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

Sponsored by Anomali

Independently conducted by Ponemon Institute LLC

Publication Date: July 2016
Part 1. Introduction

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

Companies highly value threat intelligence. As shown in Figure 1, 77 percent of respondents say threat intelligence is very valuable to their organization’s overall security mission. A similar percentage of respondents (78 percent) rate the importance of threat intelligence in achieving a strong cybersecurity posture as very high.

**Who benefits from threat intelligence?** The primary users of threat intelligence are security leaders (81 percent of respondents), incident response teams (79 percent of respondents), IT leaders (59 percent of respondents) and IT operations (57 percent of respondents). Secondary users are mainly compliance (51 percent of respondents), security operations (41 percent of respondents) and IT operations (40 percent of respondents). Fifty-seven percent of respondents say threat intelligence drives decision-making within their organizations’ security operations center (SOC).

**Threat intelligence is too voluminous and complex.** Seventy percent of respondents say threat intelligence is often too voluminous and/or complex to provide actionable intelligence. As a consequence, 52 percent of respondents believe their companies need a qualified threat analyst to maximize the value of threat intelligence. Such complexity may be preventing the use of threat data. Less than half (46 percent) of respondents say incident responders use threat data when deciding how to respond to threats.

**Very few companies are effective in using threat data.** Only 27 percent of respondents believe their organizations are very effective in utilizing threat data to pinpoint cyber threats. Reasons for ineffectiveness are: lack of staff expertise (69 percent of respondents), lack of ownership (58 percent of respondents) and lack of suitable technologies (52 percent of respondents).

**Most companies have a threat intelligence platform or plan to have one in the future.** Forty-two percent of respondents say their organizations plan to deploy a threat intelligence platform. Another 12 percent say they plan to deploy in the next 12 months and 10 percent say they will deploy more than 12 months from now. Forty-five percent of respondents say the threat intelligence platform is deployed consistently across the organization.

**Lack of in-house expertise prevents companies from using a threat intelligence platform.** Thirty-six percent of respondents say their organizations have no plans to deploy a threat platform. The primary reasons for not deploying are a lack of staff expertise (56 percent of respondents) and the cost of prevailing solutions (such as TCO) (48 percent of respondents).
It is more difficult to prioritize threat intelligence without a platform. Seventy percent of these respondents say it is very difficult (35 percent) or difficult (35 percent) to prioritize threat intelligence data without a platform. In contrast, 53 percent of respondents say the process of prioritizing threat intelligence data with a platform is very difficult (24 percent of respondents) or difficult (29 percent of respondents).

If they have no threat intelligence platform, threat analysts primarily pass on what they learn to the security operations team (71 percent of respondents) or pass results to the incident response team (62 percent of respondents). It is less likely results are given to IT security leadership, according to 45 percent of respondents.

Threat intelligence platforms pinpoint IOCs. Seventy-nine percent of respondents believe a threat intelligence platform is considered necessary to maximize the value of threat intelligence data. Seventy percent of respondents who use the platform say it helps pinpoint and prioritize incidents of compromise (IOCs), 59 percent of respondents say it integrates threat data with other enabling security solutions (such as SIEM) and 51 percent of respondents say it improves the threat analytics process.

Integrating threat intelligence platforms with security technologies and tools can be challenging. Sixty-four percent of respondents believe the integration of a threat intelligence platform with other security technologies or tools is a difficult and time-consuming task. A similar percentage (62 percent of respondents) says SIEM integration is necessary to maximize the value of threat intelligence data.

The primary parts of organizations’ security architecture threat intelligence is mostly integrated into are: SIEM (52 percent of respondents), IDS/IPS (49 percent of respondents) and firewalls (46 percent of respondents). Fifty-nine percent say such integration was very difficult (27 percent of respondents) or difficult (32 percent of respondents).

The ability to more quickly research threats is an important feature for integration. When asked what features companies would like to see as part of the integration, 61 percent of respondents say it is to enable threat analysts to more quickly research threats. Other important features are management of indicators (50 percent of respondents) and integration with malware analysis automation (sandbox) (39 percent of respondents).

In which technologies or tools does integration of data from the platform most often occur? Full or partial integration of threat intelligence is most likely to occur with the IPS/IDS (56 percent of respondents) and endpoint solutions (44 percent of respondents). Least likely to be fully or partially integrated are next generation firewalls or UTMs (37 percent of respondents) or DLP solutions (37 percent of respondents).

Which integration was the most difficult? Sixty-six percent of respondents say integration with endpoint solutions was very difficult (31 percent of respondents) or difficult (35 percent of respondents). The majority of respondents say integration involving IPS/IDS, WAF and DLP solutions was very difficult or difficult according to 56 percent, 56 percent and 55 percent, respectively.

Which technologies experience the most diminishment following integration? Endpoint security solutions experience the most diminishment, according to 62 percent of respondents who say integration was diminished significantly (29 percent) or somewhat diminished (34 percent). Fifty-seven percent of respondents say their organizations’ IPS/IDS solution was significantly diminished (21 percent) or somewhat diminished (36 percent).

Forty-eight percent of respondents say their DLP solutions were significantly diminished (19 percent) or diminished somewhat (29 percent). To a lesser extent, integration into the WAF
affected performance significantly (20 percent of respondents) or somewhat (27 percent of respondents). With respect to next generation firewall or UTM, there was significant diminishment (17 percent) or some diminishment (28 percent).

**How open source and paid feeds compare in usage.** An average of almost 10 threat intelligence feeds are used in the organizations represented in this study. Companies are mostly using paid threat intelligence feeds (39 percent of respondents), open source (free) (28 percent of respondents) or a combination of feeds (33 percent of respondents). Forty-six percent of respondents believe paid feeds provide more actionable intelligence than free sources of threat data.

**Threat intelligence is not often disseminated throughout the enterprise.** Only 32 percent of respondents say threat intelligence is used to brief or educate senior executives about cyber risks facing the company and a similar percentage (30 percent of respondents) say such communication reaches the board of directors. Thirty-six percent of respondents say such communication provides intelligence reports monthly or quarterly.

**The sharing and disseminating of threat intelligence often does not use standardized communication protocols.** Fifty-six percent of respondents say their companies do not use standardized communication protocols. If they do, it is most likely unstructured PDFs or CSVs (59 percent of respondents) or TAXII/STIX/CyBox (48 percent of respondents).
Part 2. Key findings

In this section of the report, we provide the detailed findings of the research. The complete audited 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 platforms
- Integration & performance
- Communication issues in disseminating threat intelligence
- Special analysis: Differences 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 (81 percent of respondents), incident response teams (79 percent of respondents), IT leaders (59 percent of respondents) and IT operations (57 percent of respondents). Secondary users are mainly compliance (51 percent of respondents), security operations (41 percent of respondents) and IT operations (40 percent of respondents). Fifty-seven percent of respondents say threat intelligence drives decision-making within their organizations’ security operations center (SOC).

