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

Sponsored by Anomali

Independently conducted by Ponemon Institute LLC

Publication Date: September 2017

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

Presented by Ponemon Institute, September 2017

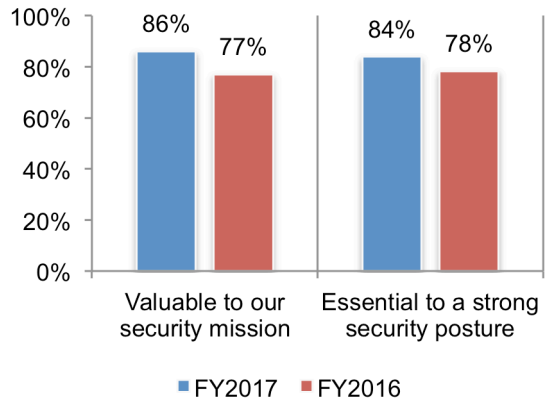
Part 1. Introduction

Ponemon Institute is pleased to present *The Value of Threat Intelligence: The Second 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. This year, 80 percent of North American respondents (628 individuals) say they use threat intelligence, an increase from 65 percent of respondents last year. A total of 1,071 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 but recognize that being able to utilize threat data to pinpoint cyber threats is a challenge.

Participants in this research were asked to rate the value of threat intelligence to their organizations' security mission and its importancewith respect to a strong security posture on a scale from 1 = low to 10 = high. As shown in Figure 1, both the value and importance increased significantly from 2016 (86 percent and 84 percent of respondents, respectively).

Figure 1. The value of threat intelligence
1 = low to 10 = high, 7+ responses



To maximize the value of threat intelligence, respondents believe a threat intelligence platform and integration with SIEM is necessary. Also essential is to have a qualified threat analyst on staff.

Trends in the use of threat intelligence

- A lack of staff expertise continues to be the number one reason the use of threat intelligence is often ineffective and prevents some companies from deploying a threat intelligence platform.
- More than half (51 percent of respondents) say incident responders use threat intelligence when responding to threats, an increase from 46 percent of respondents last year.
- Sixty-three percent of respondents say threat intelligence drives decision-making within their organizations' security operations center (SOC), an increase from 57 percent of respondents in last year's study.
- Effectiveness in using threat data increased significantly. Last year, only 27 percent of respondents gave their organization high marks for their ability to be effective in the use of

threat intelligence. However, 41 percent of respondents this year rate their organizations as highly effective in this regard.

- One reason more respondents do not believe their organizations are highly effective is that threat intelligence data continues to be too voluminous and complex to be actionable.
- Trust is critical when sharing threat intelligence data. Most respondents whose organizations share intelligence report that this sharing is mostly done with trusted security vendors or peer groups.
- While 72 percent of respondents say their organizations engage in threat hunting, only 43 percent of these respondents say such operations are effective because there are too many false positives as well as a lack of expertise.
- Threat intelligence platforms continue to make the prioritization of threat data easier and enable the integration of threat data with other solutions.
- The integration of threat intelligence in an organization's security architecture continues to increase the ability to more quickly research threats. Next generation firewalls (NGFW) and UTMs are the easiest solutions for integration. It is more difficult to achieve integration with endpoint security and IPS/IDS.

Part 2. Key findings

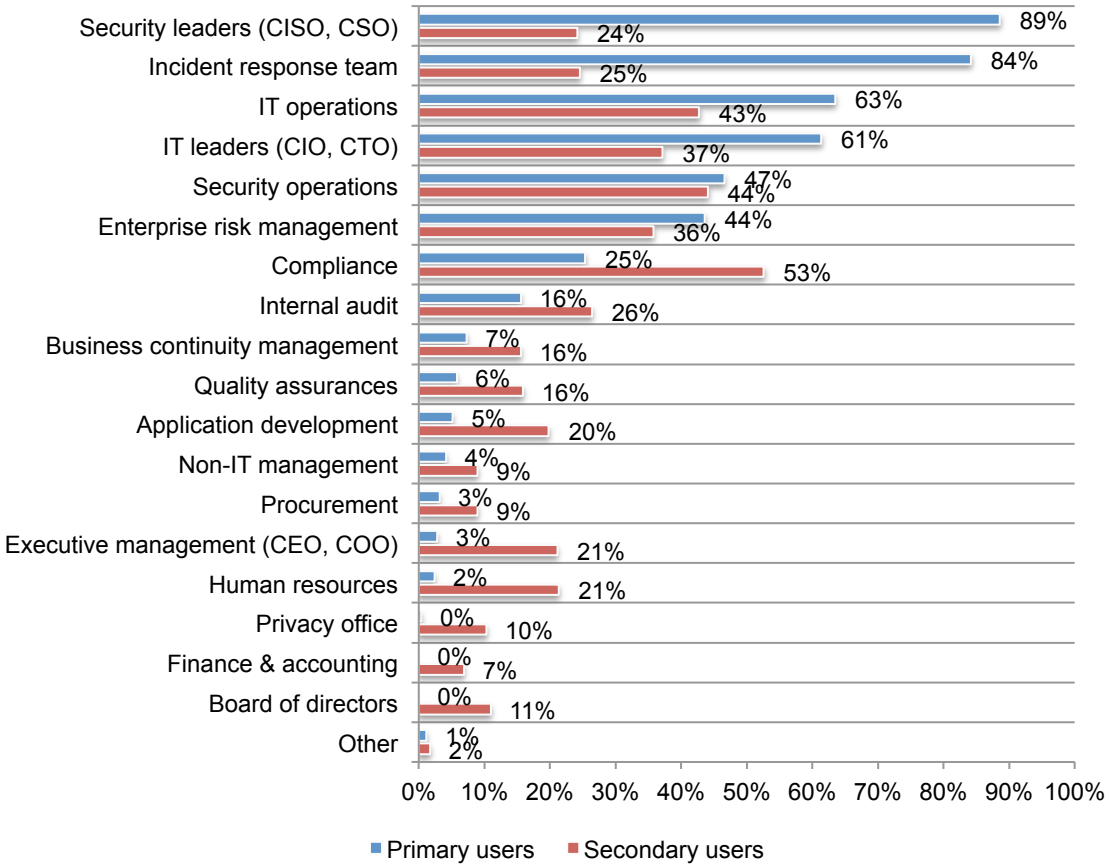
In this section of the report, we provide the detailed findings and trends of the research. The complete findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- The effectiveness of threat intelligence in mitigating risk
- Threat intelligence sharing and threat intelligence platforms
- Threat intelligence integration and performance
- Communication issues in disseminating threat intelligence
- Special analysis: Differences in findings based on position level and headcount

The effectiveness of threat intelligence in mitigating risk

Who benefits from threat intelligence? As shown in Figure 2, the primary users of threat intelligence are security leaders (89 percent of respondents), incident response teams (84 percent of respondents), IT operations (63 percent of respondents) and IT leaders (61 percent of respondents). Secondary users are mainly in compliance (53 percent of respondents) and security operations (44 percent of respondents). More than half (51 percent) of respondents say incident responders use threat data when deciding how to respond to threats, an increase from 46 percent last year. Sixty-three percent of respondents say threat intelligence drives decision-making within their organizations' SOC, an increase from 57 percent of respondents in 2016.

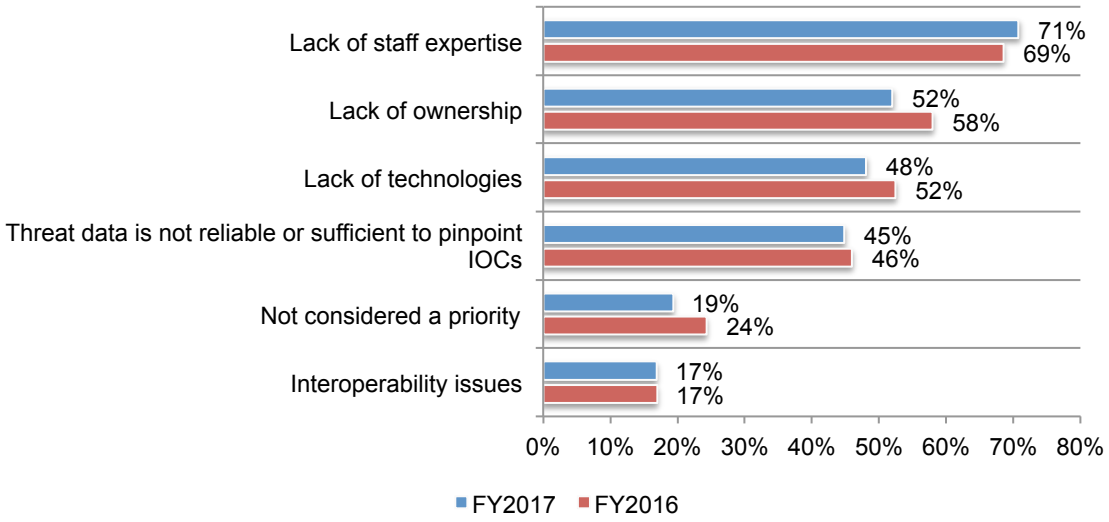
Figure 2. Who are the primary and secondary users of threat intelligence?
More than one choice permitted



More organizations are effective in using threat data. Respondents were asked to rate the effectiveness of their organizations' use of threat data to pinpoint cyber threats on a scale from 1 = low effectiveness to 10 = high effectiveness. Last year, only 27 percent of respondents believed their organizations were very effective in terms of utilizing threat data to pinpoint cyber threats (7+ on a scale from 1 to 10). This year 41, percent of respondents rate their organizations as highly effective.

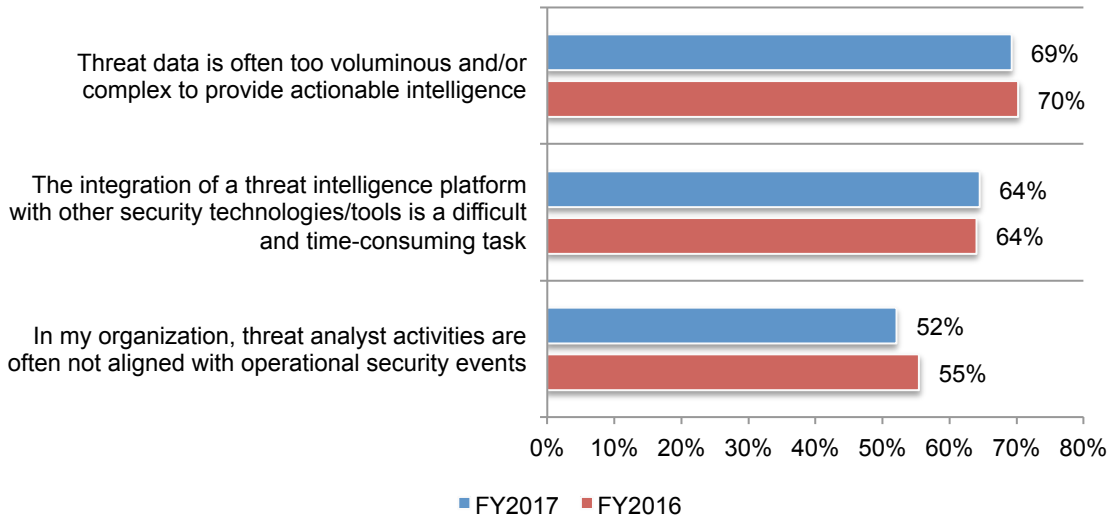
However, 59 percent of respondents do not rate their organizations' effectiveness as high, and Figure 3 presents the reasons why. These include: lack of staff expertise (71 percent of respondents), lack of ownership (52 percent of respondents) and lack of suitable technologies (48 percent of respondents).

