedicated threat intelligence platform.** Sixty-nine percent of respondents in high performing organizations have a dedicated threat intelligence platform but less than half (48 percent) of respondents in the overall sample have this.

6. **Integrate threat intelligence with its SIEM and IDS/IPS with less difficulty than the overall sample.** Eight-six percent of respondents in high performing organizations either integrate threat intelligence data from a threat intelligence platform (45 percent) or integrate built-in threat intelligence data provided by the SIEM vendor (41 percent). Eighty-one percent of these respondents say their organizations integrate threat intelligence with their IDS/IPS. High performing organizations also report that the integration with SIEM and IDS/IPS was not as difficult as the overall sample believes.

7. **Share intelligence with other organizations.** Seventy-seven percent of respondents in high performing organizations share threat intelligence with other organizations vs. 59 percent of respondents in the overall sample.

8. **Have a dedicated threat hunting team.** Fifty-nine percent of high performing organizations have a dedicated threat hunting team vs. 43 percent of respondents in the overall sample.

Part 2. Key findings

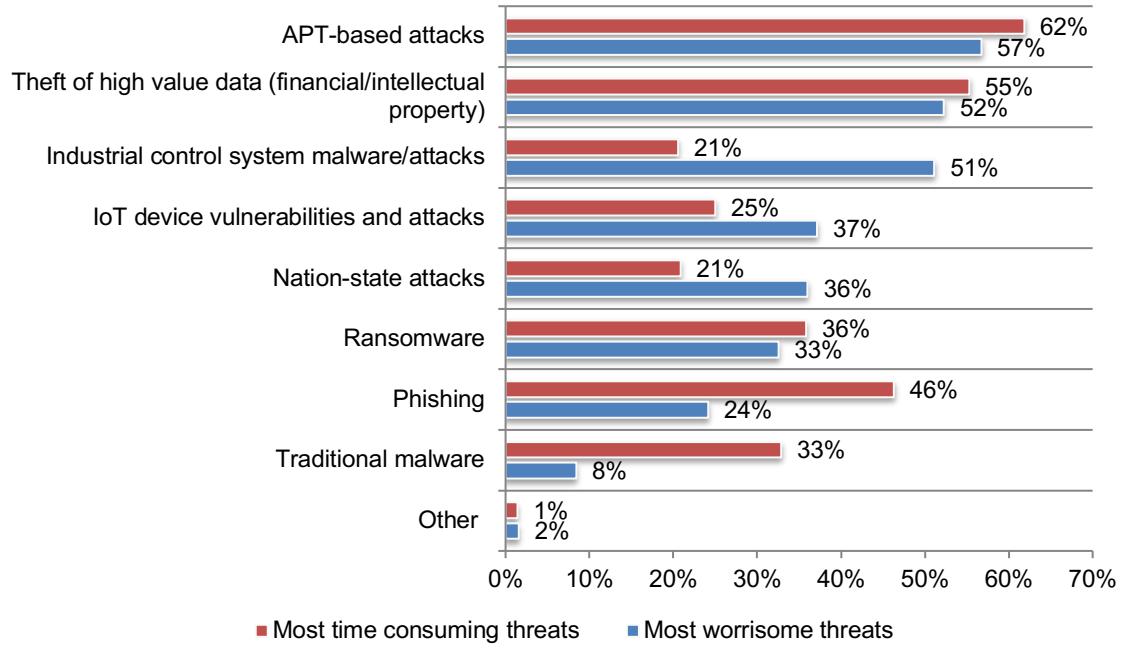
In this section of the report, we provide the detailed findings and trends of the research. Whenever possible, findings from the 2017 research are presented. The complete research is shown in the Appendix of this report. We have organized the report according to the following topics.

- The state of threat detection
- Threat detection strategies and threat hunting
- Threat intelligence platform and integration
- Best practices from high-performing organizations

The state of threat detection

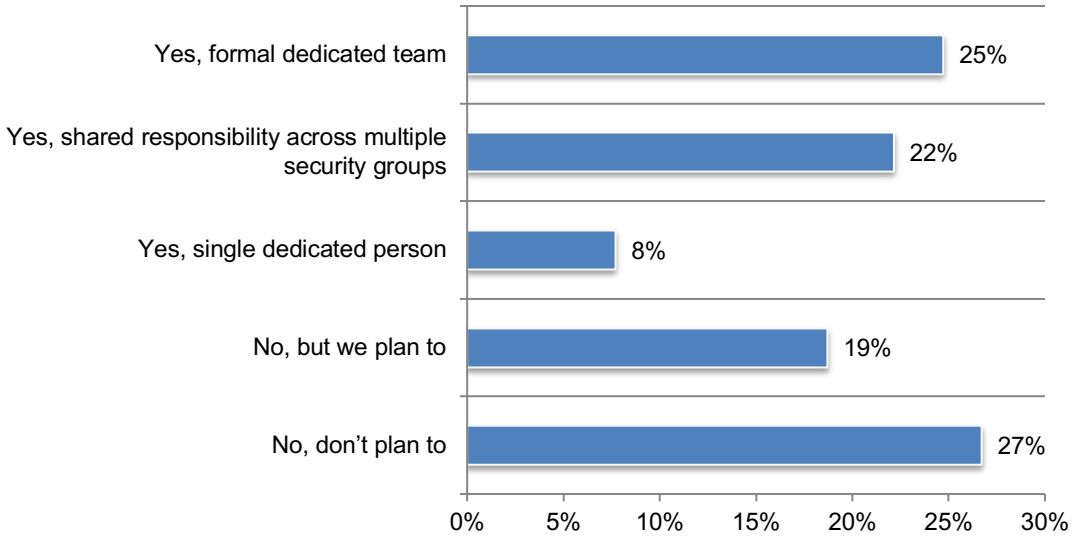
APT attacks and theft of high value data are both the most worrisome and the most time consuming to resolve. According to Figure 2, 62 percent of respondents say APT-based attacks are the most time-consuming attacks and 57 percent of respondents say it is of greatest concern. The theft of such high value data as financial information and intellectual property are also both time consuming to resolve (55 percent of respondents) and worrisome (52 percent of respondents). Forty-six percent of respondents say resolving phishing attacks is most time consuming, but only 24 percent of respondents say it is a significant concern.

Figure 2. Threats that worry you most and take the most time to resolve
Three responses permitted



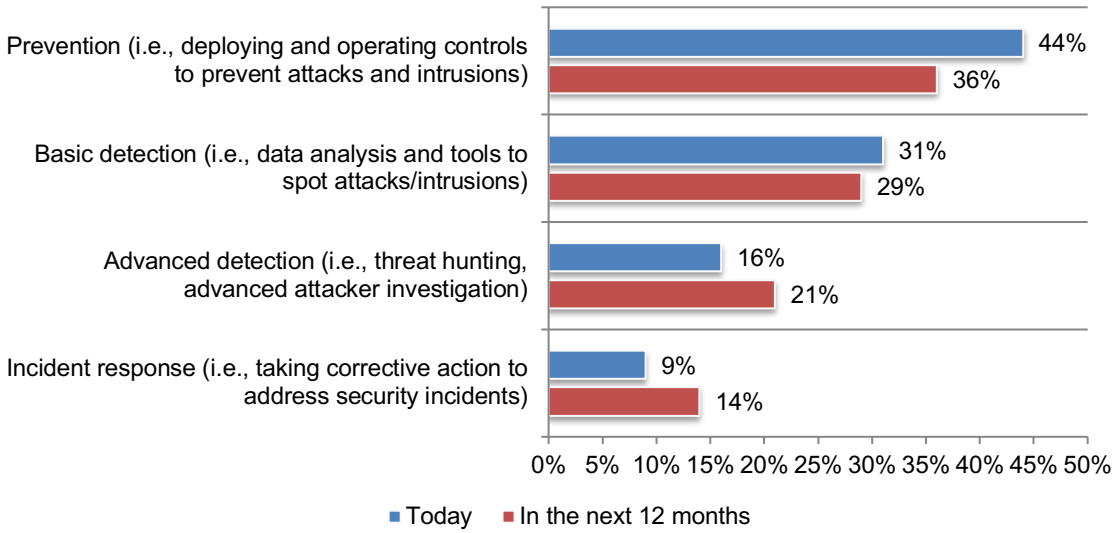
Most organizations say they have resources dedicated to threat detection. According to Figure 3, 55 percent of respondents say they have a formal dedicated team (25 percent), shared responsibility across multiple security groups (22 percent) or a single dedicated person (8 percent). However, 27 percent of respondents say their organizations have no plans to focus resources on threat detection.

Figure 3. Does your organization have resources that focus on threat detection?



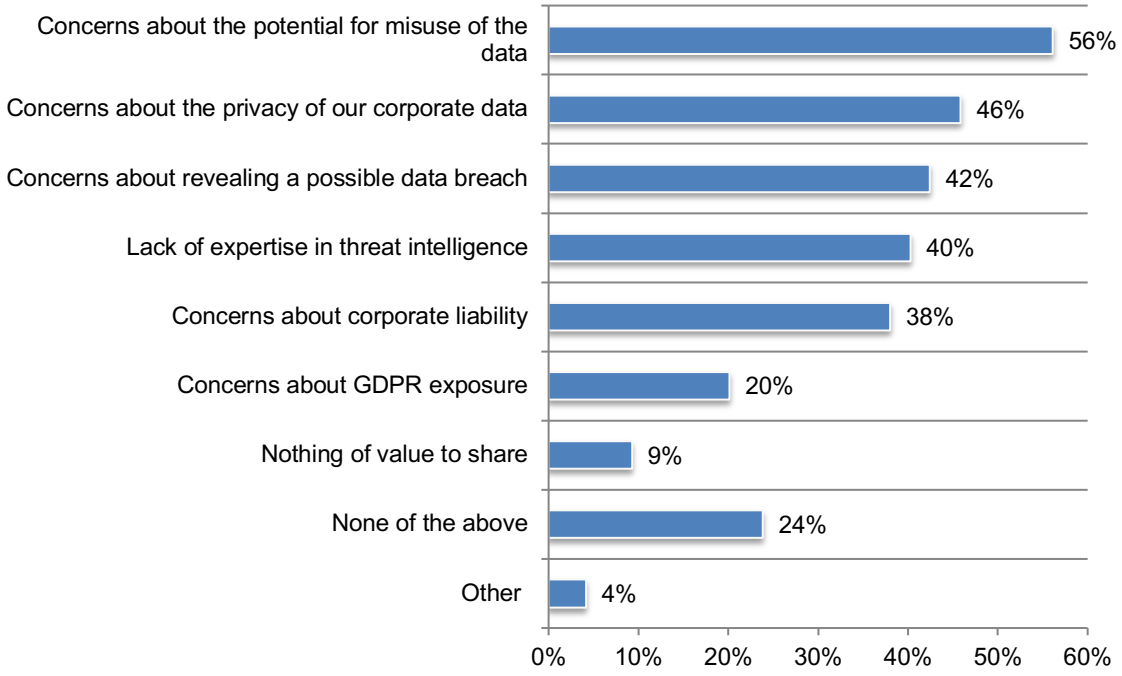
Organizations are allocating less money to prevention and more to advanced detection and incident response. As shown in Figure 4, today most of the budget (44 percent) is allocated to prevention but in the next 12 months it will decline to 36 percent. Advanced detection will increase from 16 percent to 21 percent and incident response will increase from 9 percent to 14 percent.