Figure 2. Who are the primary and secondary users of threat intelligence?

More than one choice permitted

<table>
<thead>
<tr>
<th>Position</th>
<th>Primary users</th>
<th>Secondary users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security leaders (CISO, CSO)</td>
<td>19%</td>
<td>81%</td>
</tr>
<tr>
<td>Incident response team</td>
<td>23%</td>
<td>79%</td>
</tr>
<tr>
<td>IT leaders (CIO, CTO)</td>
<td>39%</td>
<td>59%</td>
</tr>
<tr>
<td>IT operations</td>
<td>32%</td>
<td>44%</td>
</tr>
<tr>
<td>Enterprise risk management</td>
<td>32%</td>
<td>44%</td>
</tr>
<tr>
<td>Security operations</td>
<td>26%</td>
<td>41%</td>
</tr>
<tr>
<td>Compliance</td>
<td>20%</td>
<td>51%</td>
</tr>
<tr>
<td>Internal audit</td>
<td>8%</td>
<td>27%</td>
</tr>
<tr>
<td>Business continuity management</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>Non-IT management</td>
<td>5%</td>
<td>10%</td>
</tr>
<tr>
<td>Procurement</td>
<td>4%</td>
<td>8%</td>
</tr>
<tr>
<td>Application development</td>
<td>4%</td>
<td>20%</td>
</tr>
<tr>
<td>Human resources</td>
<td>4%</td>
<td>20%</td>
</tr>
<tr>
<td>Executive management (CEO, COO)</td>
<td>3%</td>
<td>17%</td>
</tr>
<tr>
<td>Board of directors</td>
<td>0%</td>
<td>9%</td>
</tr>
</tbody>
</table>
Threat intelligence is too voluminous and complex. According to Figure 3, 70 percent of respondents say threat intelligence is often too voluminous and/or complex to provide actionable intelligence. As a consequence, 52 percent of respondents believe their companies need a qualified threat analyst to maximize the value of threat intelligence.

Such complexity may be preventing the use of threat data. Less than half (46 percent) of respondents say incident responders use threat data when deciding how to respond to threats.

Figure 3. Barriers to the effective use of threat intelligence
Strongly agree and Agree responses combined

<table>
<thead>
<tr>
<th>Barriers</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat data is often too voluminous and/or complex to provide actionable intelligence</td>
<td>70%</td>
</tr>
<tr>
<td>A qualified threat analyst is essential to maximize the value of threat intelligence data</td>
<td>52%</td>
</tr>
<tr>
<td>In my organization, incident responders utilize threat data when deciding how to respond to threats</td>
<td>46%</td>
</tr>
</tbody>
</table>

Very few companies are effective in using threat data. Only 27 percent of respondents believe their organizations are very effective in utilizing threat data to pinpoint cyber threats. Figure 4 presents the reasons for being ineffective. These are lack of staff expertise (69 percent of respondents), lack of ownership (58 percent of respondents) and lack of suitable technologies (52 percent of respondents).

Figure 4. Why companies believe they are ineffective?
More than one choice permitted

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of staff expertise</td>
<td>69%</td>
</tr>
<tr>
<td>Lack of ownership</td>
<td>58%</td>
</tr>
<tr>
<td>Lack of suitable technologies</td>
<td>52%</td>
</tr>
<tr>
<td>Threat data is not reliable or sufficient to pinpoint IOCs</td>
<td>46%</td>
</tr>
<tr>
<td>Not considered a priority</td>
<td>24%</td>
</tr>
<tr>
<td>Interoperability issues</td>
<td>17%</td>
</tr>
</tbody>
</table>
Threat intelligence platforms

Most companies have a threat intelligence platform or plan to have one in the future. According to Figure 5, 42 percent of respondents say their organizations deploy a threat intelligence platform. Another 12 percent say they plan to deploy in the next 12 months and 10 percent say they will deploy more than 12 months from now. Forty-five percent of respondents say the threat intelligence platform is deployed consistently across the organization.

Figure 5. Does your organization deploy a threat intelligence platform?

Thirty-six percent of respondents say their organizations have no plans to deploy a threat platform. The primary reasons for not deploying are a lack of staff expertise (56 percent of respondents) and cost of prevailing solutions (TCO) (48 percent of respondents).

Figure 6. Why some companies do not deploy a threat intelligence platform
More than one choice permitted

- Lack of staff expertise: 56%
- Cost of prevailing solutions (TCO): 48%
- Lack of suitable technologies: 40%
- Threat data alone is sufficient to pinpoint IOCs: 36%
- Not considered a priority: 15%
It is more difficult to prioritize threat intelligence without a platform. As shown in Figure 7, 70 percent of these respondents say it is very difficult (35 percent) or difficult (35 percent) to prioritize threat intelligence data without a platform. In contrast, 53 percent of respondents say the process of prioritizing threat intelligence data with a platform is very difficult (24 percent of respondents) or difficult (29 percent of respondents).

**Figure 7. How difficult is the process of prioritizing threat intelligence?**

As discussed, a lack of in-house expertise prevents companies from having a threat intelligence platform. As shown in Figure 8, if there is no threat intelligence platform, threat analysts primarily pass on what they learn to the security operations team (71 percent of respondents) or pass results to the incident response team (62 percent of respondents). It is less likely (45 percent of respondents) results are given to IT security leadership.

**Figure 8. What do threat analysts within your organization do with the results of their efforts?**

More than one choice permitted

- Pass results to the security operations team: 71%
- Pass results to the incident response team: 62%
- Pass results to IT security leadership: 45%
- Other: 3%
Threat intelligence platforms pinpoint IOCs. Seventy-nine percent of respondents believe a threat intelligence platform is considered necessary to maximize the value of threat intelligence data. As shown in Figure 9, 70 percent of respondents who use the platform say it helps pinpoint and prioritize incidents of compromise (IOCs), 59 percent of respondents say it integrates threat data with other enabling security solutions (such as SIEM) and 51 percent of respondents say it improves the threat analytics process.