Figure 3. Why organizations believe they are ineffective in utilizing threat data
More than one choice permitted



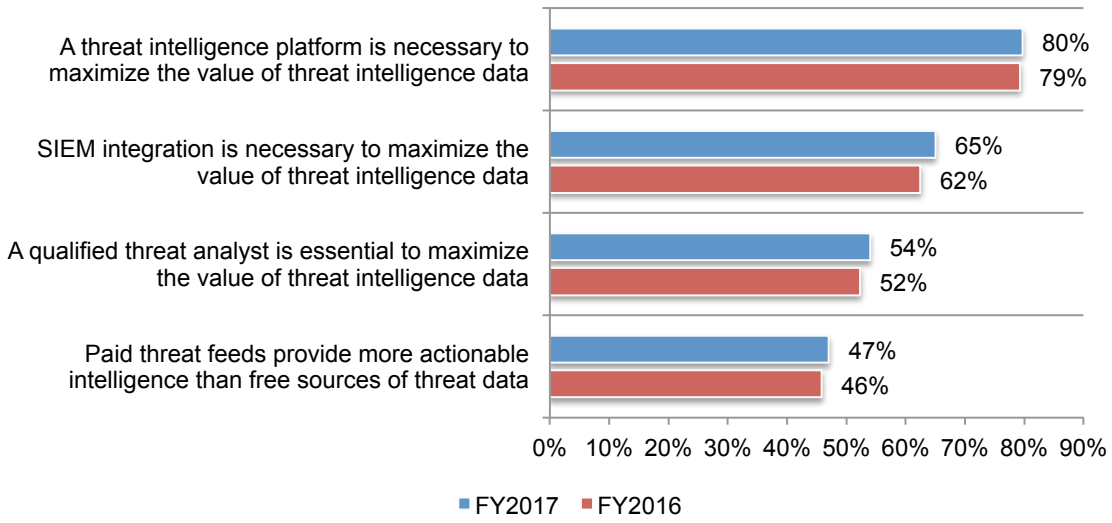
Threat intelligence continues be too voluminous and complex. Figure 4 reveals that, similar to last year's survey data, 69 percent of respondents say threat intelligence is often too voluminous and/or complex to provide actionable intelligence. Other challenges include difficulty in the integration of a threat intelligence platform with other security technologies and tools (64 percent of respondents) and a lack of alignment between analyst activities and operational security events (52 percent of respondents).

Figure 4. Challenges to achieving the effective use of threat intelligence
Strongly agree and *Agree* responses combined



To maximize the effectiveness of threat intelligence, companies need to deploy a threat intelligence platform that is integrated with SIEM. As shown in Figure 5, when asked how companies can make threat intelligence more valuable, respondents expressed a strong belief that the answer is a threat intelligence platform, SIEM integration and a qualified threat analyst

Figure 5. How to maximize the effectiveness of threat intelligence
Strongly agree and *Agree* responses combined

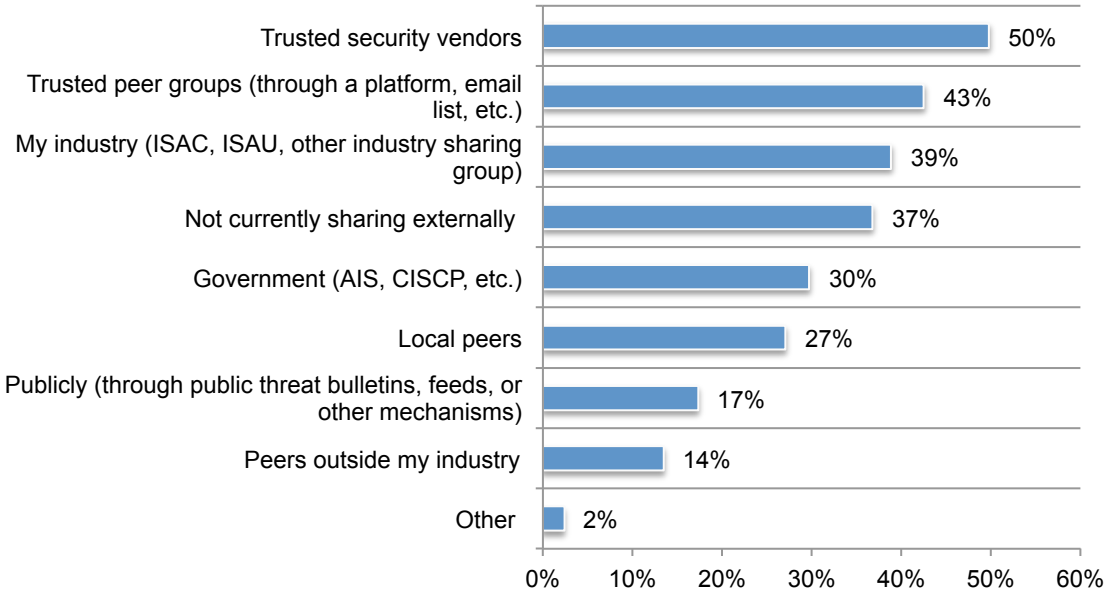


Threat intelligence sharing and threat intelligence platforms

Trust matters when sharing intelligence. Sixty-two percent of respondents say their organizations share intelligence.

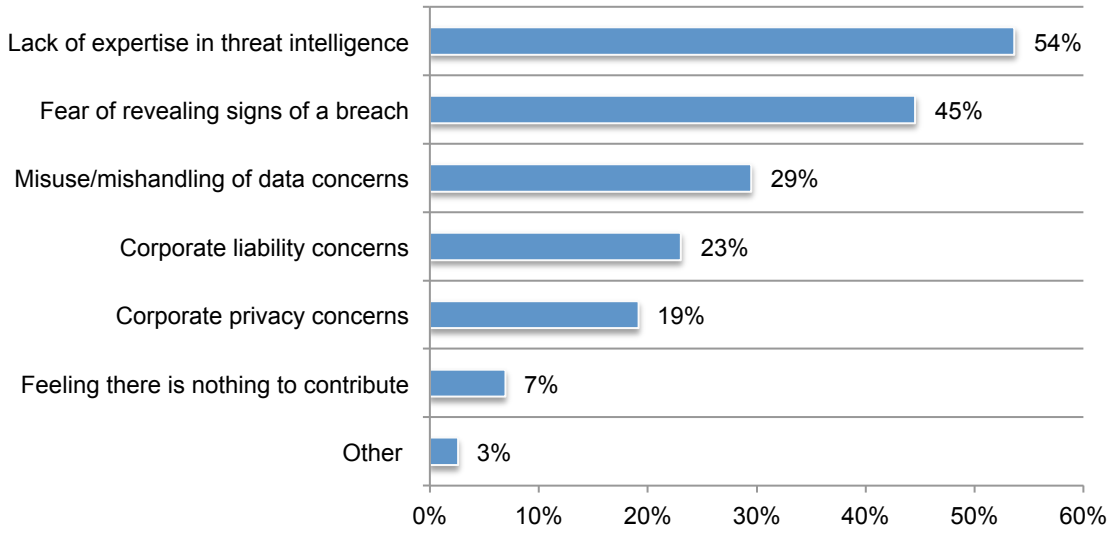
As shown in Figure 6 demonstrates, 50 percent of respondents say their organizations share with trusted security vendors followed by 43 percent of respondents who say their organizations share with trusted peer groups (through a platform, email list, etc.).

Figure 6. Who do you currently share threat intelligence with?
More than one choice permitted



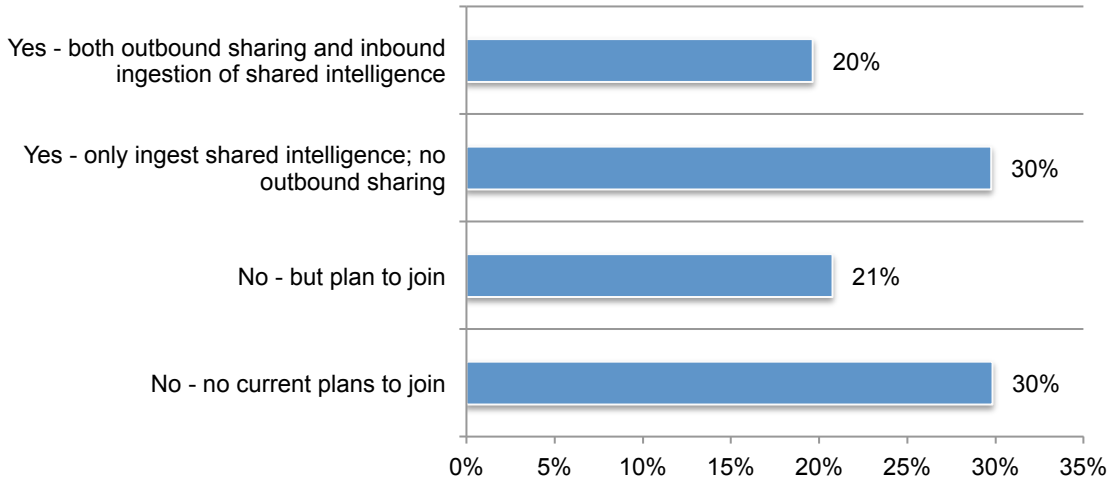
The lack of expertise in threat intelligence stops organizations from sharing threat intelligence. Thirty-eight percent of respondents say their companies are not currently sharing intelligence. The reasons given for not sharing are presented in Figure 7. The primary reasons are lack of expertise in threat intelligence (54 percent of respondents) and fear of revealing signs of a breach (45 percent of respondents).

Figure 7. Why doesn't your organization share threat intelligence?
More than one choice permitted



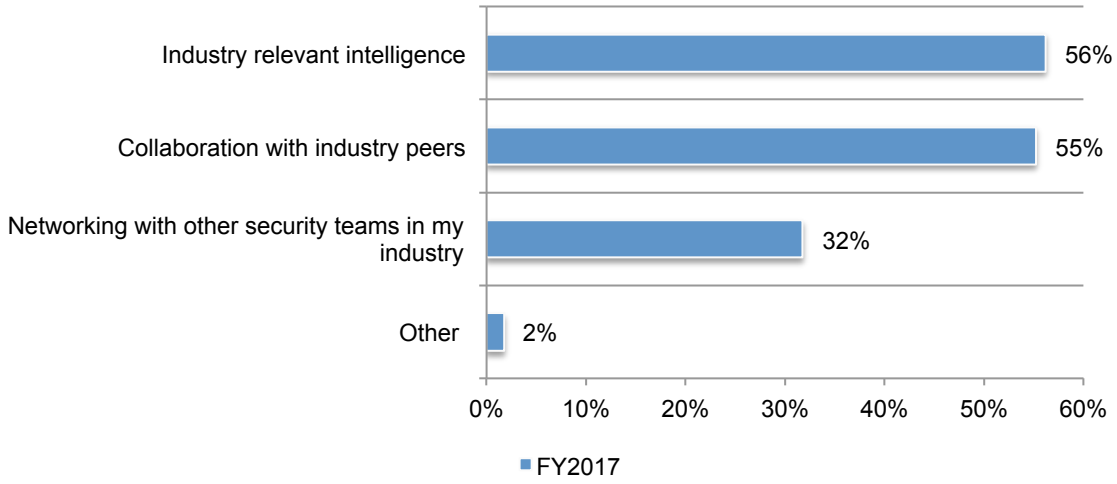
The IT Information Sharing & Analysis Center (ISAC) and the Information Sharing & Analysis Organization (ISAO) exist to facilitate the exchange of threat intelligence. Most companies (70 percent of respondents) either participate in some way with ISAC/ISAO or plan to. Figure 8 shows that 20 percent of respondents say their organizations do both outbound sharing and inbound ingestion of shared intelligence. Thirty percent of respondents only ingest shared intelligence and do not engage in outbound sharing. Twenty-one percent plan to join an industry-specific sharing community.