Figure 4. Allocation of budget today and in the next 12 months



The possible misuse of their data is why some organizations are reluctant to share threat intelligence. Fifty-nine percent of respondents say their organizations share threat intelligence with others. As shown in Figure 5, of the 41 percent of respondents who say their organizations share, 56 percent of respondents say it is because of the potential for the misuse of data and 46 percent have concerns about the privacy of corporate data.

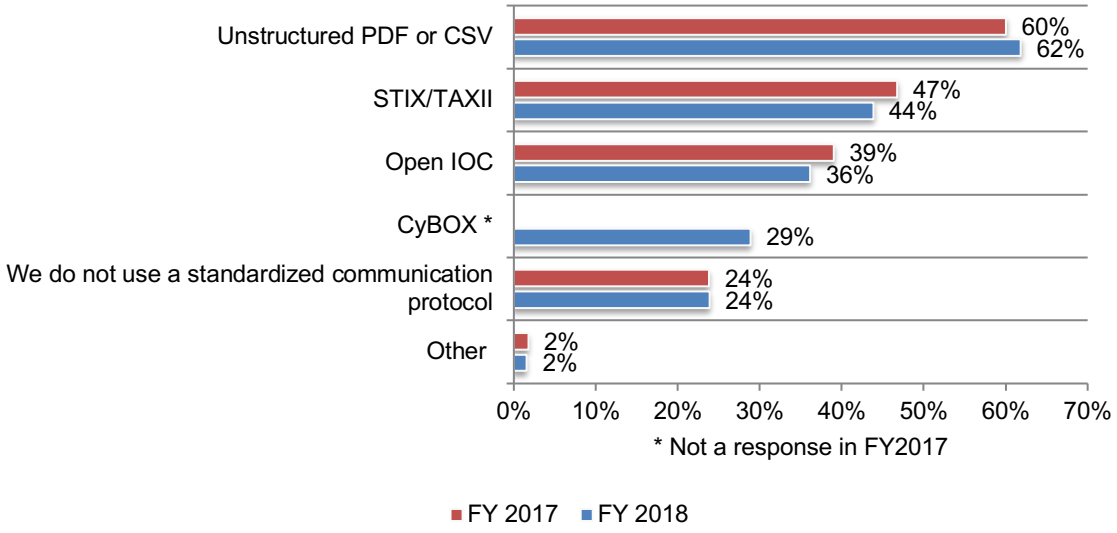
Figure 5. Reasons for not sharing threat intelligence
More than one response permitted



Threat detection strategies and threat hunting

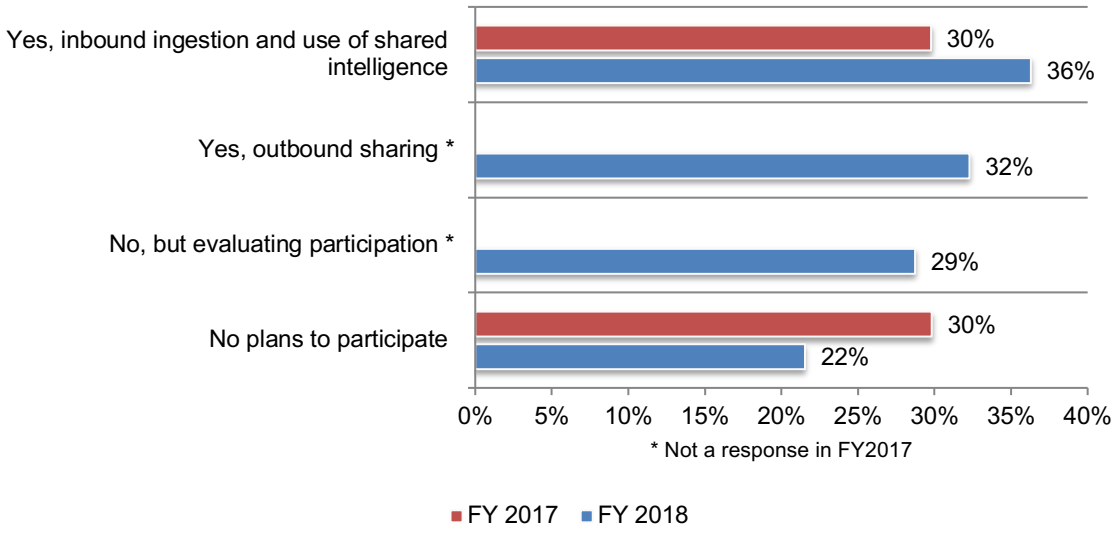
Unstructured PDF or CSV is the threat sharing protocol most often used. According to Figure 6, the threat sharing protocols used currently are consistent with last year's results. The most often used is unstructured PDF or CSV.

Figure 6. Threat intelligence information sharing protocols used
More than one response permitted



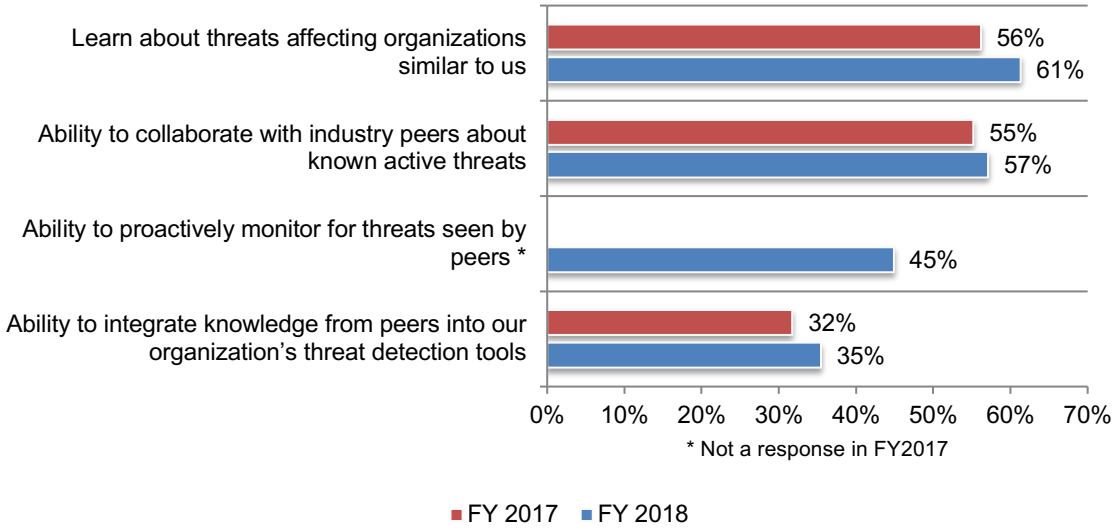
Participation in an ISAC/ISAO or other industry sharing group is increasing. As shown in Figure 7, inbound ingestion and use of shared intelligence has increased since last year. Thirty-two percent of respondents participate in outbound sharing.

Figure 7. Do you belong to or participate in an ISAC/ISAO or other industry sharing group?



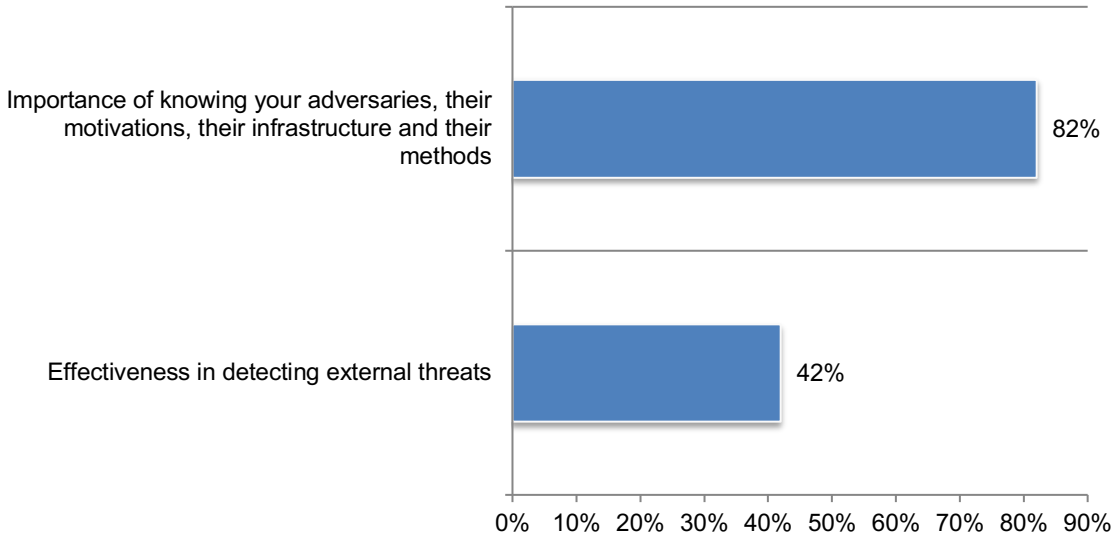
The biggest benefits are learning about threats that could affect their organization and the collaboration with peers. As shown in Figure 8, 61 percent of respondents say their organizations benefit from learning about threats affecting organizations similar to them and 57 percent of respondents say collaborating with industry peers about known active threats are very helpful to managing threats against their organizations.

Figure 8. Benefits from participation in ISAC/ISAO
More than one response permitted



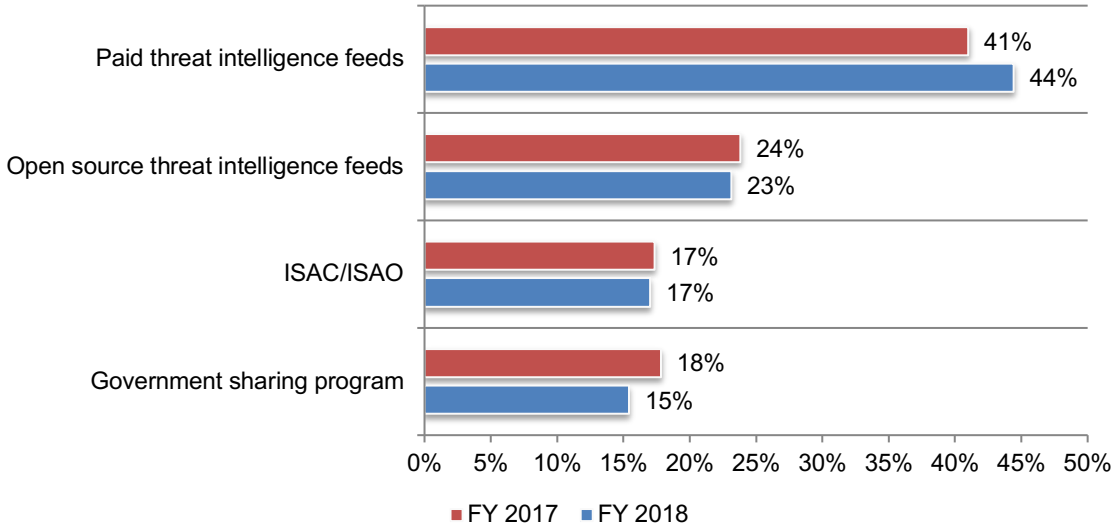
Organizations recognize the importance of having a detailed profile of their adversaries. Respondents were asked to rate the importance of knowing their adversaries, their motivations, their infrastructure and their methods on a scale of 1 = not important to 10 = high importance. As shown in Figure 9, 82 percent of respondents rated this ability as highly important. However, only 42 percent of respondents rate their effectiveness in detecting external threats as very high.