Figure 9. The main benefits of having a threat intelligence platform
More than one choice permitted

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helps pinpoint and prioritize IOCs</td>
<td>70%</td>
</tr>
<tr>
<td>Integrates threat data with other enabling security solutions (such as SIEM)</td>
<td>59%</td>
</tr>
<tr>
<td>Improves the threat analytics process</td>
<td>51%</td>
</tr>
<tr>
<td>Standardizes the reporting of threat management activities</td>
<td>47%</td>
</tr>
<tr>
<td>Streamlines the collection of threat data</td>
<td>43%</td>
</tr>
<tr>
<td>Reduces operating costs pertaining to threat detection and remediation</td>
<td>37%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

Threat intelligence integration & performance

Integrating threat intelligence platforms with security technologies and tools can be challenging. As shown in Figure 10, 64 percent of respondents believe the integration of a threat intelligence platform with other security technologies or tools is a difficult and time-consuming task. A similar percentage (62 percent of respondents) say SIEM integration is necessary to maximize the value of threat intelligence data.

Figure 10. Perceptions about the integration of threat intelligence with security technologies
Strongly agree and Agree responses combined

<table>
<thead>
<tr>
<th>Perception</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The integration of a threat intelligence platform with other security technologies/tools is a difficult and time-consuming task</td>
<td>64%</td>
</tr>
<tr>
<td>SIEM integration is necessary to maximize the value of threat intelligence data</td>
<td>62%</td>
</tr>
</tbody>
</table>
As shown in Figure 11, the primary parts of an organization’s security architecture threat intelligence is mostly integrated into are: SIEM (52 percent of respondents), IDS/IPS (49 percent of respondents) and firewalls (46 percent of respondents). Fifty-nine percent say such integration was very difficult (27 percent of respondents) or difficult (32 percent of respondents).

**Figure 11. What parts of your security architecture do you integrate threat intelligence into?**

More than one response permitted

<table>
<thead>
<tr>
<th>Integration Type</th>
<th>Response Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIEM</td>
<td>52%</td>
</tr>
<tr>
<td>IDS / IPS</td>
<td>49%</td>
</tr>
<tr>
<td>Firewall</td>
<td>46%</td>
</tr>
<tr>
<td>WAF</td>
<td>41%</td>
</tr>
<tr>
<td>Endpoint security system</td>
<td>38%</td>
</tr>
<tr>
<td>DLP</td>
<td>23%</td>
</tr>
<tr>
<td>None of the above</td>
<td>33%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

The ability to more quickly research threats is an important feature for integration. When asked what features companies would like to see as part of the integration, 61 percent of respondents say it is to enable threat analysts to more quickly research threats, as shown in Figure 12. Other important features are management of indicators (50 percent of respondents) and integration with malware analysis automation (sandbox) (39 percent of respondents).

**Figure 12. What features are important to integration?**

Three responses permitted

<table>
<thead>
<tr>
<th>Important Feature</th>
<th>Response Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable threat analysts to more quickly research threats</td>
<td>61%</td>
</tr>
<tr>
<td>Management of indicators</td>
<td>50%</td>
</tr>
<tr>
<td>Integration with malware analysis automation (sandbox)</td>
<td>39%</td>
</tr>
<tr>
<td>Integrations with SIEM, firewall, and WAF</td>
<td>38%</td>
</tr>
<tr>
<td>Providing workflow management/prioritization for analyst teams</td>
<td>34%</td>
</tr>
<tr>
<td>Management of signatures, rules and queries and integrations with IDS/IPS</td>
<td>31%</td>
</tr>
<tr>
<td>Acting as a threat intelligence knowledge base for the security organization</td>
<td>25%</td>
</tr>
<tr>
<td>Integration with brand monitoring automation</td>
<td>23%</td>
</tr>
</tbody>
</table>
In which technologies or tools does integration of data from the platform most often occur? As shown in Figure 13, full or partial integration of threat intelligence is most likely to occur with the IPS/IDS (56 percent of respondents) and endpoint security systems (44 percent of respondents). Least likely to be fully or partially integrated are next generation firewalls or UTMs (37 percent of respondents) or DLP solutions (37 percent of respondents).

Figure 13. In which technologies does integration of data from the platform most often occur?
Full and partial integration responses combined

[Bar chart showing integration percentages for IPS/IDS (36%), Endpoint security system (27%), Web application firewall (22%), Data loss prevention solution (23%), and Next generation firewall or UTM (19%).]

Which integration was the most difficult? According to Figure 14, 66 percent of respondents say integration with endpoint security systems was very difficult (31 percent of respondents) or difficult (35 percent of respondents). The majority of respondents say integration involving IPS/IDS, WAF and DLP solutions was very difficult or difficult according to 56 percent, 56 percent and 55 percent, respectively.

Figure 14. Which integration was most difficult?
Very difficult and Difficult responses combined

[Bar chart showing very difficult and difficult percentages for Endpoint security system (35%), Web application firewall (27%), IPS/IDS (29%), Data loss prevention solution (29%), and Next generation firewall or UTM (18%).]
Which technologies experience the most diminishment (a.k.a degradation) following integration? According to Figure 15, endpoint security systems experience the most diminishment, according to 62 percent of respondents who say integration was diminished significantly (28 percent) or somewhat diminished (34 percent). Fifty-seven percent of respondents say their organizations’ IPS/IDS solution was significantly diminished (21 percent) or somewhat diminished (36 percent).

Forty-eight percent of respondents say their DLP solutions were significantly diminished (19 percent) or diminished somewhat (29 percent). To a lesser extent, integration into the WAF affected performance significantly (20 percent of respondents) or somewhat (27 percent of respondents). With respect to next generation firewall or UTM, there was significant diminishment (17 percent) or some diminishment (28 percent).

Figure 15. Which technologies experience the most degradation following integration?
Significant diminishment and Some diminishment responses combined
How open source and paid feeds compare in usage. An average of almost 10 threat intelligence feeds are used in the organizations represented in this study. As shown in Figure 16, companies are mostly using paid threat intelligence feeds (39 percent of respondents), open source (free) (28 percent of respondents) or a combination of feeds (33 percent of respondents). Forty-six percent of respondents believe paid feeds provide more actionable intelligence than free sources of threat data.

Figure 16. What is the primary source of threat intelligence used by your organization?

![Bar chart showing the primary source of threat intelligence used by organizations. Paid feeds: 39%, Combination: 33%, Open source (free): 28%]

Communication issues in disseminating threat intelligence

Threat intelligence is not often disseminated throughout the enterprise. According to Figure 17, only 32 percent of respondents say threat intelligence is used to brief or educate senior executives about cyber risks facing the company and a similar percentage (30 percent of respondents) say such communication reaches the board of directors.

Figure 17. Is threat intelligence used to educate senior executives and boards of directors?