Figure 8. Do you belong/participate in an ISAC/ISAO or other industry-specific sharing community?



When asked what value their organizations receive from the ISAC, respondents say it is access to industry relevant intelligence (56 percent of respondents) and collaboration with industry peers (55 percent of respondents), as shown in Figure 9.

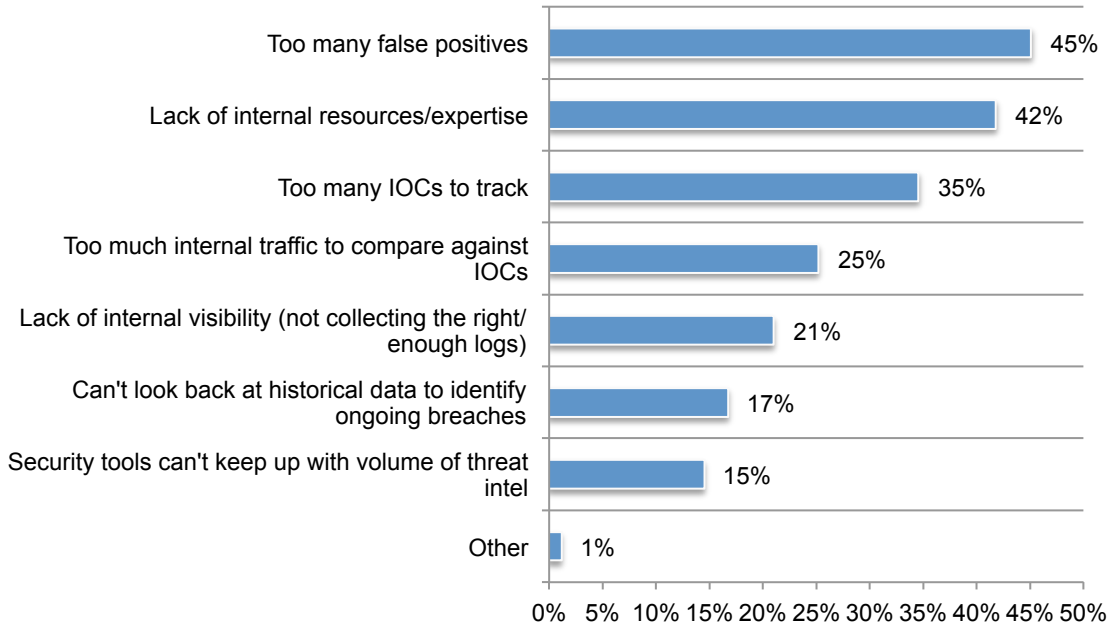
Figure 9. What value do you get from the ISAC?
More than one choice permitted



Too many challenges with threat hunting diminish its effectiveness. Seventy-two percent of respondents conduct threat hunting**.** However, only 43 percent of respondents say their threat hunting operations are very effective (16 percent of respondents) or effective (27 percent of respondents).

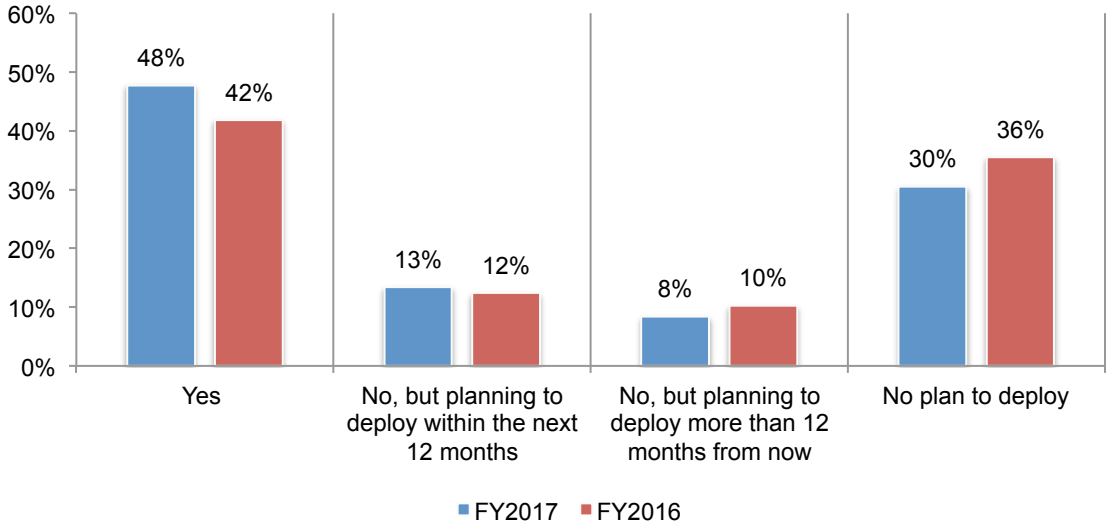
As shown in Figure 10, the biggest challenges are too many false positives (45 percent of respondents) or lack of internal resources or expertise (42 percent of respondents).

Figure 10. What threat hunting challenges do you have?
More than one choice permitted



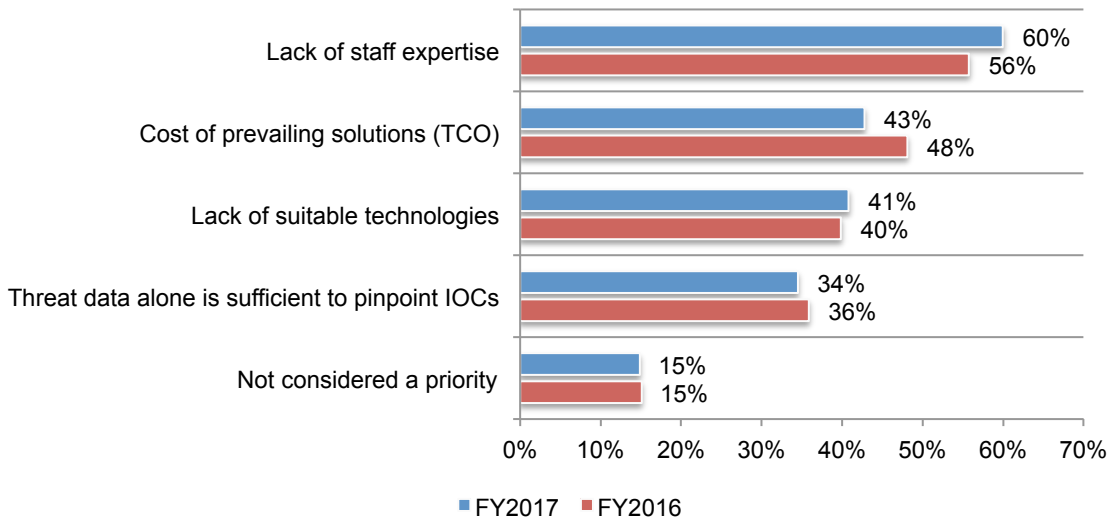
Seventy percent of respondents say their organizations deploy a threat intelligence platform or plan to. According to Figure 11, almost half (48 percent) of respondents say their organizations deploy a threat intelligence platform. Another 13 percent say their organizations plan to deploy one in the next 12 months, while 8 percent say their organizations will deploy one more than 12 months from now.

Figure 11. Does your organization deploy a threat intelligence platform?



As shown in the figure above, 30 percent of respondents say their organizations have no plans to deploy a threat platform, a decrease from 36 percent in 2016. The primary reason for not deploying continues to be the lack of staff expertise (60 percent of respondents). Another deterrent, per 43 percent of respondents, is the cost of prevailing solutions (TCO), as shown in the figure below (Figure12).

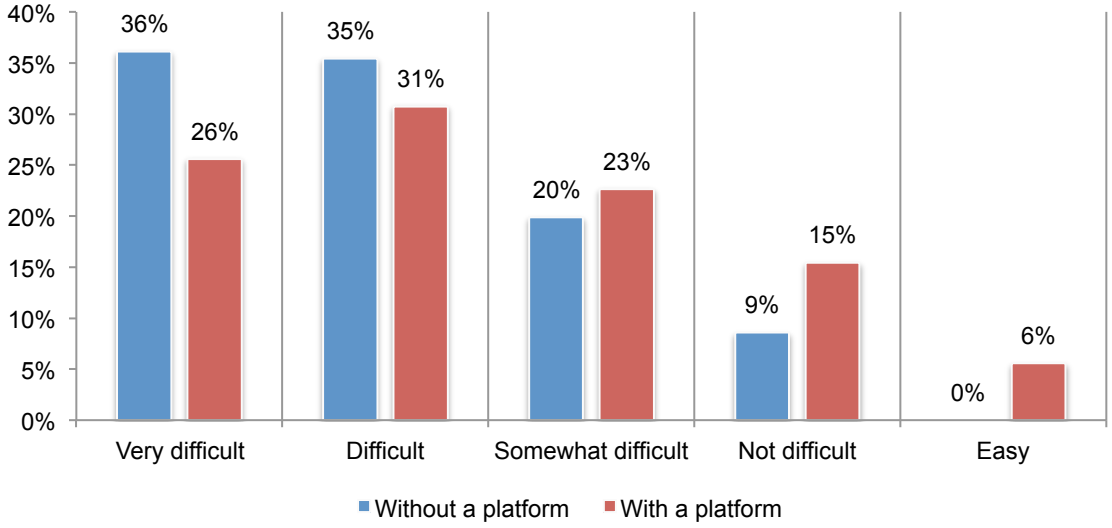
Figure 12. Why some companies do not deploy a threat intelligence platform
More than one choice permitted



It is more difficult to prioritize threat intelligence without a platform. Figure 13 reveals that 71 percent of respondents who do not deploy a platform say it is very difficult (36 percent) or difficult (35 percent) to prioritize threat intelligence data without a platform.