Figure 9. Effectiveness in detecting threats and the importance of knowing adversaries
1 = low effectiveness/importance to 10 = high effectiveness/importance, 7+ responses presented



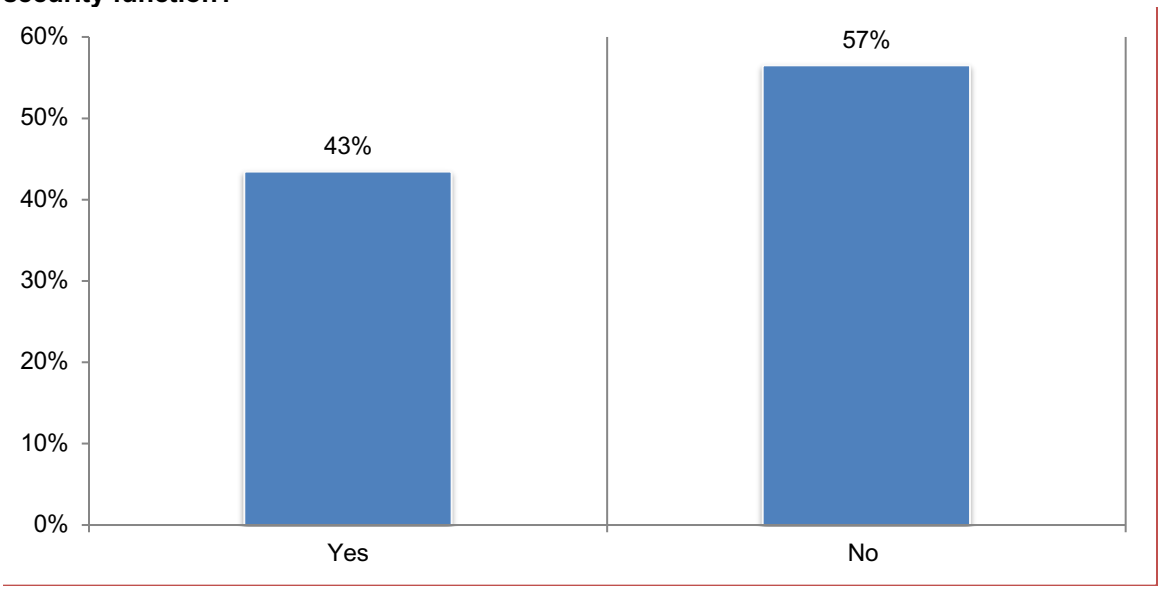
Similar to last year's research, more organization are paying for threat intelligence feeds. According to Figure 10, 44 percent of respondents say the primary source of threat intelligence feeds is purchased.

Figure 10. The primary source of threat intelligence used by your organization



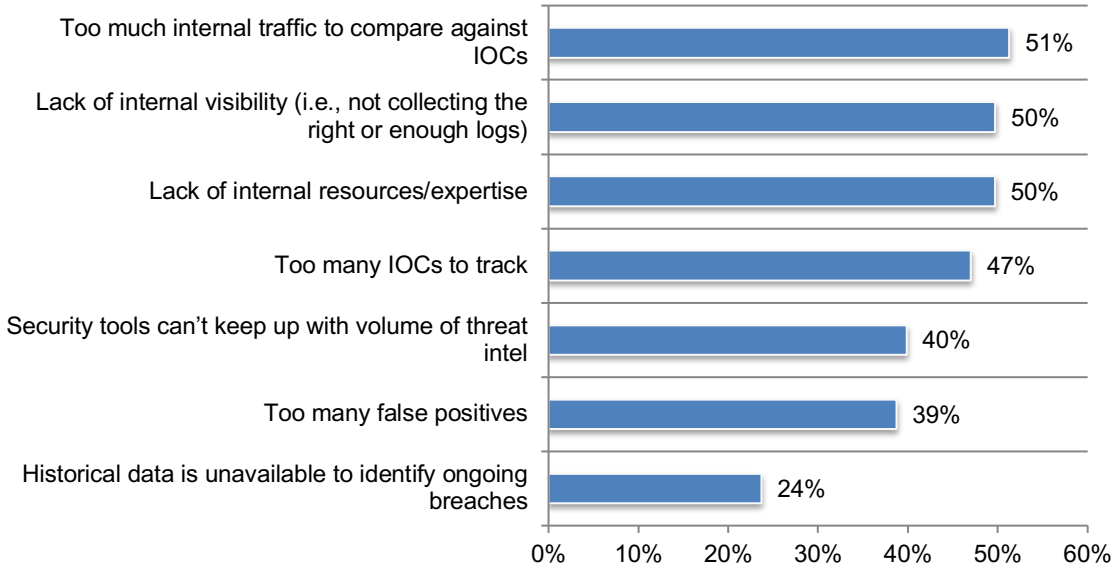
Threat intelligence data is very important to threat hunting teams. As shown in Figure 11, 43 percent of respondents say their organization has a dedicated threat hunting team within its IT security function. On average, these companies have four threat hunters on these teams. Seventy-one percent of respondents rate the importance of threat intelligence to their threat hunting team as very high.

Figure 11. Does your organization have a dedicated threat hunting team within its IT security function?



Threat hunting teams are understaffed making it difficult to compare the significant amount of internal traffic to IOCs. According to Figure 12, 51 percent of respondents say there is too much internal traffic to compare against IOCs and 50 percent of respondents say there is a lack of internal visibility due to not collecting the right or enough logs, and internal resources and expertise are not sufficient.

Figure 12. Challenges the threat hunting team face
Three responses permitted

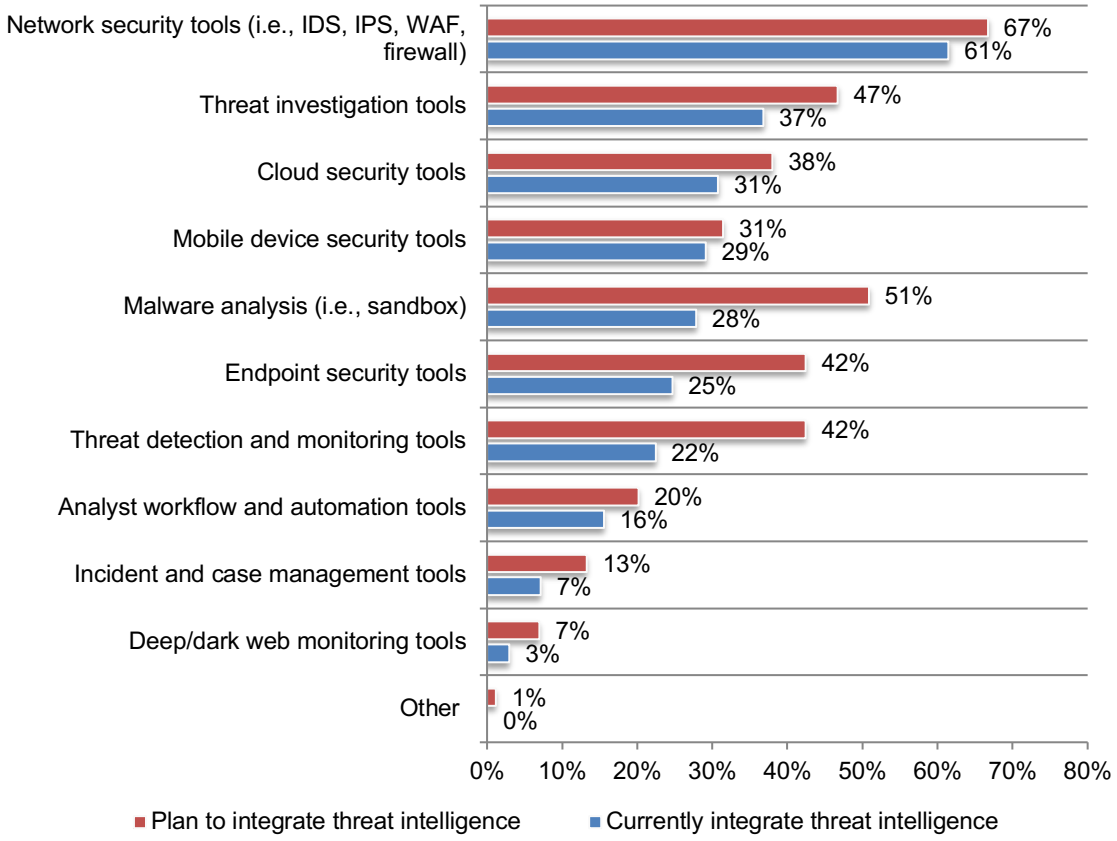


Threat intelligence integration and platforms

Integration of threat intelligence into malware analysis, endpoint security tools and threat detection monitoring tools is expected to increase significantly in the coming year. Figure 13 presents a list of tools organizations are integrating threat intelligence into.