![Bar chart showing the use of threat intelligence to educate senior executives and boards of directors. Yes: 32%, No: 44%, Unsure: 28%]

- Senior executives
- Board of directors
Figure 18 reveals that 51 percent of respondents say individuals in the IT and IT security function receive and read threat intelligence reports. However, only 25 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 32 percent of respondents. Thirty-six percent of respondents say such communication provides intelligence reports monthly or quarterly.

**Figure 18. Who reads and receives threat intelligence reports?**

![Bar chart showing percentages of respondents who read and receive threat intelligence reports.]

- 51% Yes (IT (CIO/CTO) and/or IT security (CISO/CSO) leaders)
- 25% Yes (Non-IT management)
- 34% No (IT (CIO/CTO) and/or IT security (CISO/CSO) leaders)
- 55% No (Non-IT management)
- 15% Unsure (IT (CIO/CTO) and/or IT security (CISO/CSO) leaders)
- 20% Unsure (Non-IT management)

The sharing and disseminating of threat intelligence often does not use standardized communication protocols. According to Figure 19, 56 percent of respondents say their companies do not use standardized communication protocols. If they do, it is most likely unstructured PDFs or CSVs (59 percent of respondents) or TAXII/STIX/CyBox (48 percent of respondents).

**Figure 19. What communication protocols are used?**

More than one response permitted

![Bar chart showing percentages of respondents by communication protocol.]

- 59% Unstructured PDF or CSV
- 48% TAXII/STIX/CyBOX
- 35% Open IOC
- 5% Other
Special analysis: Differences based on position level and industry

In this section, we provide an analysis of differences in perception between those respondents who hold positions at or above manager (44 percent of respondents) and those who are at or below supervisor (56 percent of respondents). The most interesting differences are as follows.

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

However, those respondents who are at the supervisor level and below believe providing workflow management/prioritization for analyst teams is more important than those in more senior positions (38 percent vs. 29 percent of respondents). Those who are in managerial positions consider management of indicators to be an important feature (55 percent vs. 47 percent of respondents).

**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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Manager &amp; above</th>
<th>Supervisor &amp; below</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable threat analysts to more quickly research threats</td>
<td>60%</td>
<td>61%</td>
</tr>
<tr>
<td>Management of indicators</td>
<td>55%</td>
<td>47%</td>
</tr>
<tr>
<td>Integration with malware analysis automation (sandbox)</td>
<td>40%</td>
<td>37%</td>
</tr>
<tr>
<td>Integrations with SIEM, firewall, and WAF</td>
<td>39%</td>
<td>37%</td>
</tr>
<tr>
<td>Providing workflow management/prioritization for analyst teams</td>
<td>29%</td>
<td>38%</td>
</tr>
<tr>
<td>Management of signatures, rules and queries and integrations with IDS/IPS</td>
<td>29%</td>
<td>32%</td>
</tr>
<tr>
<td>Integration with brand monitoring automation</td>
<td>25%</td>
<td>22%</td>
</tr>
<tr>
<td>Acting as a threat intelligence knowledge base for the security organization</td>
<td>23%</td>
<td>26%</td>
</tr>
</tbody>
</table>
**Perceptions about the SIEM integration process differ.** As shown in Figure 21, those in the trenches (supervisor and below) say the SIEM integration process was very difficult and difficult (66 percent vs. 51 percent). They are also likely to agree that there was significant or some diminishment in performance as a result of the SIEM integration (64 percent vs. 51 percent of respondents).

**Figure 21. How difficult was the SIEM integration process?**

The integration of the endpoint security process is more often considered difficult by respondents who are supervisors and below. In contrast, senior respondents say the integration process of the DLP integration process was most 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 about the diminishment in performance. In every case, the more senior level respondents are less likely to believe there was diminishment in performance due to threat intelligence integration into security architecture.

Specifically, 69 percent of respondents at the supervisor and below level say performance of the endpoint security system was diminished as opposed to 52 percent at the manager and above level.

**Figure 23. How threat intelligence integration into security architecture affects performance**

Significant diminishment and Some diminishment responses combined

![Diagram showing the percentage of respondents in different levels who believe in significant and some diminishment of various security components.](image)
Respondents at the manager level and above are more likely to believe that a threat intelligence platform is necessary to maximize the value of threat intelligence data (82 percent vs. 77 percent of respondents) and 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 (60 percent vs. 67 percent). Senior-level respondents are less likely to believe threat data is often too voluminous and/or complex to provide actionable intelligence (65 percent vs. 74 percent of respondents).

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

- A threat intelligence platform is necessary to maximize the value of threat intelligence data
  - Manager & above: 82%
  - Supervisor & below: 77%

- SIEM integration is necessary to maximize the value of threat intelligence data
  - Manager & above: 66%
  - Supervisor & below: 60%

- Threat data is often too voluminous and/or complex to provide actionable intelligence
  - Manager & above: 65%
  - Supervisor & below: 74%

- The integration of a threat intelligence platform with other security technologies/tools is a difficult and time-consuming task
  - Manager & above: 60%
  - Supervisor & below: 67%
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 key differences are as follows.

Organizations with a headcount of less than 5,000 find the integration of threat intelligence as more difficult than those organizations with a headcount above 5,000. The integration process of the endpoint security system, IPS/IDS integration process, DLP integration process and the WAF integration process (72 percent, 61 percent, 61 percent of respondents and 60 percent, respectively) are the most difficult for smaller organization.

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

![Chart showing difficulty in threat intelligence integration into security architecture](chart.png)
Smaller organizations are also more likely to experience performance diminishment with the integration of threat intelligence into security architecture. This is especially the case with the endpoint security system and SIEM.

**Figure 26. How threat intelligence integration into security architecture affects performance**

Significant diminishment and Some diminishment responses combined

<table>
<thead>
<tr>
<th>Performance of Security Element</th>
<th>Below 5,000</th>
<th>Above 5,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance of the endpoint security system</td>
<td>54%</td>
<td>69%</td>
</tr>
<tr>
<td>Performance of the SIEM</td>
<td>54%</td>
<td>62%</td>
</tr>
<tr>
<td>Performance of the IPS/IDS</td>
<td>54%</td>
<td>60%</td>
</tr>
<tr>
<td>Performance of the DLP solution</td>
<td>41%</td>
<td>54%</td>
</tr>
<tr>
<td>Performance of the WAF</td>
<td>40%</td>
<td>54%</td>
</tr>
<tr>
<td>Performance of the NGFW or UTM</td>
<td>35%</td>
<td>54%</td>
</tr>
</tbody>
</table>

Both large and smaller organizations believe a threat intelligence platform is necessary to maximize the value of threat intelligence data (82 percent and 77 percent of respondents, respectively). They also agree that threat data is often too voluminous and/or complex to provide actionable intelligence (71 percent and 69 percent of respondents).