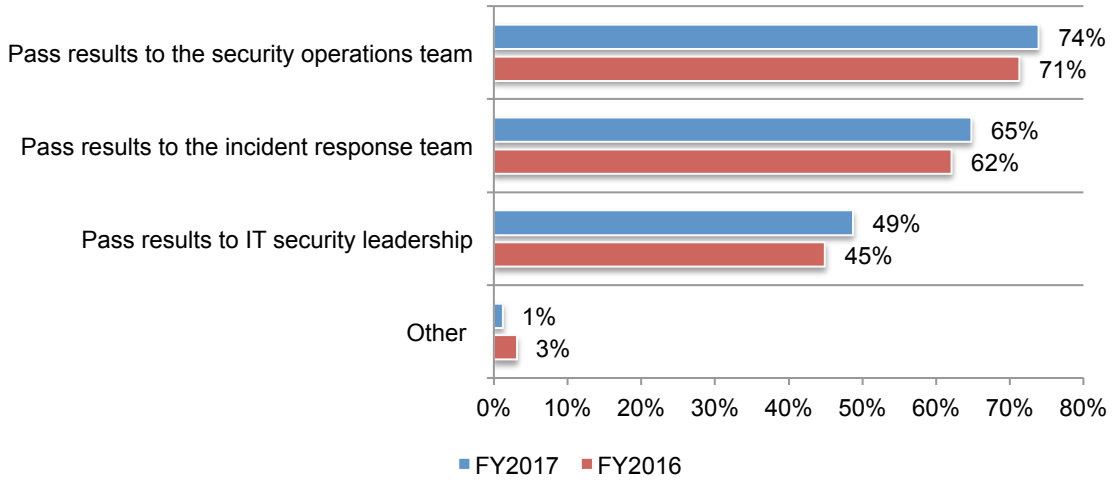
In contrast, 57 percent of respondents say the process of prioritizing threat intelligence data with a platform is very difficult (26 percent of respondents) or difficult (31 percent of respondents).

Figure 13. How difficult is the process of prioritizing threat intelligence without a platform?



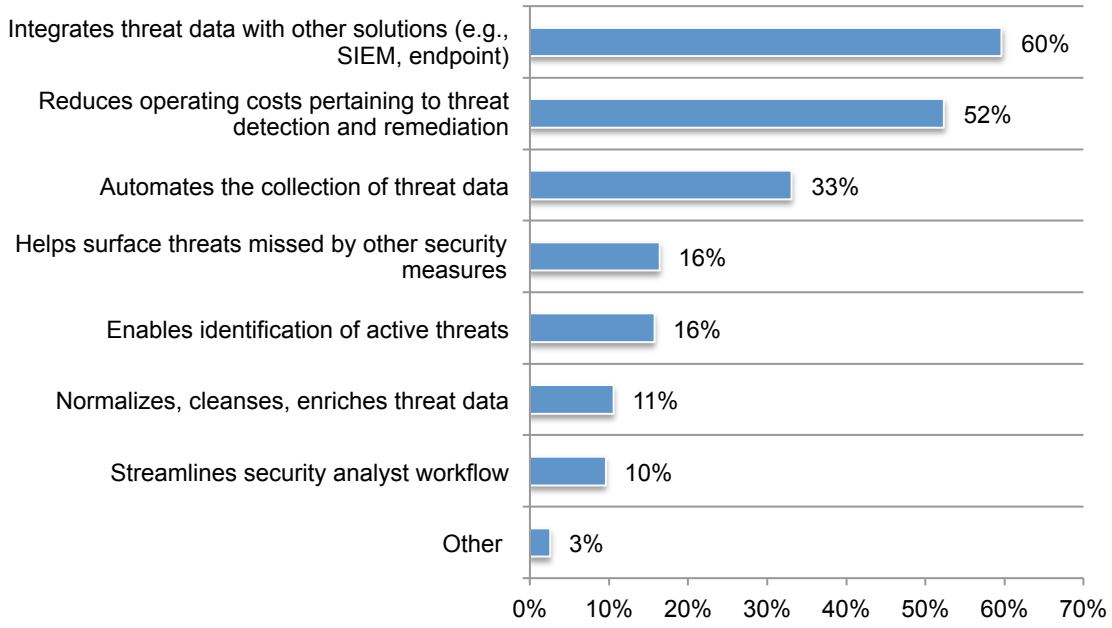
As shown in Figure 14, if there is no threat intelligence platform, threat analysts primarily pass what they learn on to the security operations team (74 percent of respondents) or the incident response team (65 percent of respondents). It is less likely (49 percent of respondents) that results are passed on to IT security leadership.

Figure 14. If there is no threat intelligence platform, what do threat analysts within your organization do with the results of their efforts?
More than one choice permitted



Threat intelligence platforms enable the integration of threat data with other solutions. As shown in Figure 15, more than half (60 percent) of respondents say it integrates threat data with other solutions such as SIEM and endpoints as well as reduces operating costs pertaining to threat detection and remediation (52 percent of respondents).

Figure 15. The main benefits of having a threat intelligence platform
More than one choice permitted

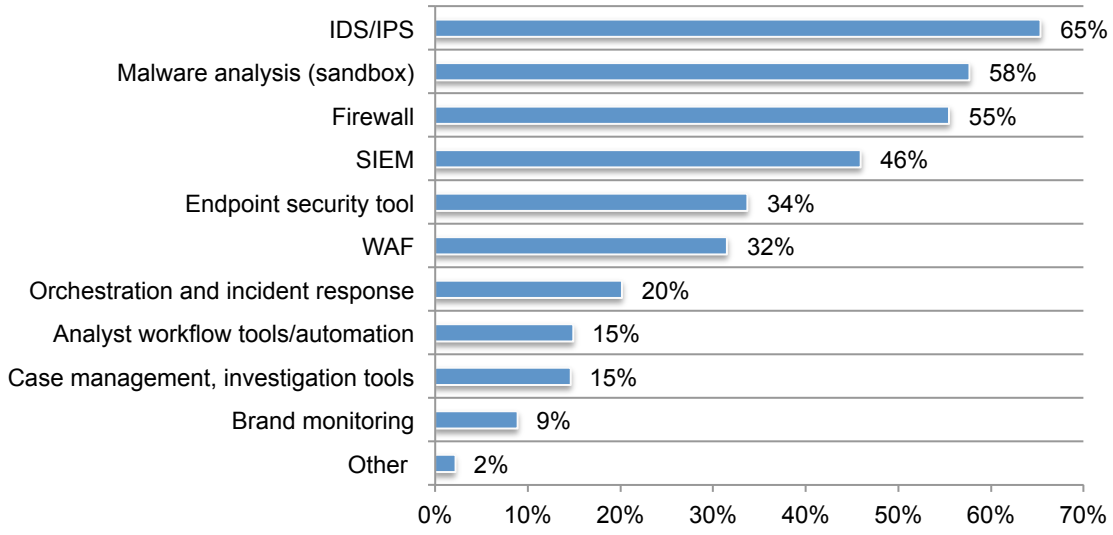


Threat intelligence integration and performance

Threat intelligence is most often integrated into IDS/IPS. As shown in Figure 16, the primary parts of an organization's security architecture into which threat intelligence is mostly integrated are: IDS/IPS (65 percent of respondents), malware analysis (sandbox) (58 percent of respondents) and firewalls (55 percent of respondents).

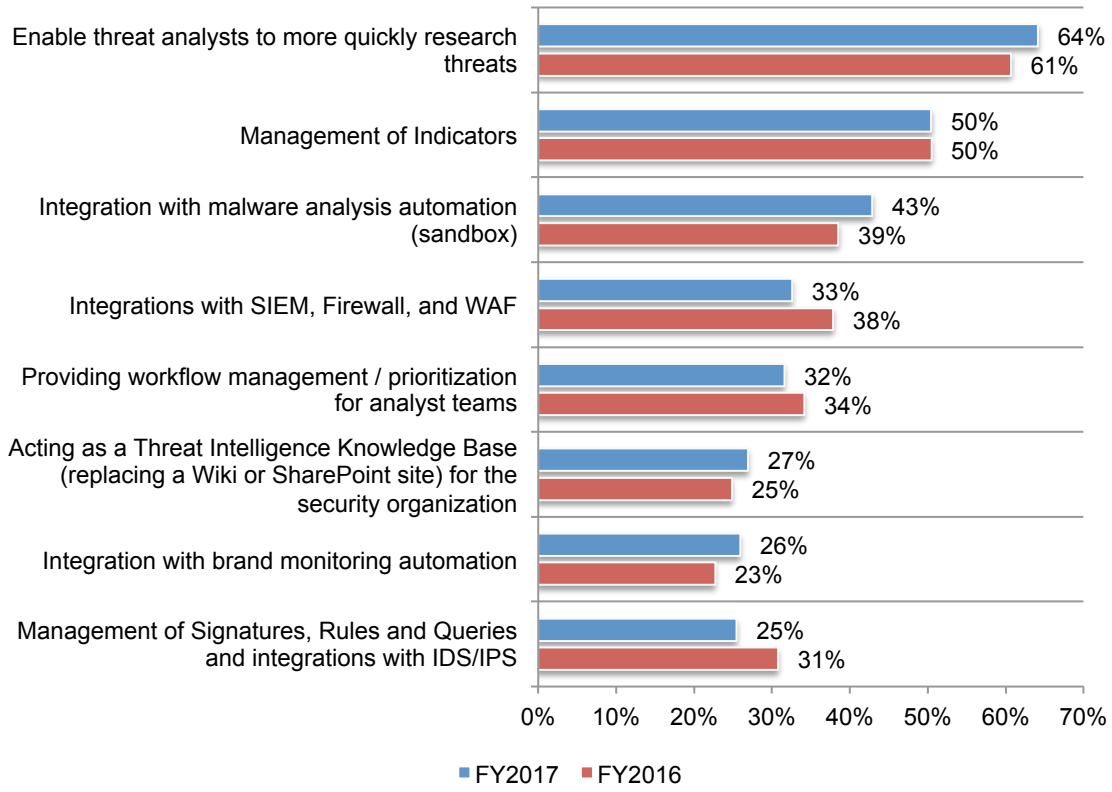
Fifty-nine percent say such integration is very difficult (27 percent of respondents) or difficult (32 percent of respondents).

Figure 16. What parts of your security architecture do you integrate threat intelligence into?
More than one choice permitted



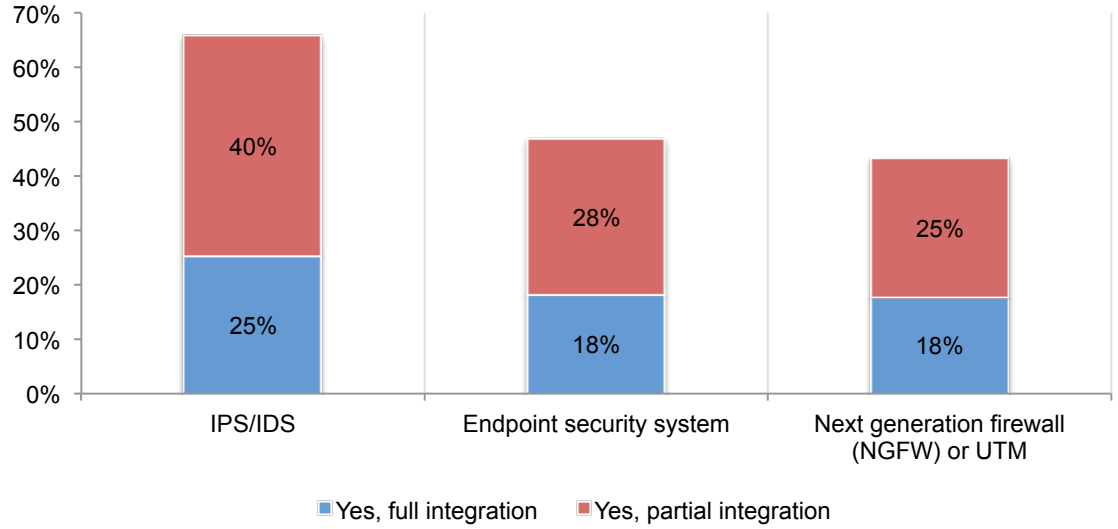
The ability to research threats more quickly is an important feature for integration. When asked what features companies would like to see as part of the integration, 64 percent of respondents say it is to enable threat analysts to more quickly research threats, as shown in Figure 17. Other important features are the management of indicators (50 percent of respondents) and integration with malware analysis automation (sandbox) (43 percent of respondents).