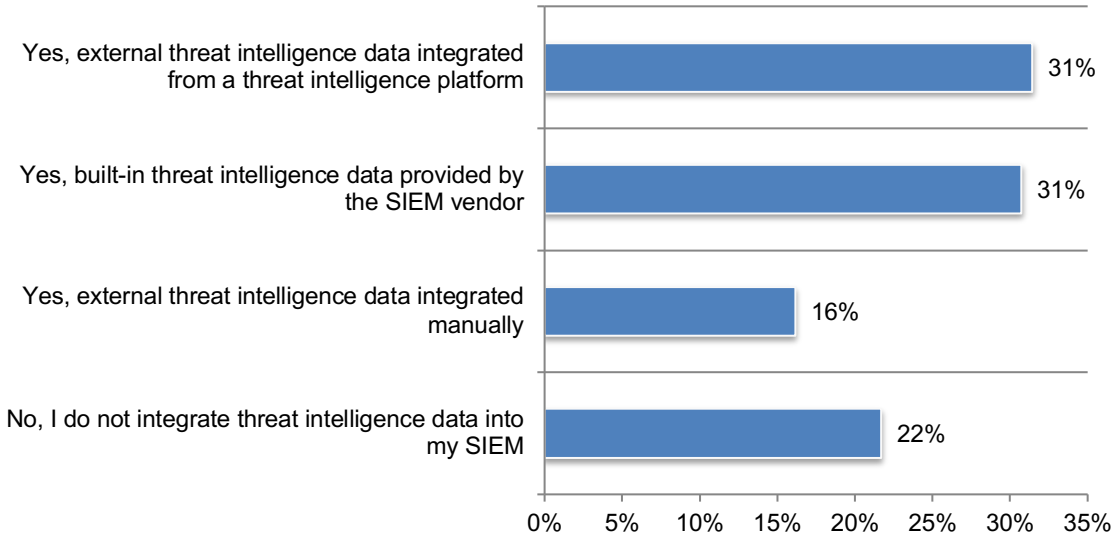
Network security tools are the most commonly used for threat intelligence integration (61percent of respondents). Expected to increase significantly are malware analysis (28 percent of respondents to 51 percent of respondents), endpoint security tools (25 percent of respondents to 42 percent of respondents) and threat detection and monitoring tools (22 percent of respondents to 42 percent of respondents).

Figure 13. Tools used today and in the future for threat intelligence integration
More than one response permitted



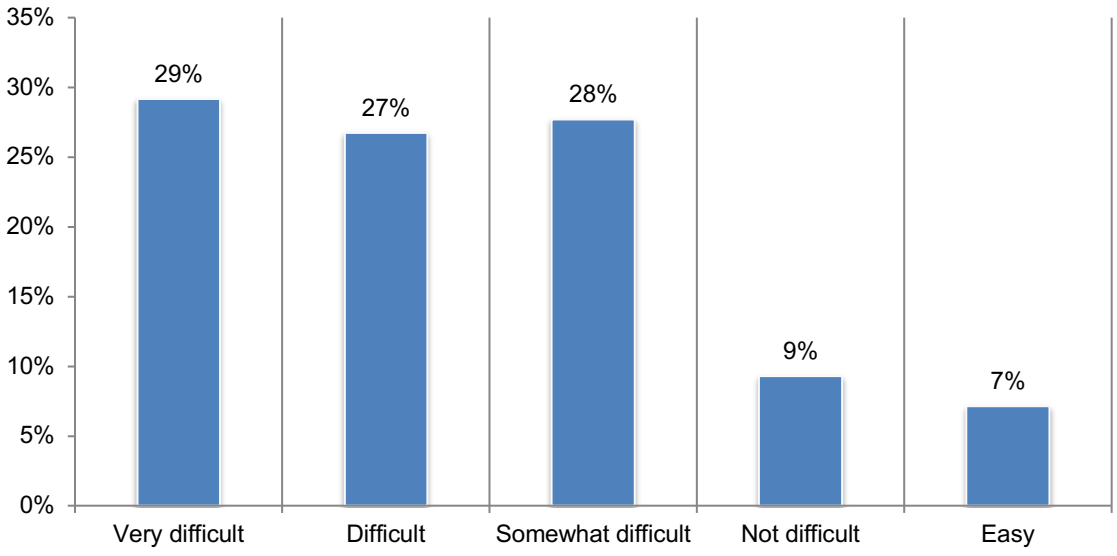
Most organizations are integrating threat intelligence data with its SIEM. According to Figure 14, only 22 percent of respondents are not integrating threat intelligence into its SIEM. The most common integrations are external intelligence data integrated from a threat intelligence platform or built-in threat intelligence data provided by the SIEM vendor.

Figure 14. Does your organization integrate threat intelligence data with its SIEM?



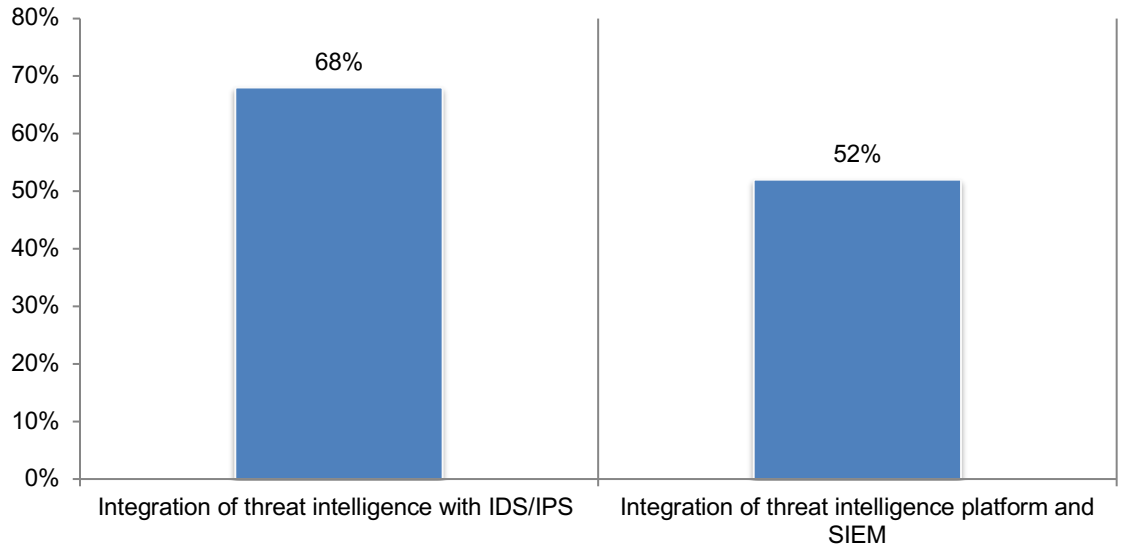
Integration of threat intelligence with the SIEM platform is difficult. According to Figure 15, only 16 percent of respondents say integration was not difficult or easy.

Figure 15. How difficult was the integration of threat intelligence in your organization's SIEM?



Despite the difficulty, integration with IDS/IPS and SIEM is considered valuable in improving an organization's use of threat intelligence. Respondents were asked to rate the value of integration with SIEM and IDS/IPS from 1 = no value to 5 = high value. Figure 16 shows the 4+ responses. Sixty-eight percent of respondents say their IDS/IPS integration is very valuable and 52 percent of respondents say their SIEM integration is very valuable.

Figure 16. The value received from integration with SIEM and IDS/IPS
1 = low value to 5 = high value, 4+ responses presented

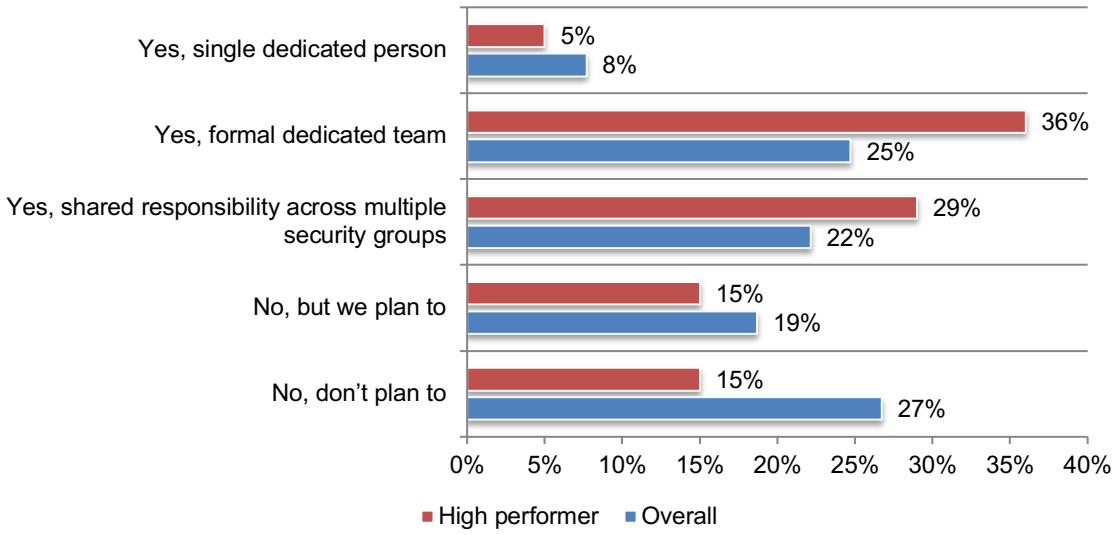


Best practices in high performing organizations

In this section of the report, we present a special analysis of 198 respondents who self-reported that their companies are highly effective in detecting external threats. To understand the threat intelligence practices and strategies that make these organizations more successful, we compare their responses to the overall sample.

High performing organizations are more likely to have resources that focus on threat detection. As shown in Figure 17, 41 percent of high performing organization have resources that focus on threat detection vs. only 33 percent of respondents in the overall sample.

Figure 17. Does your organization have resources that focus on threat detection?

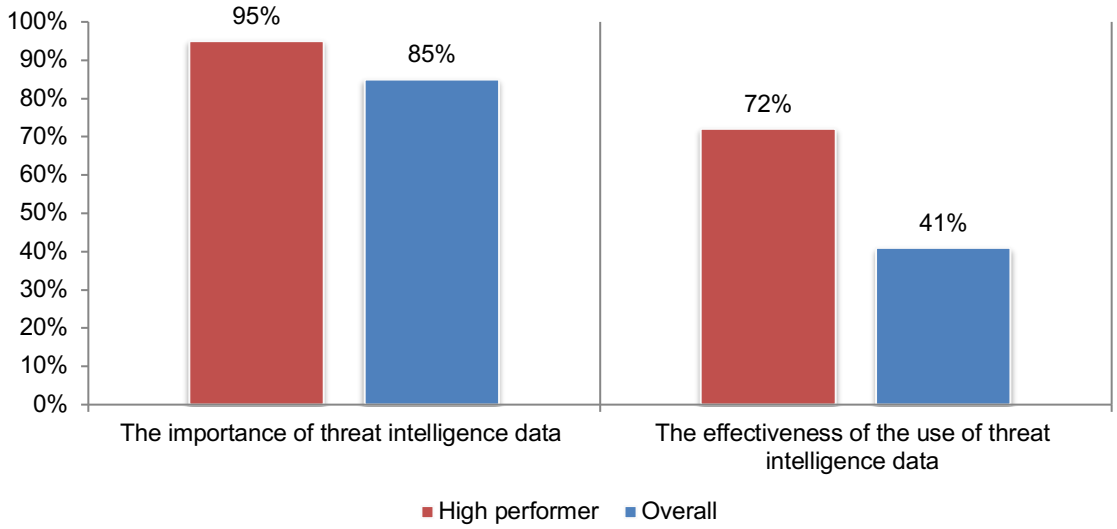


High performing organizations are highly effective in using threat intelligence data as part of their threat detection efforts. As shown in Figure 18, almost all respondents in high performing organizations (95 percent) say threat intelligence data is very important to their organizations' security threat detection efforts. Eighty-five percent of respondents in the overall sample rate the importance as very high.