**Figure 27. Perceptions about the value of threat intelligence**

Strongly agree and Agree responses combined

<table>
<thead>
<tr>
<th>Perceived Need</th>
<th>Below 5,000</th>
<th>Above 5,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>A threat intelligence platform is necessary to maximize the value of threat intelligence data</td>
<td>77%</td>
<td>82%</td>
</tr>
<tr>
<td>Threat data is often too voluminous and/or complex to provide actionable intelligence</td>
<td>71%</td>
<td>69%</td>
</tr>
<tr>
<td>The integration of a threat intelligence platform with other security technologies/tools is a difficult and time-consuming task</td>
<td>67%</td>
<td>61%</td>
</tr>
<tr>
<td>SIEM integration is necessary to maximize the value of threat intelligence data</td>
<td>59%</td>
<td>66%</td>
</tr>
</tbody>
</table>
Part 3. Methods

A sampling frame of 31,910 IT or IT security practitioners located in North America and the United Kingdom were selected as participants in the research. Table 1 shows 1,224 total returns. Screening and reliability checks required the removal of 152 surveys. Our final sample consisted of 1,072 surveys or a 3.4 percent response rate.

<table>
<thead>
<tr>
<th>Table 1. Sample response</th>
<th>Freq</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>31,910</td>
<td>100.0%</td>
</tr>
<tr>
<td>Total returns</td>
<td>1,224</td>
<td>3.8%</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>152</td>
<td>0.5%</td>
</tr>
<tr>
<td>Final sample</td>
<td>1,072</td>
<td>3.4%</td>
</tr>
</tbody>
</table>

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

Pie Chart 1. Position level within the organization

Pie Chart 2 shows that 69 percent of the respondents are from organizations with a global headcount of more than 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 health and pharmaceutical (10 percent of respondents).

**Pie Chart 3. Primary industry segment**

Pie Chart 4 shows that 60 percent of the respondents’ organizations are located in North America, and 27 percent are in Europe.

**Pie Chart 4. Headquarter location of the organization**
Pie Chart 5 reports the global footprint of the respondents’ organization. Thirty-four percent of the respondents have operations in 2 or more countries in multiple regions, 28 percent have operations in all global regions and 26 percent of respondents have operations in 2 or more countries in one region.

Pie Chart 5. 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 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 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 May 2016.

<table>
<thead>
<tr>
<th>Survey response</th>
<th>Combined</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>31,910</td>
<td>100.0%</td>
</tr>
<tr>
<td>Total returns</td>
<td>1,224</td>
<td>3.8%</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>152</td>
<td>0.5%</td>
</tr>
<tr>
<td>Final sample</td>
<td>1,072</td>
<td>3.4%</td>
</tr>
</tbody>
</table>

**Part 1. Screening questions**

<table>
<thead>
<tr>
<th>Question</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1a. Does your organization utilize threat intelligence as part of its cybersecurity program or infrastructure?</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>64%</td>
</tr>
<tr>
<td>No (stop)</td>
<td>36%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reason</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not considered a priority</td>
<td>30%</td>
</tr>
<tr>
<td>Lack of staff expertise</td>
<td>51%</td>
</tr>
<tr>
<td>Lack of technologies</td>
<td>47%</td>
</tr>
<tr>
<td>Cost of prevailing solutions (TCO)</td>
<td>58%</td>
</tr>
<tr>
<td>Threat data is insufficient to pinpoint IOCs</td>
<td>42%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>230%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>S2. What best defines your level of involvement in your organization’s IT security operations?</td>
<td></td>
</tr>
<tr>
<td>Significant involvement</td>
<td>41%</td>
</tr>
<tr>
<td>Some involvement</td>
<td>59%</td>
</tr>
<tr>
<td>Minimal or no involvement (stop)</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role/function</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security leader (e.g., CISO)</td>
<td>19%</td>
</tr>
<tr>
<td>Security threat analyst</td>
<td>13%</td>
</tr>
<tr>
<td>Security operations</td>
<td>37%</td>
</tr>
<tr>
<td>Security systems engineering</td>
<td>6%</td>
</tr>
<tr>
<td>Security architecture</td>
<td>6%</td>
</tr>
<tr>
<td>Security policy / compliance</td>
<td>6%</td>
</tr>
<tr>
<td>Security project management</td>
<td>3%</td>
</tr>
<tr>
<td>Incident response / disaster recovery</td>
<td>10%</td>
</tr>
<tr>
<td>None of the above (stop)</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
### Part 2. Organizational characteristics

#### D1. What best defines your position level within the organization?

<table>
<thead>
<tr>
<th>Position Level</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive/VP</td>
<td>5%</td>
</tr>
<tr>
<td>Director</td>
<td>17%</td>
</tr>
<tr>
<td>Manager</td>
<td>22%</td>
</tr>
<tr>
<td>Supervisor</td>
<td>15%</td>
</tr>
<tr>
<td>Staff/Associate</td>
<td>10%</td>
</tr>
<tr>
<td>Technician</td>
<td>29%</td>
</tr>
<tr>
<td>Contractor</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

#### D2. What best defines the global employee headcount of your organization?

<table>
<thead>
<tr>
<th>Employee Count Range</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 100</td>
<td>3%</td>
</tr>
<tr>
<td>100 to 500</td>
<td>14%</td>
</tr>
<tr>
<td>501 to 1,000</td>
<td>14%</td>
</tr>
<tr>
<td>1,001 to 5,000</td>
<td>23%</td>
</tr>
<tr>
<td>5,001 to 10,000</td>
<td>15%</td>
</tr>
<tr>
<td>10,001 to 25,000</td>
<td>11%</td>
</tr>
<tr>
<td>25,001 to 50,000</td>
<td>9%</td>
</tr>
<tr>
<td>50,001 to 75,000</td>
<td>6%</td>
</tr>
<tr>
<td>More than 75,000</td>
<td>5%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