Figure 17. What features are important to integration?
Three choices permitted



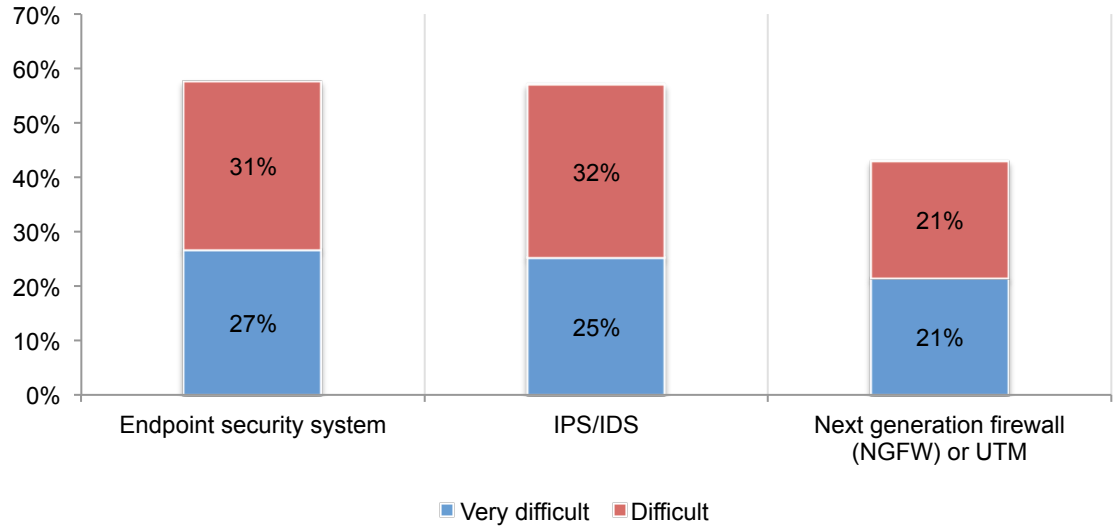
In which technologies or tools does integration of data from the platform most often occur? As shown in Figure 18, full or partial integration of threat intelligence is most likely to occur with the IPS/IDS (65 percent of respondents). Endpoint security systems (46 percent of respondents) and NGFWs or UTMs (43 percent of respondents) are the least deployed.

Figure 18. In which technologies does integration of data from the platform most often occur?
Full and *Partial integration* responses combined



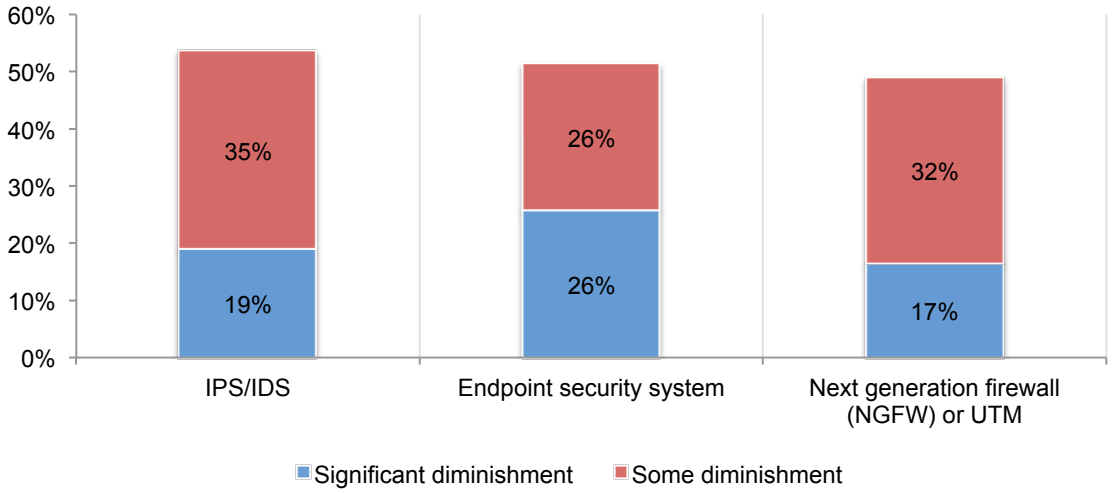
NGFWs or UTMs are least difficult to integrate. As the data in Figure 19 show**,** 58 percent of respondents say integration with endpoint security systems is very difficult (27 percent of respondents) or difficult (31 percent of respondents); 57 percent of respondents say integration involving IPS/IDS is very difficult (25 percent) or difficult (32 percent). Only 42 percent say integration is difficult.

Figure 19. Which integration was most difficult?
Very difficult and *Difficult* responses



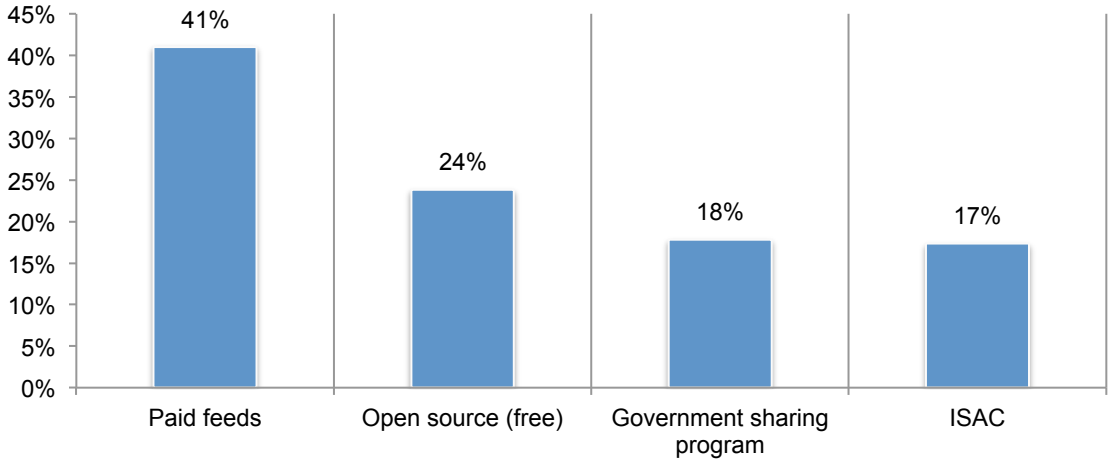
NGFW or UTMs experience the least diminishment (i.e., degradation) following integration. According to Figure 20, IPS/IDS experience the most diminishment, according to 54 percent of respondents. These respondents say integration was diminished significantly (19 percent) or somewhat diminished (35 percent). Fifty-two percent of respondents say their organizations' endpoint security system faces significant (26 percent) or some diminishment (26 percent). NGFW or UTM experience significant (17 percent) or some diminishment (32 percent).

Figure 20. Which technologies experience the most diminishment following integration?
Significant diminishment and *Some diminishment* responses combined



H**ow open source and paid fees compare in usage.** An average of almost nine threat intelligence feeds are used in the organizations represented in this study. As shown in Figure 21, companies are mostly using paid threat intelligence feeds (41 percent of respondents) or a combination of open source (free) feeds (24 percent of respondents) or a government sharing program (18 percent respondents).

Figure 21. What is the primary source of threat intelligence used by your organization?



Communication issues in disseminating threat intelligence

Threat intelligence is not often disseminated throughout the enterprise. According to Figure 22, only 38 percent of respondents say threat intelligence is used to brief or educate senior executives about cyber risks facing the company. A similar percentage (36 percent of respondents) say such communication reaches the board of directors.

Figure 22. How threat intelligence is used to educate senior executives and the board of directors

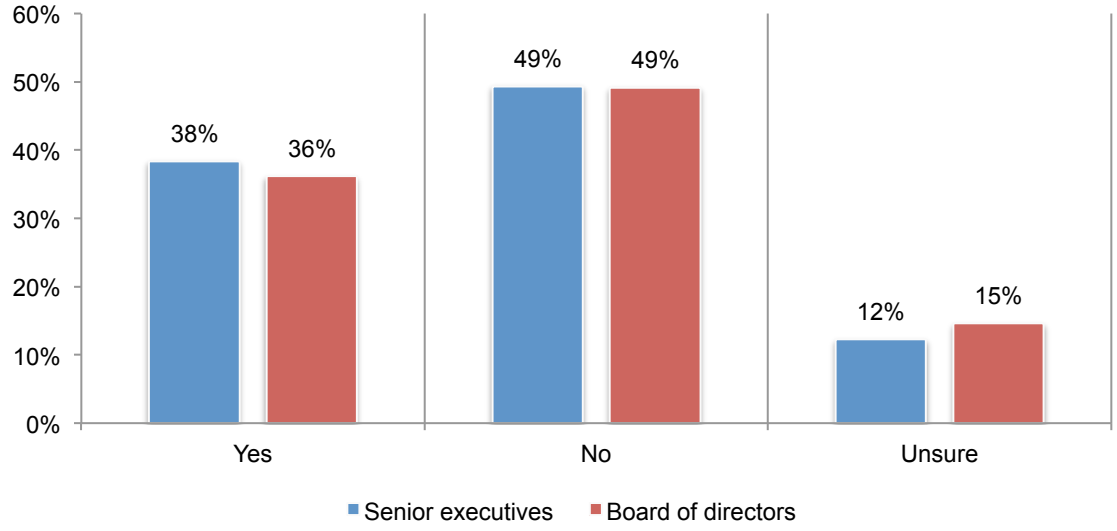
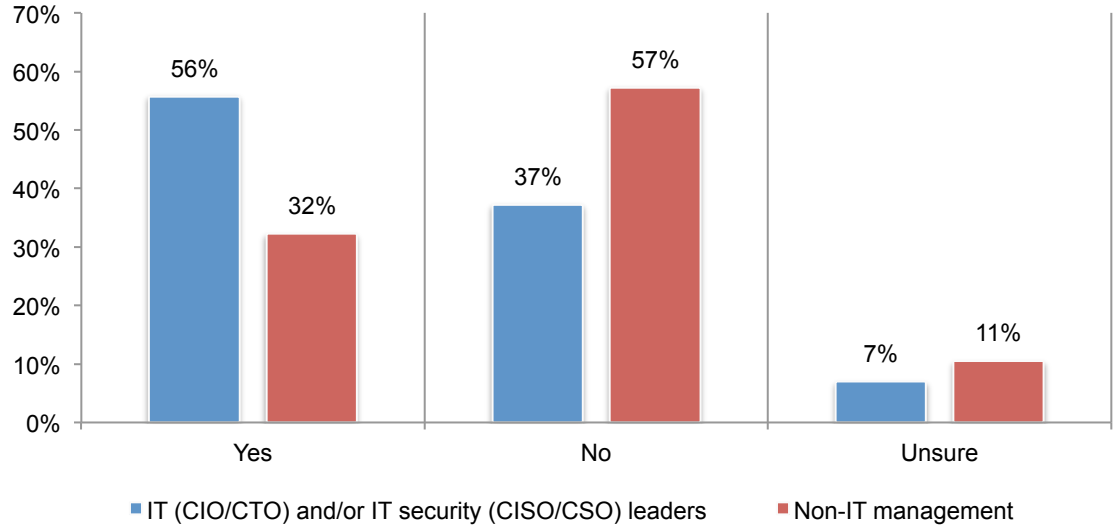