Seventy-two percent of respondents in high performing organizations rate their organizations' use of threat intelligence data as part of its threat detection efforts as highly effective. In contrast, 41 percent of respondents in the overall sample rate their effectiveness as very high.

Figure 18. The importance of threat intelligence data and effectiveness in the use of threat intelligence data

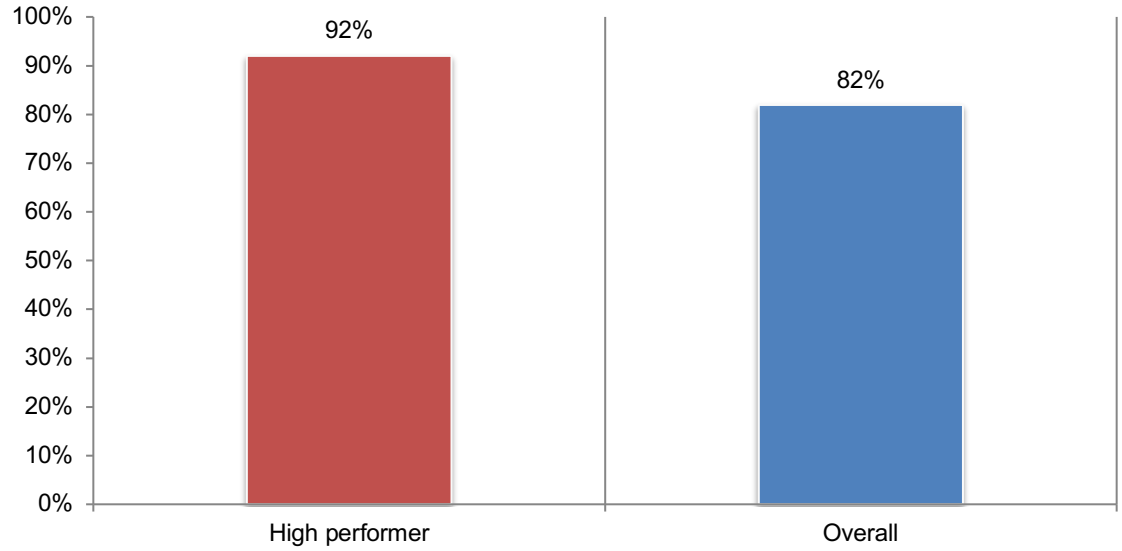
1 = low to 10 = high, 7+ responses only



High performing organizations value information about their adversaries. As shown in Figure 19, virtually all high performing organizations want to understand the motivations, infrastructure and methods of attackers.

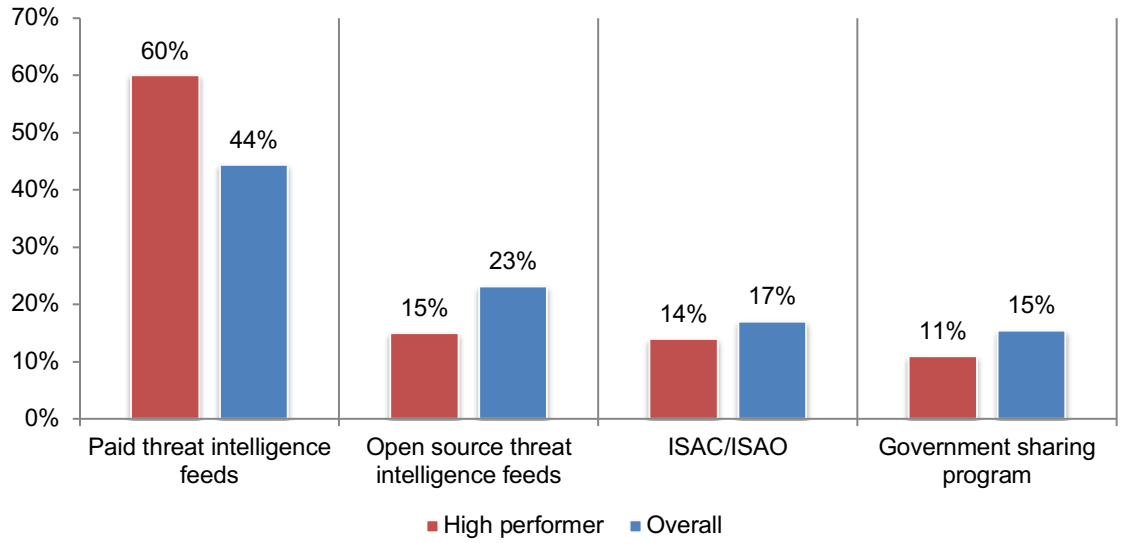
Figure 19. The importance of knowing adversaries, their motivations, infrastructure and methods

1 = low importance to 10 = high importance, 7+ responses



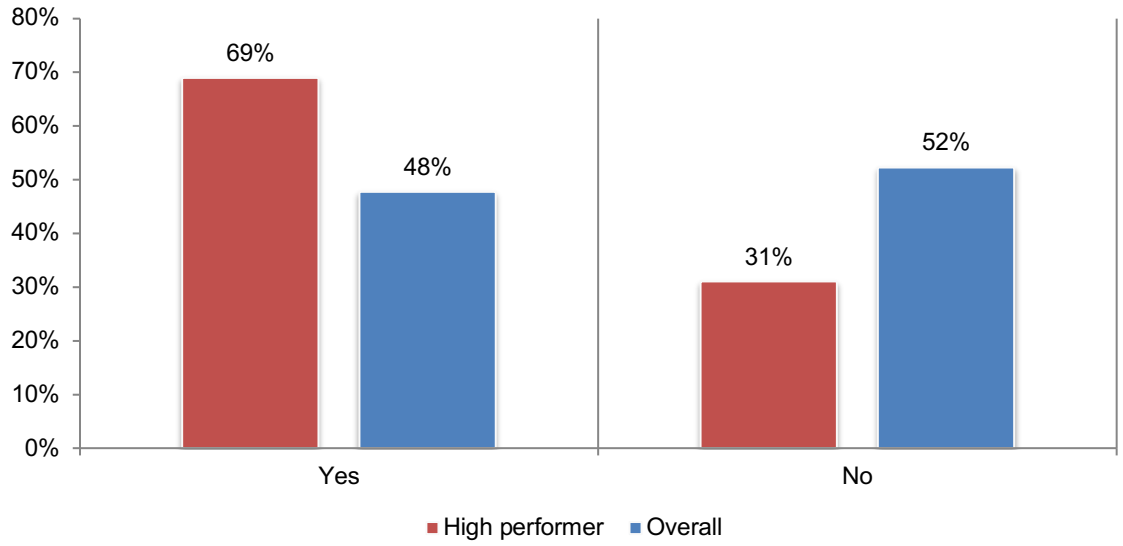
High performing organizations pay for threat intelligence. As shown in Figure 20, 60 percent of respondents say the primary source of threat intelligence is paid threat intelligence feeds. Twenty-three percent of respondents in the overall sample are more likely than high performing organizations to use open source threat intelligence feeds.

Figure 20. What is the primary source of threat intelligence used by your organization?



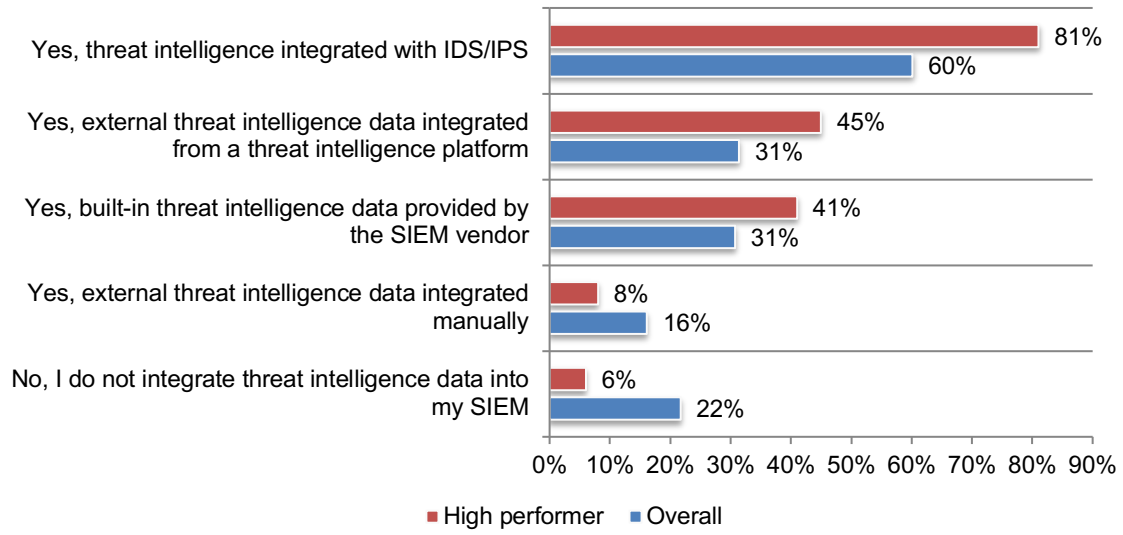
High performing organizations have a dedicated threat intelligence platform. As shown in Figure 21, 69 percent of respondents in high performing organizations have a dedicated threat intelligence platform but less than half (48 percent) of respondents in the overall sample.

Figure 21. Does your organization have a dedicated threat intelligence platform?



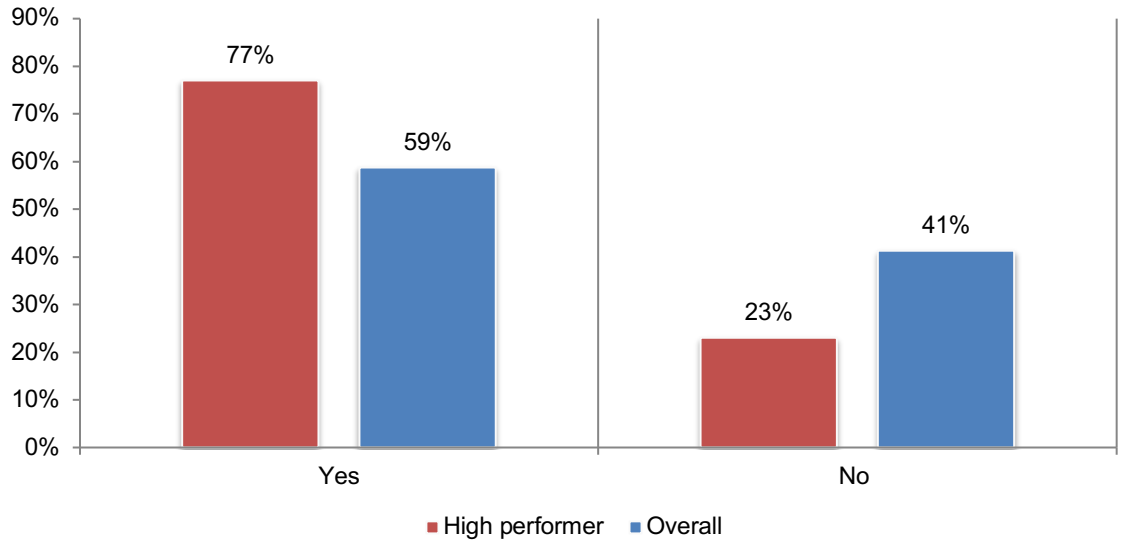
High performing organizations integrate threat intelligence with its SIEM and IDS/IPS. According to Figure 22, 86 percent of respondents in high performing organization either integrate threat intelligence data from a threat intelligence platform (45 percent) or integrate built-in threat intelligence data provided by the SIEM vendor (41 percent). Eighty-one percent of respondents in high performing organization say their organizations integrate threat intelligence with their IDS/IPS. High performing organizations also report that the integration with SIEM and IDS/IPS was not as difficult as the overall sample believes.