#### D3. What best defines your organization’s primary industry segment?

<table>
<thead>
<tr>
<th>Industry Segment</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture &amp; food services</td>
<td>1%</td>
</tr>
<tr>
<td>Communications</td>
<td>2%</td>
</tr>
<tr>
<td>Consumer products</td>
<td>5%</td>
</tr>
<tr>
<td>Defense &amp; aerospace</td>
<td>1%</td>
</tr>
<tr>
<td>Education &amp; research</td>
<td>2%</td>
</tr>
<tr>
<td>Energy &amp; utilities</td>
<td>6%</td>
</tr>
<tr>
<td>Entertainment &amp; media</td>
<td>3%</td>
</tr>
<tr>
<td>Financial services</td>
<td>17%</td>
</tr>
<tr>
<td>Health &amp; pharmaceutical</td>
<td>10%</td>
</tr>
<tr>
<td>Hospitality</td>
<td>4%</td>
</tr>
<tr>
<td>Industrial/manufacturing</td>
<td>8%</td>
</tr>
<tr>
<td>Public sector</td>
<td>11%</td>
</tr>
<tr>
<td>Retail</td>
<td>9%</td>
</tr>
<tr>
<td>Services</td>
<td>9%</td>
</tr>
<tr>
<td>Technology &amp; software</td>
<td>8%</td>
</tr>
<tr>
<td>Transportation</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

#### D4. Where is your organization headquartered? Please choose only one region.

<table>
<thead>
<tr>
<th>Region</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America (U.S. &amp; Canada)</td>
<td>60%</td>
</tr>
<tr>
<td>Europe</td>
<td>27%</td>
</tr>
<tr>
<td>Middle east and Africa</td>
<td>3%</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>7%</td>
</tr>
<tr>
<td>Latin America (plus Mexico)</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
D5. What best defines your organization’s global footprint

<table>
<thead>
<tr>
<th>Operations</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mostly in one country</td>
<td>12%</td>
</tr>
<tr>
<td>In 2 or more countries in one region</td>
<td>26%</td>
</tr>
<tr>
<td>In 2 or more countries in multiple regions</td>
<td>34%</td>
</tr>
<tr>
<td>In all global regions</td>
<td>28%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

**Part 3. Background questions**

**Q1.** Using the following 10-point scale, please rate the importance of threat intelligence with respect to your organization’s ability to achieve a strong cybersecurity posture. 1 = low (irrelevant) to 10 = high (essential).

<table>
<thead>
<tr>
<th>Rating (1-10)</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2</td>
<td>3%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>5%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>14%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>26%</td>
</tr>
<tr>
<td>9 or 10</td>
<td>52%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
<tr>
<td><strong>Extrapolated average</strong></td>
<td>7.90</td>
</tr>
</tbody>
</table>

**Q2a.** Using the following 10-point scale, please rate your organization’s effectiveness in utilizing threat data to pinpoint cyber threats. 1 = low (ineffective) to 10 = high (very effective).

<table>
<thead>
<tr>
<th>Rating (1-10)</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2</td>
<td>12%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>23%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>38%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>18%</td>
</tr>
<tr>
<td>9 or 10</td>
<td>9%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
<tr>
<td><strong>Extrapolated average</strong></td>
<td>5.28</td>
</tr>
</tbody>
</table>

**Q2b.** [Ratings at 5 or below] Why is your organization relatively ineffective in utilizing threat data?

<table>
<thead>
<tr>
<th>Reason</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of staff expertise</td>
<td>69%</td>
</tr>
<tr>
<td>Lack of ownership</td>
<td>58%</td>
</tr>
<tr>
<td>Lack of suitable technologies</td>
<td>52%</td>
</tr>
<tr>
<td>Threat data is not reliable or sufficient to pinpoint IOCs</td>
<td>46%</td>
</tr>
<tr>
<td>Not considered a priority</td>
<td>24%</td>
</tr>
<tr>
<td>Interoperability issues</td>
<td>17%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>267%</td>
</tr>
</tbody>
</table>

**Q3.** What is the primary source of threat intelligence used by your organization?

<table>
<thead>
<tr>
<th>Source</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open source (free)</td>
<td>28%</td>
</tr>
<tr>
<td>Paid feeds</td>
<td>39%</td>
</tr>
<tr>
<td>Combination</td>
<td>33%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>
Q4. Approximately, how many threat intelligence feeds are used by your organization today?

<table>
<thead>
<tr>
<th>Number of Threat Intelligence Feeds</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>22%</td>
</tr>
<tr>
<td>2 to 5</td>
<td>16%</td>
</tr>
<tr>
<td>6 to 10</td>
<td>35%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>17%</td>
</tr>
<tr>
<td>21 to 40</td>
<td>7%</td>
</tr>
<tr>
<td>More than 40</td>
<td>4%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Extrapolated average 9.78

Q5a. Who are the **primary users** of threat intelligence within your organization? Please select all that apply.

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application development</td>
<td>4%</td>
</tr>
<tr>
<td>Board of directors</td>
<td>0%</td>
</tr>
<tr>
<td>Business continuity management</td>
<td>8%</td>
</tr>
<tr>
<td>Compliance</td>
<td>26%</td>
</tr>
<tr>
<td>Enterprise risk management</td>
<td>44%</td>
</tr>
<tr>
<td>Executive management (CEO, COO)</td>
<td>3%</td>
</tr>
<tr>
<td>Human resources</td>
<td>3%</td>
</tr>
<tr>
<td>Incident response team</td>
<td>79%</td>
</tr>
<tr>
<td>Internal audit</td>
<td>20%</td>
</tr>
<tr>
<td>IT leaders (CIO, CTO)</td>
<td>59%</td>
</tr>
<tr>
<td>IT operations</td>
<td>57%</td>
</tr>
<tr>
<td>Non-IT management</td>
<td>5%</td>
</tr>
<tr>
<td>Procurement</td>
<td>4%</td>
</tr>
<tr>
<td>Security leaders (CISO, CSO)</td>
<td>81%</td>
</tr>
<tr>
<td>Security operations</td>
<td>44%</td>
</tr>
</tbody>
</table>

Q5b. Who are the **secondary users** of threat intelligence within your organization? Please select all that apply.

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application development</td>
<td>20%</td>
</tr>
<tr>
<td>Board of directors</td>
<td>9%</td>
</tr>
<tr>
<td>Business continuity management</td>
<td>15%</td>
</tr>
<tr>
<td>Compliance</td>
<td>51%</td>
</tr>
<tr>
<td>Enterprise risk management</td>
<td>32%</td>
</tr>
<tr>
<td>Executive management (CEO, COO)</td>
<td>17%</td>
</tr>
<tr>
<td>Human resources</td>
<td>20%</td>
</tr>
<tr>
<td>Incident response team</td>
<td>23%</td>
</tr>
<tr>
<td>Internal audit</td>
<td>27%</td>
</tr>
<tr>
<td>IT leaders (CIO, CTO)</td>
<td>39%</td>
</tr>
<tr>
<td>IT operations</td>
<td>40%</td>
</tr>
<tr>
<td>Non-IT management</td>
<td>10%</td>
</tr>
<tr>
<td>Procurement</td>
<td>8%</td>
</tr>
<tr>
<td>Security leaders (CISO, CSO)</td>
<td>19%</td>
</tr>
<tr>
<td>Security operations</td>
<td>41%</td>
</tr>
</tbody>
</table>

Q6a. Does your organization deploy a threat intelligence platform?