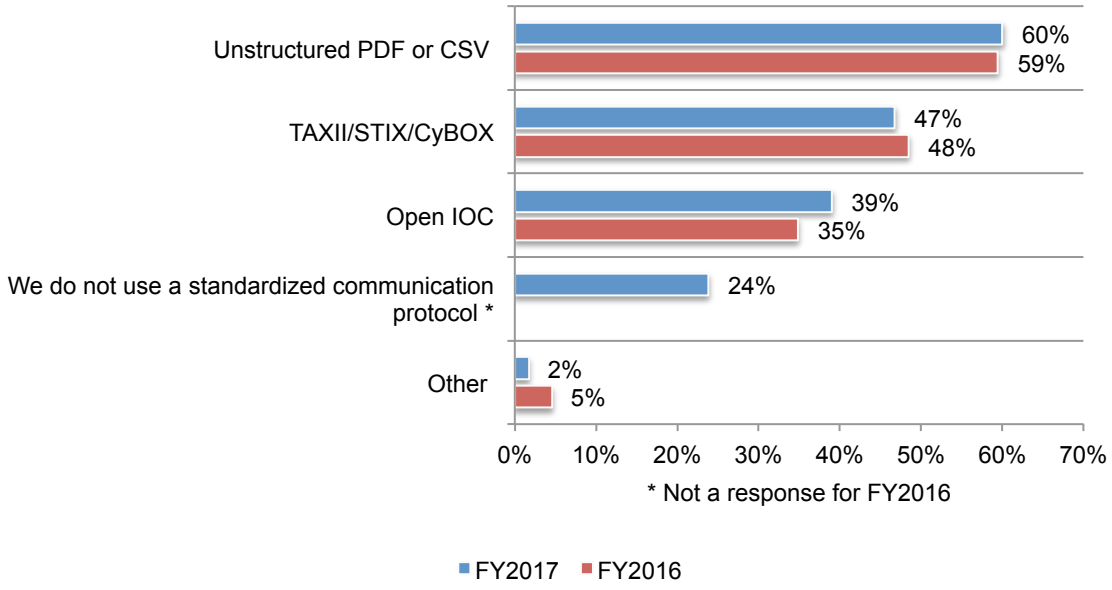
Figure 23 reveals that 56 percent of respondents say that individuals in the IT and IT security function receive and read threat intelligence reports. However, only 32 percent of respondents say such reports are circulated among their companies' non-IT management. Such reports are typically issued and disseminated at no regular interval or on demand, according to 27 percent of respondents. Forty-one percent of respondents say such communication provides intelligence reports monthly or quarterly.

Figure 23. Who reads and receives threat intelligence reports?



The sharing and disseminating of threat intelligence does not frequently take place through standardized communication protocols. As Figure 24 illustrates, 60 percent of respondents say their companies use unstructured PDFs or CSVs, while 47 percent of respondents say their organizations use TAXII/STIX/CyBox.

Figure 24. What communication protocols are used?
More than one choice permitted



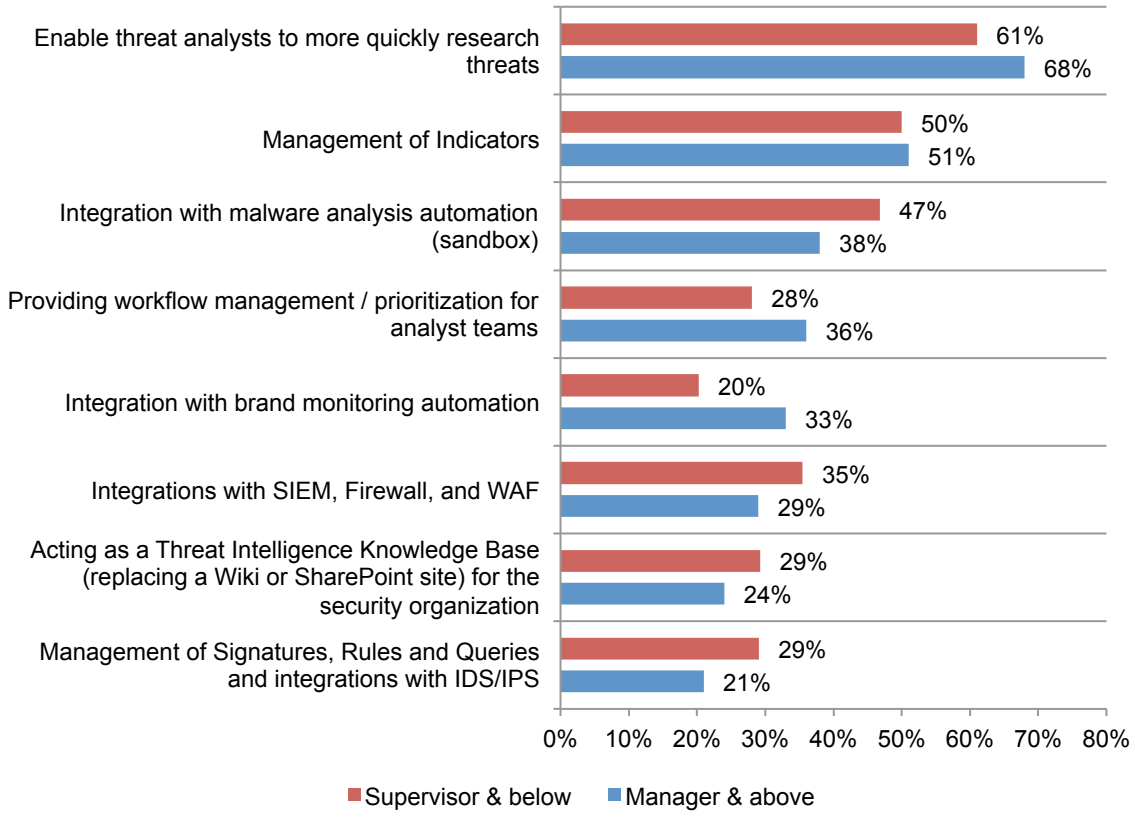
Differences based on position level and headcount

In this section, we provide an analysis of differences in perception between respondents who hold positions at or above the managerial level (43 percent of respondents) and those who are at or below the supervisory level (57 percent of respondents). The following are the most interesting differences.

Ability to more quickly research threats is critical. As shown in Figure 20, both groups of respondents consider enabling threat analysts to research threats more quickly the most important feature with regard to the integration of threat intelligence into an organization's security architecture.

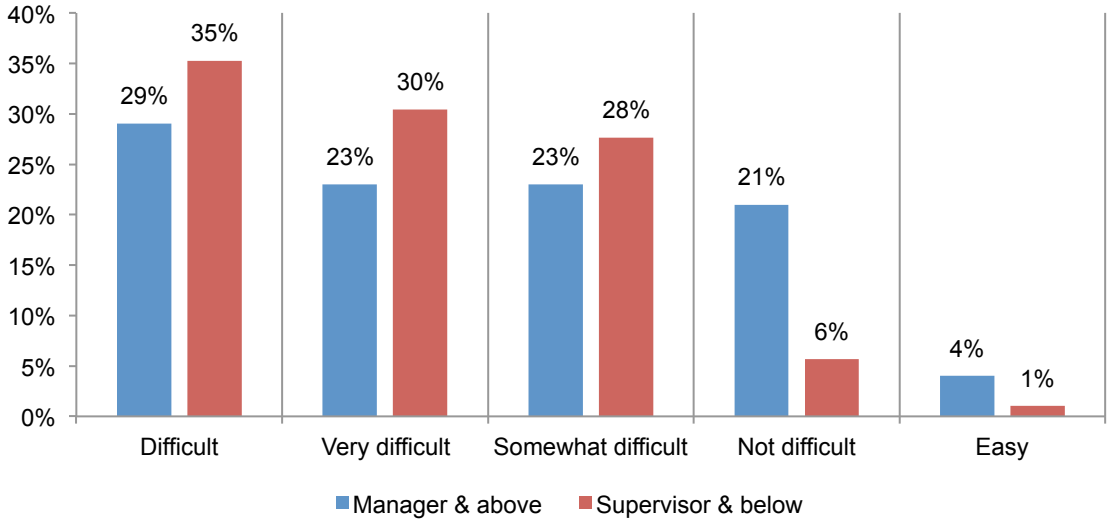
However, for the same issue, respondents who are at the supervisory level or below are more likely to mention integration with malware analysis automation (sandbox), integrations with SIEM, Firewall and WAF and management of Signatures, Rules and Queries and integrations with IDS/IPS (47 percent vs. 38 percent; 35 percent vs. 29 percent and 29 percent vs. 21 percent, respectively). Those in managerial positions consider providing workflow management/prioritization for analyst teams and integration with brand monitoring automation (36 percent vs. 28 percent and 33 percent vs. 20 percent).

Figure 20. Features you would like to see as part of threat integration into security architecture that you don't already have
Three choices permitted



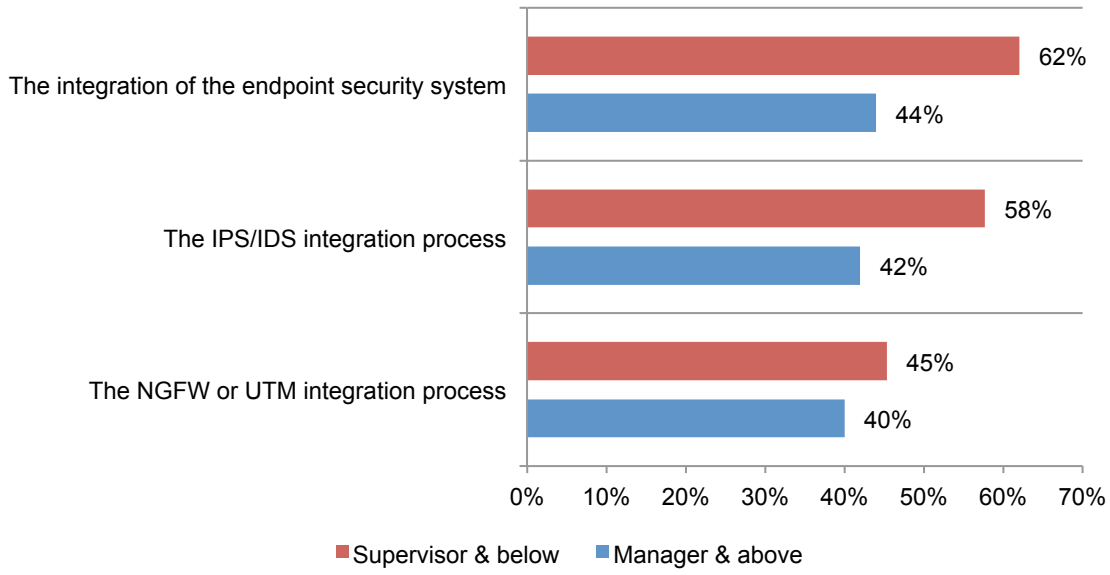
Perceptions of the SIEM integration process differ. As shown in Figure 21, those in the trenches (supervisor and below) say that the SIEM integration process is very difficult or difficult (65 percent of supervisors and below vs. 52 percent of managers and above).