Figure 22. Does your organization integrate threat intelligence data with its SIEM and/or IDS/IPS?



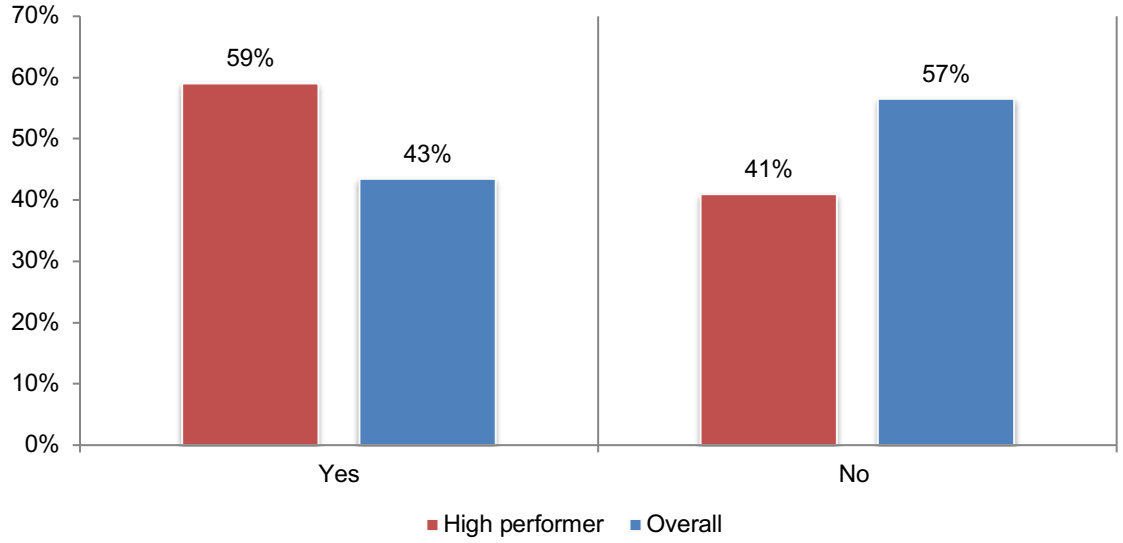
High performing organizations share intelligence with other organizations. According to Figure 23, 77 percent of respondents in high performing organizations share threat intelligence with other organizations vs. 59 percent of respondents in the overall sample.

Figure 23. Does your organization share threat intelligence with other organizations?



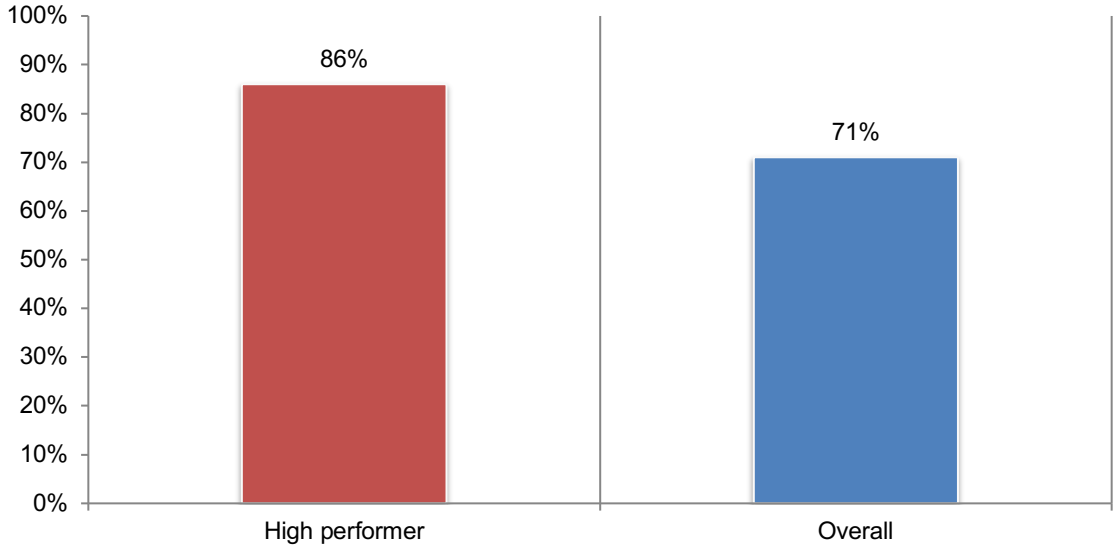
The majority of high performing organizations have a dedicated threat hunting team. As shown in Figure 24, 59 percent of high performing organizations have a dedicated threat hunting team vs. 43 percent of respondents in the overall sample.

Figure 24. Does your organization have a dedicated threat hunting team within its IT security function?



Threat intelligence is important to high performing organizations' threat hunting team. Eighty-six percent of high performing organizations believe threat intelligence is important for their threat hunting teams. Most of the overall sample (71 percent of respondents) believe threat intelligence is critical for their threat hunting teams.

Figure 25. The importance of threat intelligence data to an organization's threat hunting team 1 = low importance to 10 = high importance, 7+ responses



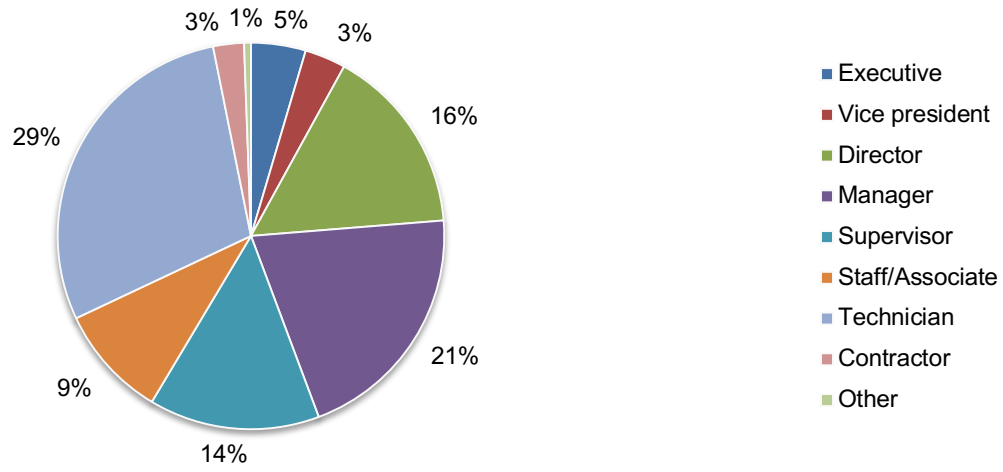
Part 3. Methods

A sampling frame of 29,058 IT or IT security practitioners located in North America and the United Kingdom were selected as participants in the research. Table 1 shows that there were 1,216 total returned surveys. Screening and reliability checks led to the removal of 118 surveys. Our final sample consisted of 1,098 surveys, a 3.8 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	29,058	100.0%
Total returns	1,216	4.2%
Rejected or screened surveys	118	0.4%
Final sample	1,098	3.8%

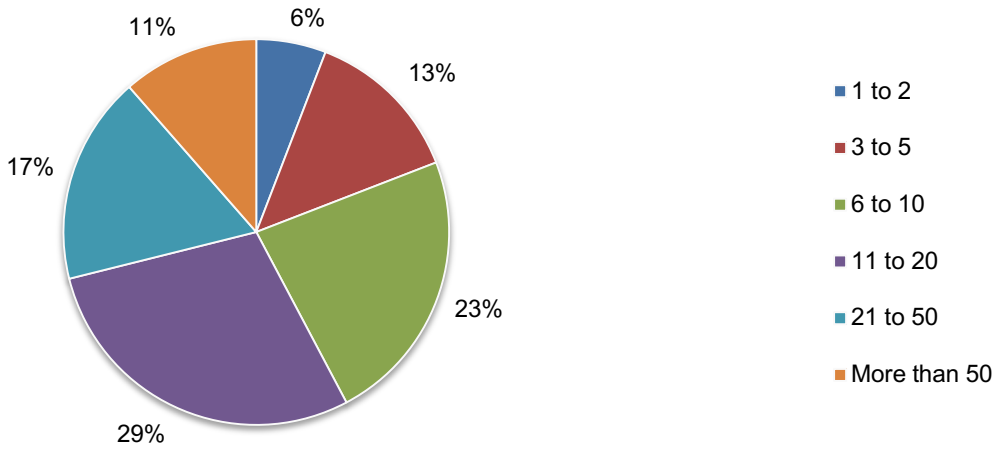
Pie Chart 1 reports the respondents' organizational level within participating organizations. By design, more than half of respondents (59 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



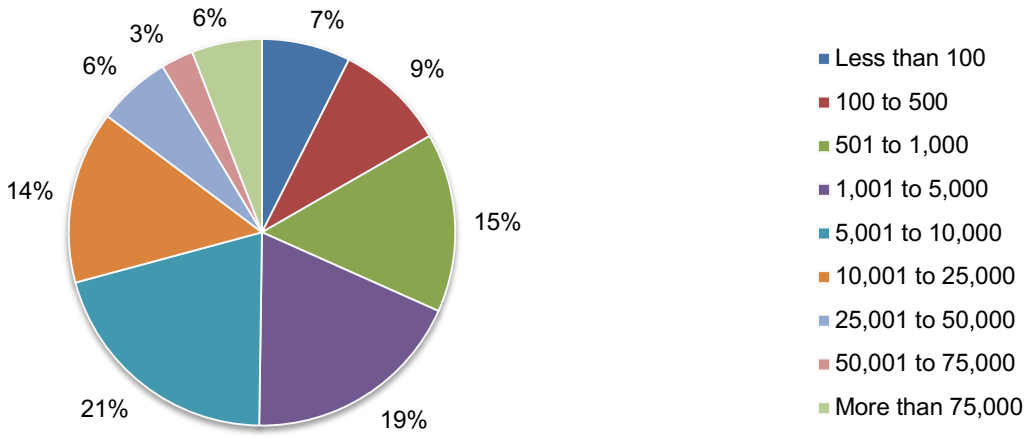
As Pie Chart 3 illustrates, 52 percent of the respondents' organizations have between 6 to 20 dedicated IT security employees.