<table>
<thead>
<tr>
<th>Deployment Plan</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes (Go to Q7)</td>
<td>42%</td>
</tr>
<tr>
<td>No, but planning to deploy within the next 12 months</td>
<td>12%</td>
</tr>
<tr>
<td>No, but planning to deploy more than 12 months from now</td>
<td>10%</td>
</tr>
<tr>
<td>No plan to deploy</td>
<td>36%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
<tr>
<td>Q6b. If no, why doesn’t your organization deploy a threat intelligence platform?</td>
<td>Combined</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Not considered a priority</td>
<td>15%</td>
</tr>
<tr>
<td>Lack of staff expertise</td>
<td>56%</td>
</tr>
<tr>
<td>Lack of suitable technologies</td>
<td>40%</td>
</tr>
<tr>
<td>Cost of prevailing solutions (TCO)</td>
<td>48%</td>
</tr>
<tr>
<td>Threat data alone is sufficient to pinpoint IOCs</td>
<td>36%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>195%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q6c. If no, how difficult is the process of prioritizing threat intelligence data (without a platform)?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very difficult</td>
<td>35%</td>
</tr>
<tr>
<td>Difficult</td>
<td>35%</td>
</tr>
<tr>
<td>Somewhat difficult</td>
<td>21%</td>
</tr>
<tr>
<td>Not difficult</td>
<td>9%</td>
</tr>
<tr>
<td>Easy</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q6d. If no, what do threat analysts within your organization do with the results of their efforts?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass results to the security operations team</td>
<td>71%</td>
</tr>
<tr>
<td>Pass results to the incident response team</td>
<td>62%</td>
</tr>
<tr>
<td>Pass results to IT security leadership</td>
<td>45%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>3%</td>
</tr>
<tr>
<td>Total [Go to Q18a]</td>
<td>181%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q7. What are the main benefits of having a threat intelligence platform? Please select all that apply.</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helps pinpoint and prioritize IOCs</td>
<td>70%</td>
</tr>
<tr>
<td>Streamlines the collection of threat data</td>
<td>43%</td>
</tr>
<tr>
<td>Improves the threat analytics process</td>
<td>51%</td>
</tr>
<tr>
<td>Standardizes the reporting of threat management activities</td>
<td>47%</td>
</tr>
<tr>
<td>Reduces operating costs pertaining to threat detection and remediation</td>
<td>37%</td>
</tr>
<tr>
<td>Integrates threat data with other enabling security solutions (such as SIEM)</td>
<td>59%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>312%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q8. Is the threat intelligence platform deployed consistently across the organization?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>45%</td>
</tr>
<tr>
<td>No</td>
<td>55%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q9. How difficult is the process of prioritizing threat intelligence data (with a platform)?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very difficult</td>
<td>24%</td>
</tr>
<tr>
<td>Difficult</td>
<td>29%</td>
</tr>
<tr>
<td>Somewhat difficult</td>
<td>24%</td>
</tr>
<tr>
<td>Not difficult</td>
<td>16%</td>
</tr>
<tr>
<td>Easy</td>
<td>7%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
### Q10a. What parts of your security architecture do you integrate threat intelligence into? Please select all that apply.

<table>
<thead>
<tr>
<th>Integration</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>46%</td>
</tr>
<tr>
<td>SIEM</td>
<td>52%</td>
</tr>
<tr>
<td>Endpoint security system</td>
<td>38%</td>
</tr>
<tr>
<td>IDS / IPS</td>
<td>49%</td>
</tr>
<tr>
<td>WAF</td>
<td>41%</td>
</tr>
<tr>
<td>DLP</td>
<td>23%</td>
</tr>
<tr>
<td>None of the above (Go to Q11)</td>
<td>33%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>3%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>284%</strong></td>
</tr>
</tbody>
</table>

### Q10b. What features would you like to see as part of the integration that you don’t already have? Top 3 choices

<table>
<thead>
<tr>
<th>Feature</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of Indicators</td>
<td>50%</td>
</tr>
<tr>
<td>Integrations with SIEM, Firewall, and WAF</td>
<td>38%</td>
</tr>
<tr>
<td>Management of Signatures, Rules and Queries and integrations with IDS/IPS</td>
<td>31%</td>
</tr>
<tr>
<td>Acting as a Threat Intelligence Knowledge Base (replacing a Wiki or SharePoint site) for the security organization</td>
<td>25%</td>
</tr>
<tr>
<td>Enable threat analysts to more quickly research threats</td>
<td>61%</td>
</tr>
<tr>
<td>Providing workflow management / prioritization for analyst teams</td>
<td>34%</td>
</tr>
<tr>
<td>Integration with malware analysis automation (sandbox)</td>
<td>39%</td>
</tr>
<tr>
<td>Integration with brand monitoring automation</td>
<td>23%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>300%</strong></td>
</tr>
</tbody>
</table>

### Q10c. How difficult was the integration process?

<table>
<thead>
<tr>
<th>Difficulty</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very difficult</td>
<td>27%</td>
</tr>
<tr>
<td>Difficult</td>
<td>32%</td>
</tr>
<tr>
<td>Somewhat difficult</td>
<td>25%</td>
</tr>
<tr>
<td>Not difficult</td>
<td>12%</td>
</tr>
<tr>
<td>Easy</td>
<td>4%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

### Q10d. How does integration affect performance of the SIEM?

<table>
<thead>
<tr>
<th>Performance</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant diminishment</td>
<td>25%</td>
</tr>
<tr>
<td>Some diminishment</td>
<td>34%</td>
</tr>
<tr>
<td>Minimal diminishment</td>
<td>22%</td>
</tr>
<tr>
<td>No diminishment</td>
<td>19%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

### Q10e. How many days of log data does your organization keep live and online in your SIEM?

<table>
<thead>
<tr>
<th>Days of Log Data</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 day</td>
<td>1%</td>
</tr>
<tr>
<td>1 to 7 days</td>
<td>13%</td>
</tr>
<tr>
<td>1 to 4 weeks</td>
<td>37%</td>
</tr>
<tr>
<td>1 to 3 months</td>
<td>24%</td>
</tr>
<tr>
<td>4 to 6 months</td>
<td>12%</td>
</tr>
<tr>
<td>7 to 12 months</td>
<td>10%</td>
</tr>
<tr>
<td>1 to 2 years</td>
<td>2%</td>
</tr>
<tr>
<td>More than 2 years</td>
<td>1%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
### Q11a. Does your threat intelligence platform integrate data from the platform into an IPS/IDS?