Figure 21. How difficult was the SIEM integration process?



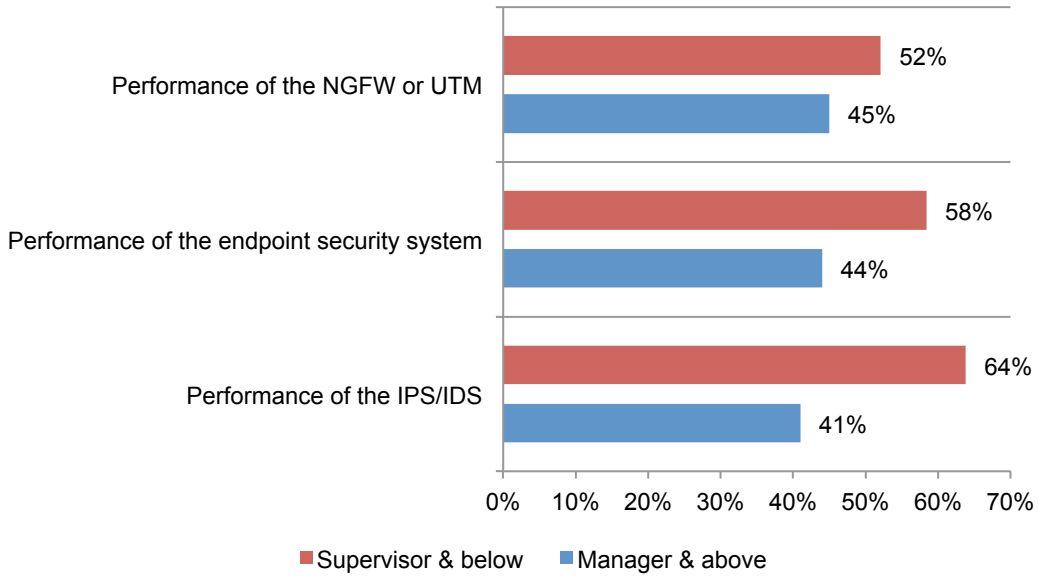
In all cases of integration, respondents who are supervisors and below are most likely to consider the integration of the endpoint security process, the IPS/IDS integration process and the NGFW or UTM integration process difficult.

Figure 22. Difficulty in threat intelligence integration into security architecture
Very difficult and *Difficult* responses combined



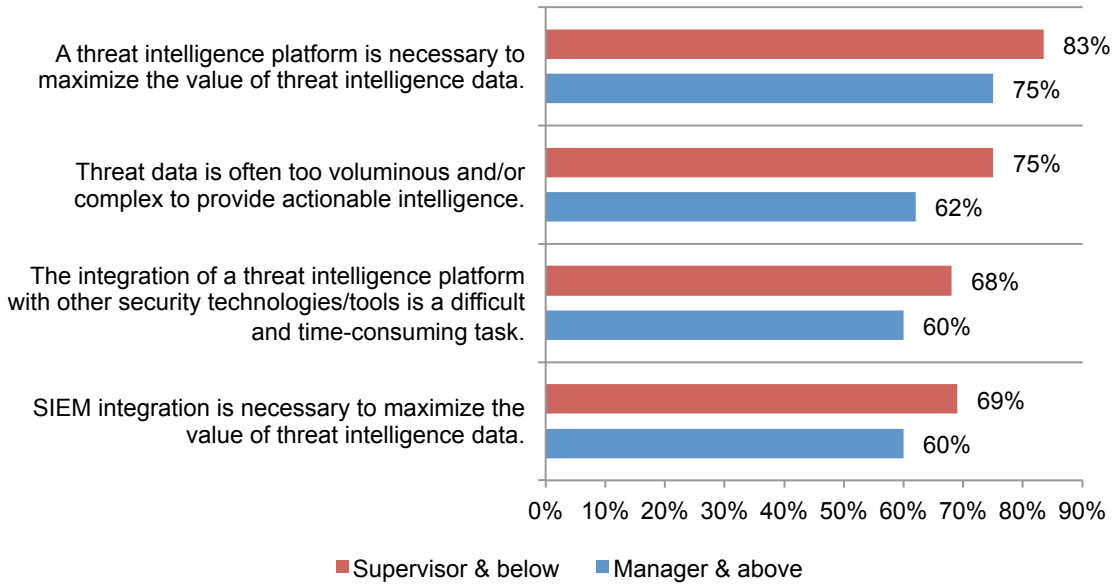
There are also some significant differences in perceptions regarding the diminishment in performance. In every case, respondents who are supervisors and below are more likely to believe there is diminishment in performance due to threat intelligence integration into security architecture. Specifically, 64 percent of supervisors and below believe that the performance of the IPS/IDS is diminished due to threat intelligence integration, whereas only 41 percent of respondents who hold positions at the manager level and above do.

Figure 23. How threat intelligence integration into security architecture affects performance
Significant diminishment and *Some diminishment* responses combined



Respondents at the supervisory level and below are more likely to believe that a threat intelligence platform is necessary for maximizing the value of threat intelligence data (83 percent vs. 75 percent of manager and above respondents) and are less likely to agree that the integration of a threat intelligence platform with other security technologies or tools is a difficult and a time-consuming task (68 percent vs. 60 percent). Senior-level respondents are less likely to believe threat data is often too voluminous and/or complex to provide actionable intelligence (62 percent vs. 75 percent of respondents).

Figure 24. Perceptions about the value of threat intelligence
Strongly agree and *Agree* responses combined

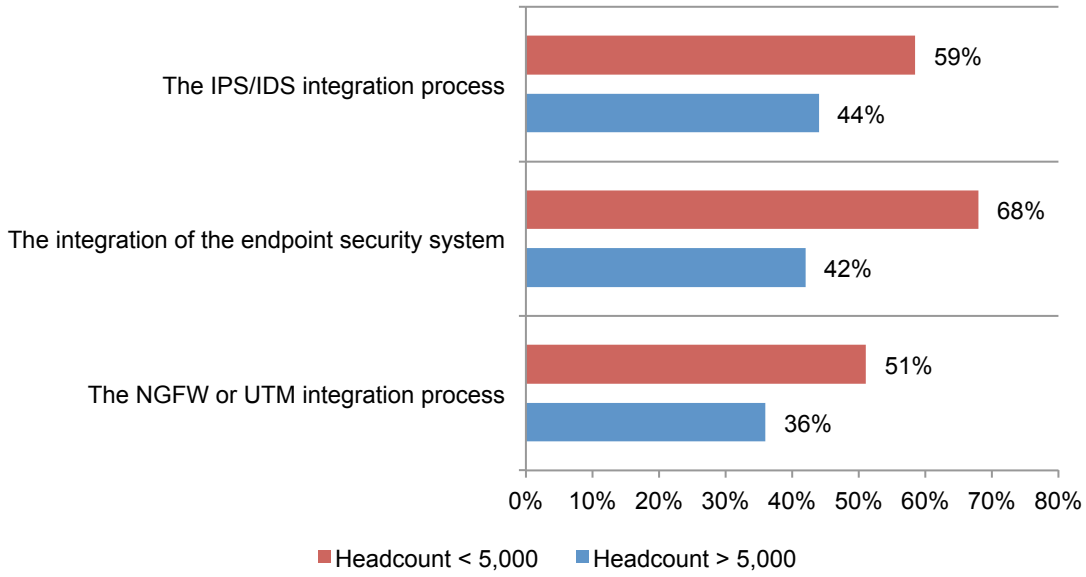


Differences based on the size of the organization

In this section, we analyze the differences between companies with a headcount above 5,000 (54 percent of respondents) and below 5,000 (46 percent of respondents). The following are the key differences.

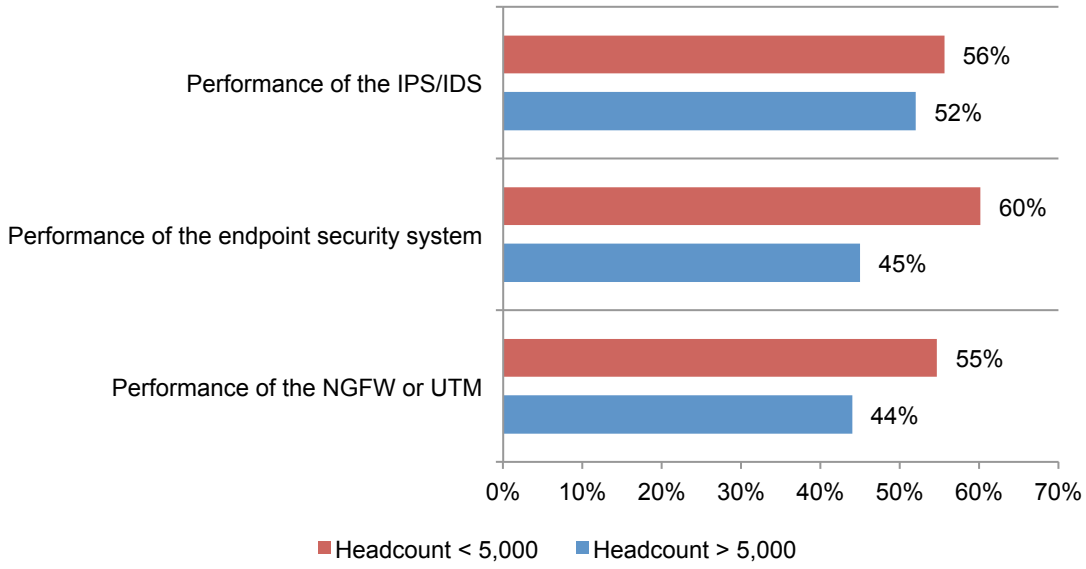
Organizations with a headcount under 5,000 find the integration of threat intelligence more difficult than organizations with a headcount over 5,000. The integration process of the endpoint security system, IPS/IDS integration process and DLP integration process (68 percent, 59 percent and 51 percent of respondents, respectively) are the most difficult for smaller organizations.