Pie Chart 3. Employees are dedicated to IT security



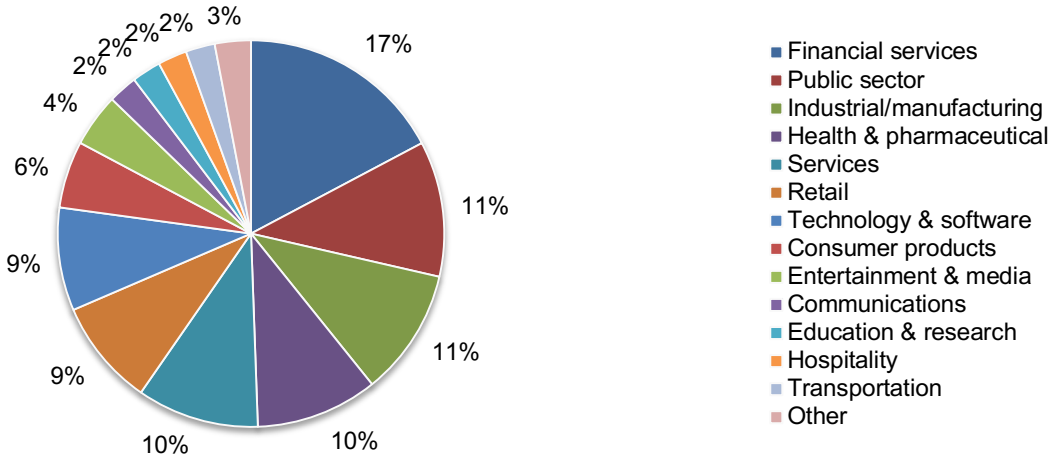
As Pie Chart 3 illustrates, 50 percent of the respondents are from organizations with a global headcount exceeding 5,000 employees.

Pie Chart 3. Global employee headcount of the organization



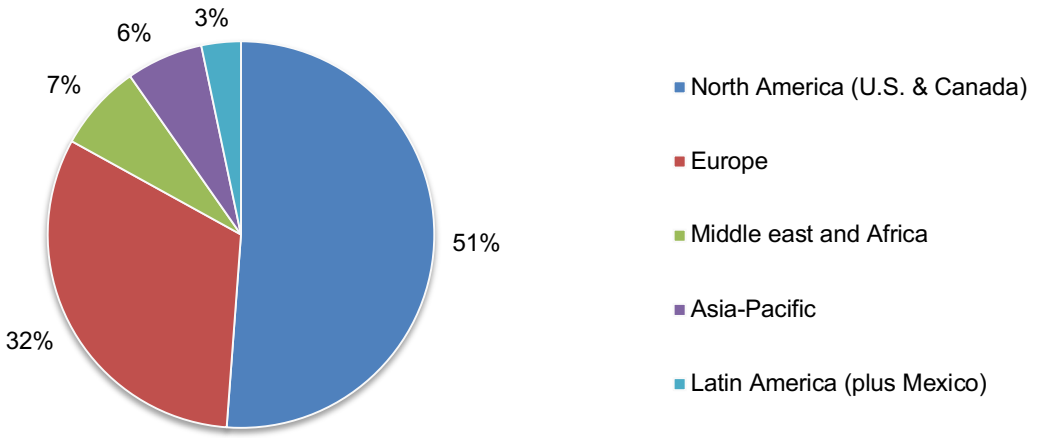
Pie Chart 4 reports the industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by public sector (11 percent of respondents), industrial/manufacturing (11 percent of respondents), health and pharmaceuticals (10 percent of respondents) and service sector (10 percent of respondents).

Pie Chart 4. Primary industry segment



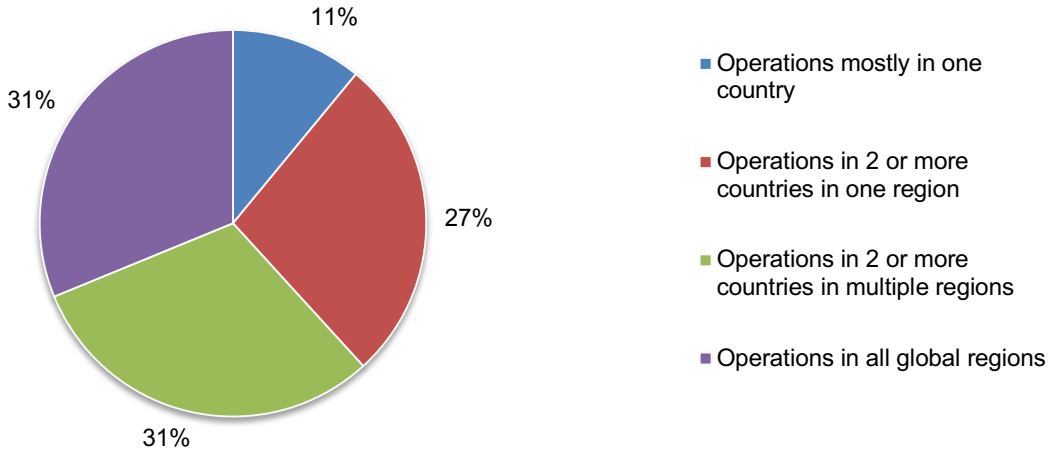
As shown in Pie Chart 5, more than half (51 percent) of the respondents' organizations are headquartered in North America and 32 percent of respondents are headquartered in Europe.

Pie Chart 5. Headquarter location of the organization



Pie Chart 6 reports the global footprint of respondents' organization. Thirty-one percent of the respondents have operations in mostly one country, 31 percent of the respondents have operations in 2 or more countries in in multiple regions, 27 percent of respondents have operations in 2 or more countries in one region and 11 percent of respondents have operations in all global regions.

Pie Chart 6. Organizations' 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 of this survey is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners located in the North America 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 have resulted 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 between July 19 to August 6, 2018.

Survey response	FY 2018	FY 2017
Sampling frame	29,058	30,570
Total returns	1,216	1,201
Rejected or screened surveys	118	130
Final sample	1,098	1,071
Response rate	3.78%	3.50%

Part 1. Screening questions

S1a. Does your organization utilize threat intelligence as part of its cybersecurity program or infrastructure?	FY 2018	FY 2017
Yes (skip to S2a)	76%	74%
No	24%	26%
Total	100%	100%

S1b. If no, why not?	FY 2018	FY 2017
Not considered a priority	16%	23%
Lack of qualified staff	57%	53%
Lack of technologies	38%	42%
Protection-based technologies are sufficient	30%	
Other (please specify)	2%	2%
Total	144%	120%

(Stop)

S2a. Does your organization include **threat intelligence** in its cybersecurity program?	FY 2018
Yes (skip to S3)	74%
No	26%
Total	100%

S2b. If no, why not?	FY 2018
Not considered a priority	14%
Lack of qualified staff	53%
Lack of technologies	37%
Lack of budget to use for threat intelligence	37%
Not enough return on investment (ROI)	33%
Threat intelligence is not useful to pinpoint threats	18%
None of the above	24%
Total	216%

(Stop)

S3. What best defines your organizational role or function with respect to its cybersecurity program?	FY 2018	FY 2017
Security leader (e.g., CISO, CIO)	20%	22%
Threat analyst	13%	13%
Threat hunter	12%	
Threat intelligence analyst	6%	
Security operations	20%	32%
Security systems engineering	9%	4%
Security architecture	6%	5%
Policy / compliance	6%	7%
Incident response / disaster recovery	9%	11%
None of the above (stop)	0%	0%
Total	100%	95%

S4. What best defines your level of involvement in your organization's IT security operations?	FY 2018
Continuous involvement	50%
Daily involvement	32%
Weekly involvement	12%
Monthly involvement	7%
Minimal to no involvement (stop)	0%
Total	100%

Part 2. Organizational characteristics

D1. What best defines your position level within the organization?	FY 2018	FY 2017
Executive	5%	6%
Vice president	3%	
Director	16%	17%
Manager	21%	22%
Supervisor	14%	15%
Staff/Associate	9%	10%
Technician	29%	27%
Contractor	3%	3%
Other	1%	0%
Total	100%	100%

D2. How many employees are dedicated to IT security in your organization?	FY 2018
1 to 2	6%
3 to 5	13%
6 to 10	23%
11 to 20	29%
21 to 50	17%
More than 50	11%
Total	100%
Extrapolated value	20%

D3. What best defines the global employee headcount of your organization?	FY 2018	FY 2017
Less than 100	7%	1%
100 to 500	9%	15%
501 to 1,000	15%	16%
1,001 to 5,000	19%	22%
5,001 to 10,000	21%	16%
10,001 to 25,000	14%	10%
25,001 to 50,000	6%	9%
50,001 to 75,000	3%	7%
More than 75,000	6%	5%
Total	100%	100%
Extrapolated value	13,479	

D4. What best defines your organization's primary industry segment?	FY 2018	FY 2017
Agriculture & food services	1%	0%
Communications	2%	2%
Consumer products	6%	5%
Defense & aerospace	1%	1%
Education & research	2%	2%
Entertainment & media	4%	2%
Financial services	17%	17%
Health & pharmaceutical	10%	10%
Hospitality	2%	3%
Industrial/manufacturing	11%	10%
Public sector	11%	11%
Retail	9%	9%
Services	10%	10%
Technology & software	9%	9%
Transportation	2%	3%
Other	1%	0%
Total	100%	95%

D5. Where is your organization headquartered? Please choose only one region.	FY 2018	FY 2017
North America (U.S. & Canada)	51%	58%
Europe	32%	29%
Middle east and Africa	7%	3%
Asia-Pacific	6%	6%
Latin America (plus Mexico)	3%	3%
Total	100%	100%

D6. What best defines your organization's global footprint? Please select only one choice	FY 2018	FY 2017
Operations mostly in one country	11%	12%
Operations in 2 or more countries in one region	27%	27%
Operations in 2 or more countries in multiple regions	31%	33%
Operations in all global regions	31%	29%
Total	100%	100%

Part 3. The state of threat detection in organizations

Q1. What threats worry you most? Please select your top three choices.	FY 2018
Industrial control system malware/attacks	51%
IoT device vulnerabilities and attacks	37%
Nation-state attacks	36%
Theft of high value data (financial/intellectual property)	52%
APT-based attacks	57%
Ransomware	33%
Phishing	24%
Traditional malware	8%
Other (please specify)	2%
Total	300%

Q2. What threats take up most of your IT security team's time? Please select your top three choices.	FY 2018
Industrial control system malware/attacks	21%
IoT device vulnerabilities and attacks	25%
Nation-state attacks	21%
Theft of high value data (financial/intellectual property)	55%
APT-based attacks	62%
Ransomware	36%
Phishing	46%
Traditional malware	33%
Other (please specify)	1%
Total	300%