Figure 25. Difficulty in threat intelligence integration into security architecture
Very difficult and *Difficult* responses combined



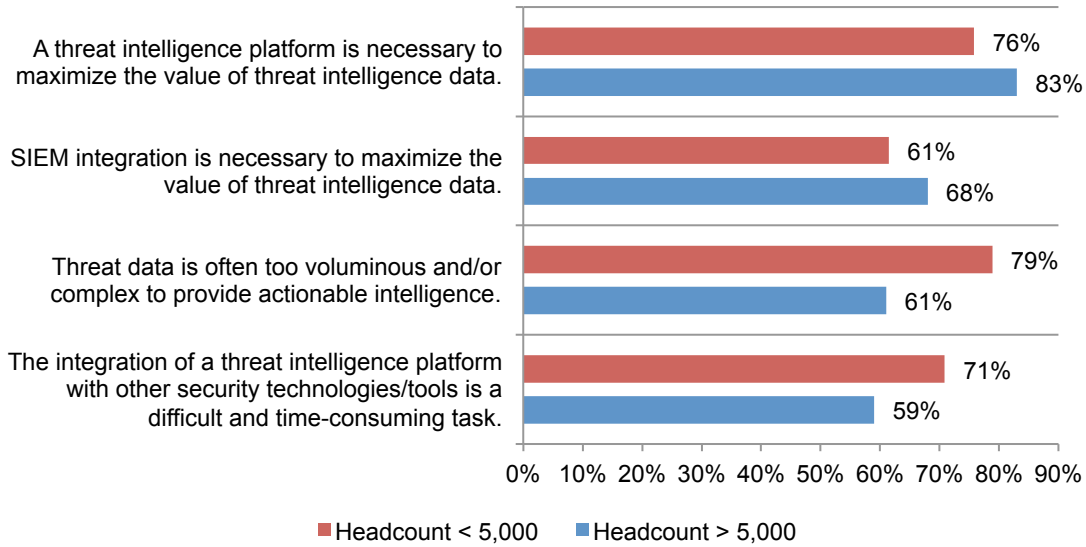
Smaller organizations are also more likely to experience performance diminishment with the integration of threat intelligence into their security architecture. This is especially the case with the endpoint security system (60 percent of smaller organizations compared to 45 percent of larger ones).

Figure 26. How threat intelligence integration into security architecture affects performance
Significant diminishment and *Some diminishment* responses combined



Both larger and smaller organizations believe a threat intelligence platform is necessary for maximizing the value of threat intelligence data (83 percent and 76 percent of respondents, respectively). Smaller organizations, though, are more likely to believe that threat data is often too voluminous and/or complex to provide actionable intelligence.

Figure 27. Perceptions of the value of threat intelligence
Strongly agree and *Agree* responses combined



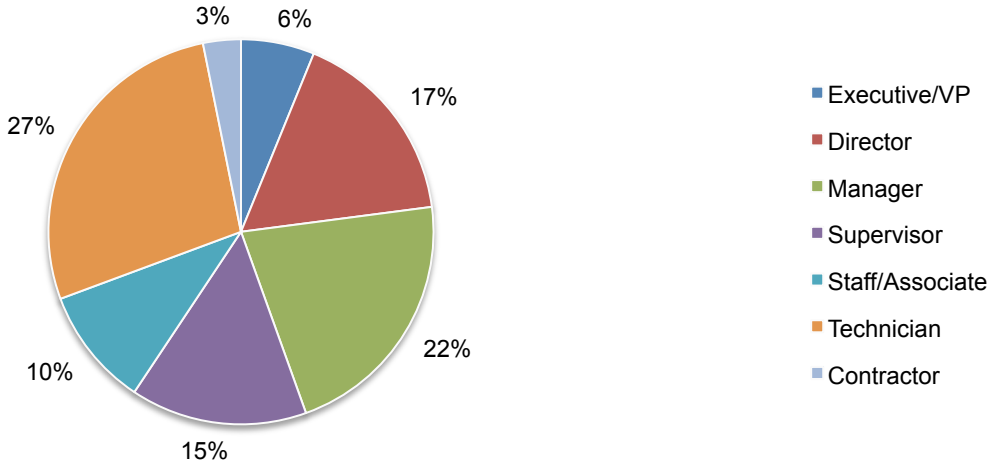
Part 3. Methods

A sampling frame of 30,570 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 1,201 total returned surveys. Screening and reliability checks led to the removal of 130 surveys. Our final sample consisted of 1,071 surveys, a 3.5 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	30,570	100.0%
Total returns	1,201	3.9%
Rejected or screened surveys	130	0.4%
Final sample	1,071	3.5%

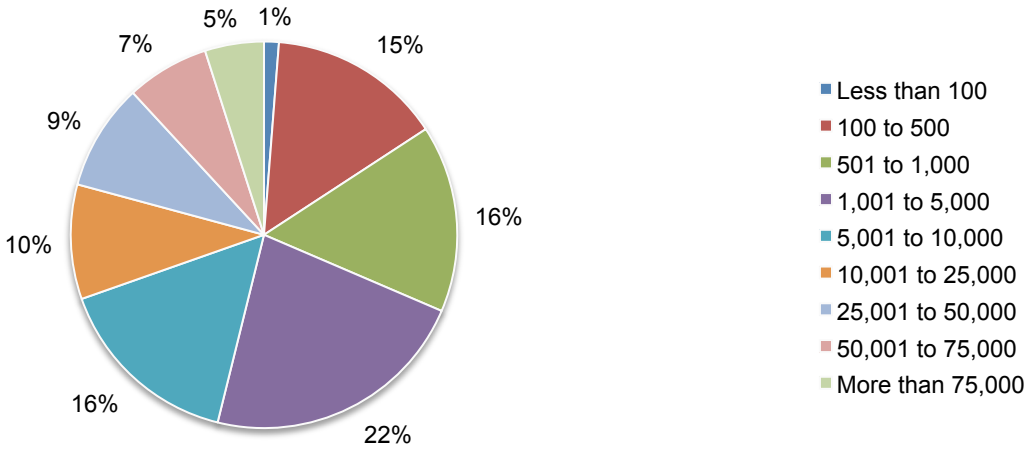
Pie Chart 1 reports the respondents' organizational level within participating organizations. By design, more than half of respondents (60 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



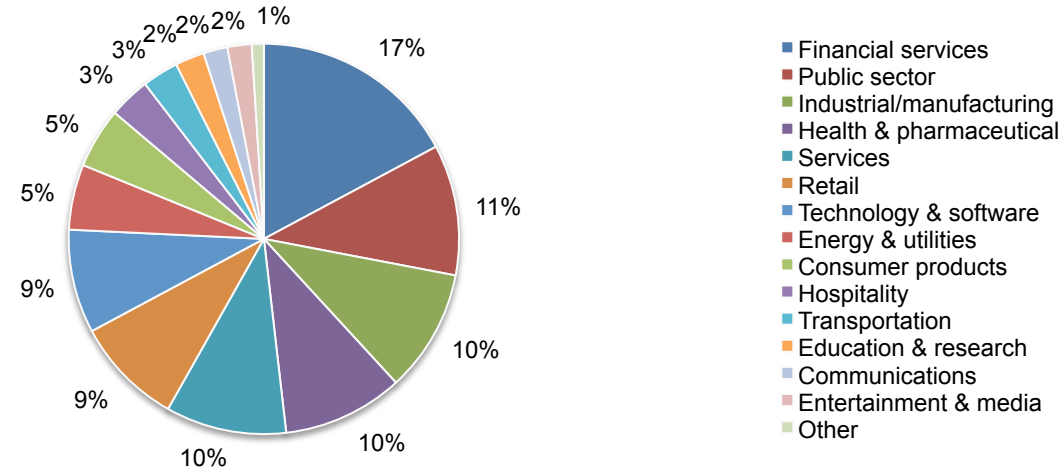
As Pie Chart 2 illustrates, 69 percent of the respondents are from organizations with a global headcount exceeding 1,000 employees.

Pie Chart 2. Global employee headcount of the organization



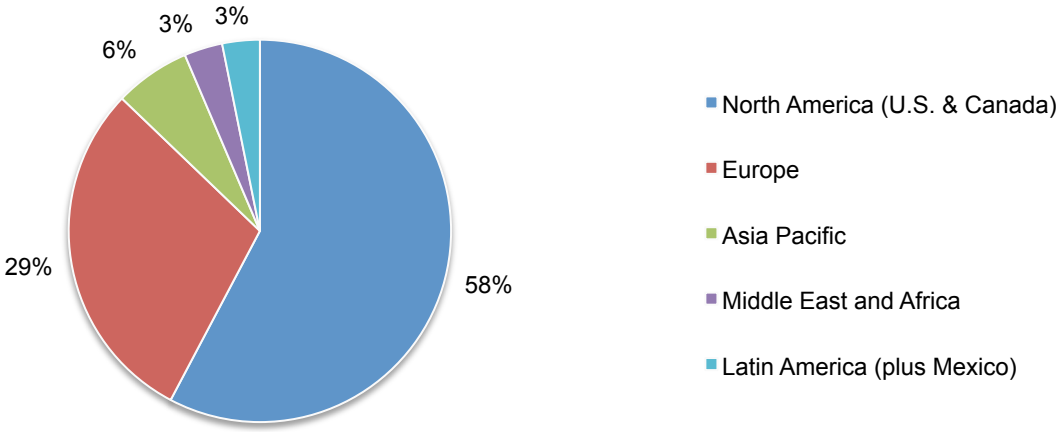
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by public sector (11 percent of respondents) and industrial/manufacturing (10 percent of respondents).

Pie Chart 3. Primary industry segment



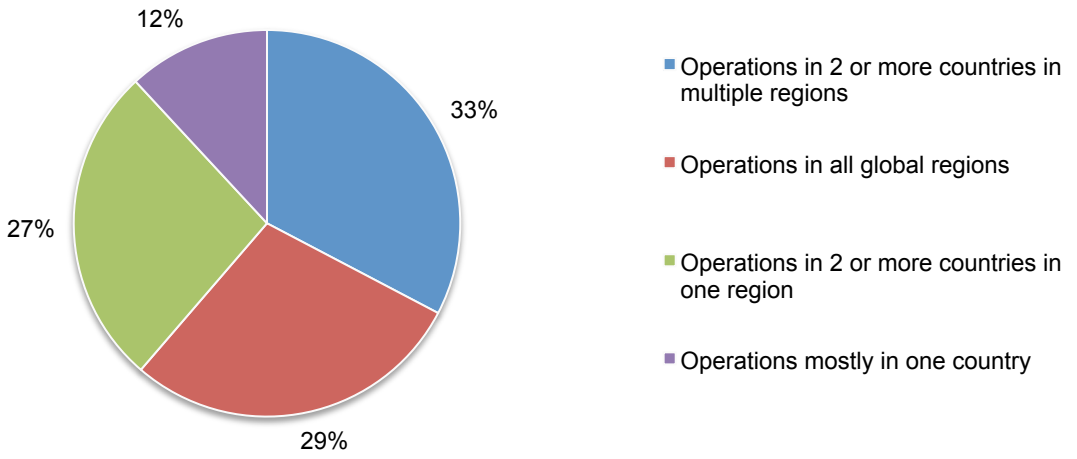
As shown in Pie Chart 4, more than half (58 percent) of the respondents' organizations are headquartered in North America and 29 percent are headquartered in Europe.

Pie Chart 4. Headquarter location of the organization



Pie Chart 5 reports the global footprint of respondents' organization. Thirty-three percent of the respondents have operations in 2 or more countries in multiple regions, 29 percent have operations in all global regions and 27 percent have operations in 2 or more countries in one region.

Pie Chart 5. 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.