Q3. Does your organization have resources that focus on threat detection?	FY 2018
Yes, single dedicated person	8%
Yes, formal dedicated team	25%
Yes, shared responsibility across multiple security groups	22%
No, but we plan to	19%
No, don't plan to	27%
Total	100%

Q4. Using the following 10-point scale, please rate your organization's overall effectiveness in detecting external threats. 1 = low effectiveness to 10 = high effectiveness.	FY 2018
1 or 2	7%
3 or 4	13%
5 or 6	39%
7 or 8	24%
9 or 10	18%
Total	100%
Extrapolated average	6.17

Part 4. Threat intelligence practices

Q5. Using the following 10-point scale, please rate the **importance** of threat intelligence data to your organization's security threat detection efforts. 1 = low importance to 10 = high importance	FY 2018	FY 2017
1 or 2	0%	1%
3 or 4	1%	4%
5 or 6	14%	11%
7 or 8	24%	25%
9 or 10	61%	59%
Total	100%	100%
Extrapolated average	8.40	8.23

Q6. Using the following 10-point scale, please rate the **effectiveness** of your organization's use of threat intelligence data as part of it threat detection efforts. 1 = low effectiveness to 10 = high effectiveness	FY 2018	FY 2017
1 or 2	9%	7%
3 or 4	16%	16%
5 or 6	33%	36%
7 or 8	26%	25%
9 or 10	15%	16%
Total	100%	100%
Extrapolated average	5.95	6.05

Q7. Using the following 10-point scale, please rate the importance of knowing your adversaries, their motivations, their infrastructure and their methods. 1 = low importance to 10 = high importance	FY 2018
1 or 2	0%
3 or 4	6%
5 or 6	12%
7 or 8	24%
9 or 10	58%
Total	100%
Extrapolated average	8.18

Q8. What is the primary source of threat intelligence used by your organization? Please select all that apply.	FY 2018	FY 2017
Open source threat intelligence feeds	23%	24%
Paid threat intelligence feeds	44%	41%
ISAC/ISAO	17%	17%
Government sharing program	15%	18%
Other (please specify)	0%	0%
Total	100%	100%

Q9. Approximately, how many threat intelligence feeds are used by your organization today?	FY 2018	FY 2017
One	22%	22%
2 to 5	25%	21%
6 to 10	29%	30%
11 to 20	19%	21%
21 to 40	5%	4%
More than 40	0%	2%
Total	100%	100%
Extrapolated average	7.73	8.58

Q10. Approximately, how many threat intelligence sources do you pay for?	FY 2018
One	41%
2 to 5	43%
6 to 10	11%
11 to 20	4%
21 to 40	0%
More than 40	0%
Total	100%
Extrapolated average	3.47

Q11. Does your organization **currently integrate** threat intelligence into the following tools? Please select all that apply.	FY 2018	FY 2017
Malware analysis (i.e. sandbox)	28%	58%
Endpoint security tools	25%	34%
Network security tools (i.e. IDS, IPS, WAF, firewall)	61%	55%
Cloud security tools	31%	
Mobile device security tools	29%	
Threat detection and monitoring tools	22%	
Threat investigation tools	37%	
Analyst workflow and automation tools	16%	15%
Incident and case management tools	7%	15%
Deep/dark web monitoring tools	3%	
Other	0%	2%
Total	259%	179%

Q12. Does your organization **plan to integrate** threat intelligence into the following tools in the next 12 months? Please select all that apply.	FY 2018
Malware analysis (i.e. sandbox)	51%
Endpoint security tools	42%
Network security tools (i.e. IDS, IPS, WAF, firewall)	67%
Cloud security tools	38%
Mobile device security tools	31%
Threat detection and monitoring tools	42%
Threat investigation tools	47%
Analyst workflow and automation tools	20%
Incident and case management tools	13%
Deep/dark web monitoring tools	7%
Other (please specify)	1%
Total	360%

Threat intelligence platform is an enabling technology that helps enterprises aggregate and correlate incoming threat data from many different sources and speed the process of digging out the relevant indicators of compromise. Threat intelligence platforms provide a single funnel for channeling and analyzing threat data emanating from disparate sources and open-source organizations that provide notifications of new or emerging exploits and vulnerabilities.

Q13a. Does your organization have a dedicated threat intelligence platform?	FY 2018
Yes	48%
No (skip to Q19a)	52%
Total	100%

Q13b. If yes, what is your organization's primary SIEM platform?	FY 2018
ArcSight	16%
Splunk	16%
IBM QRadar	14%
LogRhythm	12%
McAfee	10%
Exabeam	4%
Rapid7	5%
Securonix	6%
AlienVault	14%
Other (please specify)	4%
Total	100%

Q14. How long is data kept live and online in your organization's SIEM?	FY 2018	FY 2017
Less than 1 day	4%	1%
1 to 7 days	14%	13%
1 to 4 weeks	35%	32%
1 to 3 months	22%	25%
4 to 6 months	10%	14%
7 to 12 months	8%	11%
More than 2 years	6%	4%
Total	100%	100%
Extrapolated value (days)	100	100

Q15. Does your organization integrate threat intelligence data with its SIEM?	FY 2018
Yes, built-in threat intelligence data provided by the SIEM vendor	31%
Yes, external threat intelligence data integrated manually	16%
Yes, external threat intelligence data integrated from a threat intelligence platform	31%
No, I do not integrate threat intelligence data into my SIEM	22%
Total	100%

Q16. Does the integration of threat intelligence data in your organization's SIEM diminish the performance of the SIEM?	FY 2018	FY 2017
Yes, significant diminishment	13%	22%
Yes, some diminishment	24%	34%
Yes, minimal diminishment	30%	23%
No diminishment	33%	21%
Total	100%	100%

Q17. How difficult was the integration of threat intelligence in your organization's SIEM?	FY 2018
Very difficult	29%
Difficult	27%
Somewhat difficult	28%
Not difficult	9%
Easy	7%
Total	100%

Q18. How would you rate the value received from the integration of your organization's threat intelligence platform and SIEM? 1 = low value to 5 = high value.	FY 2018
1	14%
2	14%
3	19%
4	27%
5	25%
Total	100%

Q19a. Do you integrate threat intelligence data with your IDS/IPS?	FY 2018	FY 2017
Yes, full integration	60%	66%
No (Skip to Q22a)	40%	34%
Total	100%	100%

Q19b. If yes, how does your organization integrate threat intelligence data with IDS/IPS?	FY 2018
Built-in threat intelligence data provided by the IDS/IPS vendor	49%
External threat intelligence data integrated manually	22%
External threat intelligence data integrated from a threat intelligence platform	29%
Total	100%

Q20. How difficult was it to integrate threat intelligence data with your organization's IDS/IPS?	FY 2018	FY 2017
Very difficult	24%	25%
Difficult	30%	32%
Somewhat difficult	17%	25%
Not difficult	25%	15%
Easy	5%	3%
Total	100%	100%

Q21. How would you rate the value received from the integration of threat intelligence with your organization's IDS/IPS 1 = low value to 5 = high value	FY 2018
1	6%
2	10%
3	16%
4	40%
5	28%
Total	100%

Q22a. Does your organization share threat intelligence with other organizations?	FY 2018
Yes (skip to Q23)	59%
No	41%
Total	100%

Q22b. If no, why doesn't your organization share threat intelligence with other organizations?	FY 2018
Nothing of value to share	9%
Concerns about the privacy of our corporate data	46%
Concerns about corporate liability	38%
Concerns about the potential for misuse of the data	56%
Lack of expertise in threat intelligence	40%
Concerns about revealing a possible data breach	42%
Concerns about GDPR exposure	20%
None of the above	24%
Other (please specify)	4%
Total	280%

Skip to Q25

Q23. What threat intelligence information sharing protocols does your organization use to share and disseminate threat intelligence data? Please select all that apply.	FY 2018	FY 2017
STIX/TAXII	44%	47%
CyBOX	29%	
Open IOC	36%	39%
Unstructured PDF or CSV	62%	60%
We do not use a standardized communication protocol	24%	24%
Other	2%	2%
Total	196%	171%

Q24a. Do you belong to or participate in an ISAC/ISAO or other industry sharing group?	FY 2018	FY 2017
Yes, inbound ingestion and use of shared intelligence *	36%	30%
Yes, outbound sharing	32%	
No, but evaluating participation (skip to Q25)	29%	
No plans to participate (skip to Q25)	22%	30%
Total	119%	30%

* wording slightly different in 2018

Q24b. If yes, what are the benefits of participation in an ISAC/ISAO or other industry sharing group? Please select all that apply.	FY 2018	FY 2017
Learn about threats affecting organizations similar to us	61%	56%
Ability to collaborate with industry peers about known active threats	57%	55%
Ability to proactively monitor for threats seen by peers	45%	
Ability to integrate knowledge from peers into our organization's threat detection tools	35%	32%
Total	199%	143%

Q25. Does your organization have a dedicated threat hunting team within its IT security function?	FY 2018
Yes	43%
No (skip to Q29)	57%
Total	100%

Q26. How many security threat hunters does your organization have on its threat hunting team?	FY 2018
One	25%
2 to 5	51%
6 to 10	20%
More than 10	3%
Total	100%
Extrapolated value	4.07

Q27. Using the following 10-point scale, please rate the importance of threat intelligence data to your organization's threat hunting team. 1 = low importance to 10 = high importance	FY 2018
1 or 2	2%
3 or 4	11%
5 or 6	16%
7 or 8	19%
9 or 10	52%
Total	100%
Extrapolated average	7.65

Q28. What challenges does your threat hunting team face? Please select the top three choices.	FY 2018
Too many IOCs to track	47%
Too much internal traffic to compare against IOCs	51%
Too many false positives	39%
Security tools can't keep up with volume of threat intel	40%
Historical data is unavailable to identify ongoing breaches	24%
Lack of internal resources/expertise	50%
Lack of internal visibility (i.e. not collecting the right or enough logs)	50%
Other	0%
Total	300%

Part 5. Budget and investments

Q29. What is your annual IT security budget?	FY 2018
Less than $100,000	0%
$101,000 to $500,000	7%
$501,000 to $1,000,000	17%
$1,100,000 to $5,000,000	32%
$5,100,000 to $10,000,000	26%
$10,100,000 to $50,000,000	14%
$50,100,000 to $100,000,000	3%
More than $100,000,000	1%
Total	100%
Extrapolated average	$9,977,150

Q30. Please allocate 100 percentage points to show how your IT security budget is allocated today and will be allocated in the next 12 months.	Today	In the next 12 months
Prevention (i.e. deploying and operating controls to prevent attacks and intrusions)	44%	36%
Basic detection (i.e. data analysis and tools to spot attacks/intrusions)	31%	29%
Advanced detection (i.e. threat hunting, advanced attacker investigation)	16%	21%
Incident response (i.e. taking corrective action to address security incidents)	9%	14%
Total	100%	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.

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