<table>
<thead>
<tr>
<th>Option</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, full integration</td>
<td>20%</td>
</tr>
<tr>
<td>Yes, partial integration</td>
<td>36%</td>
</tr>
<tr>
<td>No</td>
<td>44%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q11b. How difficult was the integration process?

<table>
<thead>
<tr>
<th>Difficulty Level</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very difficult</td>
<td>27%</td>
</tr>
<tr>
<td>Difficult</td>
<td>29%</td>
</tr>
<tr>
<td>Somewhat difficult</td>
<td>23%</td>
</tr>
<tr>
<td>Not difficult</td>
<td>17%</td>
</tr>
<tr>
<td>Easy</td>
<td>4%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q11c. How does integration affect performance of the IPS/IDS?

<table>
<thead>
<tr>
<th>Impact Level</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant diminishment</td>
<td>21%</td>
</tr>
<tr>
<td>Some diminishment</td>
<td>36%</td>
</tr>
<tr>
<td>Minimal diminishment</td>
<td>20%</td>
</tr>
<tr>
<td>No diminishment</td>
<td>22%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q12a. Does your threat intelligence platform integrate data from the platform into a next generation firewall (NGFW) or UTM?

<table>
<thead>
<tr>
<th>Option</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, full integration</td>
<td>18%</td>
</tr>
<tr>
<td>Yes, partial integration</td>
<td>19%</td>
</tr>
<tr>
<td>No</td>
<td>64%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q12b. How difficult was the integration process?

<table>
<thead>
<tr>
<th>Difficulty Level</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very difficult</td>
<td>20%</td>
</tr>
<tr>
<td>Difficult</td>
<td>18%</td>
</tr>
<tr>
<td>Somewhat difficult</td>
<td>28%</td>
</tr>
<tr>
<td>Not difficult</td>
<td>22%</td>
</tr>
<tr>
<td>Easy</td>
<td>12%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q12c. How does integration affect performance of the NGFW or UTM?

<table>
<thead>
<tr>
<th>Impact Level</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant diminishment</td>
<td>17%</td>
</tr>
<tr>
<td>Some diminishment</td>
<td>28%</td>
</tr>
<tr>
<td>Minimal diminishment</td>
<td>25%</td>
</tr>
<tr>
<td>No diminishment</td>
<td>30%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q13a. Does your threat intelligence platform integrate data from the platform into a web application firewall (WAF)?

<table>
<thead>
<tr>
<th>Option</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, full integration</td>
<td>21%</td>
</tr>
<tr>
<td>Yes, partial integration</td>
<td>22%</td>
</tr>
<tr>
<td>No</td>
<td>57%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
<tr>
<td>Q13b. How difficult was the integration process?</td>
<td>Combined</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Very difficult</td>
<td>29%</td>
</tr>
<tr>
<td>Difficult</td>
<td>27%</td>
</tr>
<tr>
<td>Somewhat difficult</td>
<td>29%</td>
</tr>
<tr>
<td>Not difficult</td>
<td>9%</td>
</tr>
<tr>
<td>Easy</td>
<td>5%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q13c. How does integration affect performance of the WAF?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant diminishment</td>
<td>20%</td>
</tr>
<tr>
<td>Some diminishment</td>
<td>27%</td>
</tr>
<tr>
<td>Minimal diminishment</td>
<td>31%</td>
</tr>
<tr>
<td>No diminishment</td>
<td>22%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q14a. Does your threat intelligence platform integrate data from the platform into a data loss prevention (DLP) solution?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, full integration</td>
<td>14%</td>
</tr>
<tr>
<td>Yes, partial integration</td>
<td>23%</td>
</tr>
<tr>
<td>No</td>
<td>64%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q14b. How difficult was the integration process?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very difficult</td>
<td>26%</td>
</tr>
<tr>
<td>Difficult</td>
<td>29%</td>
</tr>
<tr>
<td>Somewhat difficult</td>
<td>28%</td>
</tr>
<tr>
<td>Not difficult</td>
<td>13%</td>
</tr>
<tr>
<td>Easy</td>
<td>5%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q14c. How does integration affect performance of the DLP solution?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant diminishment</td>
<td>19%</td>
</tr>
<tr>
<td>Some diminishment</td>
<td>29%</td>
</tr>
<tr>
<td>Minimal diminishment</td>
<td>29%</td>
</tr>
<tr>
<td>No diminishment</td>
<td>23%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q15a. Does your threat intelligence platform integrate data from the platform into an endpoint security system?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, full integration</td>
<td>17%</td>
</tr>
<tr>
<td>Yes, partial integration</td>
<td>27%</td>
</tr>
<tr>
<td>No</td>
<td>56%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q15b. How difficult was the integration process?</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very difficult</td>
<td>31%</td>
</tr>
<tr>
<td>Difficult</td>
<td>35%</td>
</tr>
<tr>
<td>Somewhat difficult</td>
<td>21%</td>
</tr>
<tr>
<td>Not difficult</td>
<td>10%</td>
</tr>
<tr>
<td>Easy</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q15c. How does integration affect performance of the endpoint security system?

<table>
<thead>
<tr>
<th>Effect</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant diminishment</td>
<td>28%</td>
</tr>
<tr>
<td>Some diminishment</td>
<td>34%</td>
</tr>
<tr>
<td>Minimal diminishment</td>
<td>20%</td>
</tr>
<tr>
<td>No diminishment</td>
<td>18%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q16. 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? Top 3 choices

<table>
<thead>
<tr>
<th>Function</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of Indicators</td>
<td>48%</td>
</tr>
<tr>
<td>Integrations with SIEM, Firewall, and WAF</td>
<td>67%</td>
</tr>
<tr>
<td>Management of Signatures, Rules and Queries and integrations with IDS/IPS</td>
<td>29%</td>
</tr>
<tr>
<td>Acting as a Threat Intelligence Knowledge Base (replacing a Wiki or SharePoint site) for the security organization</td>
<td>32%</td>
</tr>
<tr>
<td>Enable threat analysts to more quickly research threats</td>
<td>48%</td>
</tr>
<tr>
<td>Providing workflow management / prioritization for analyst teams</td>
<td>22%</td>
</tr>
<tr>
<td>Integration with malware analysis automation (sandbox)</td>
<td>36%</td>
</tr>
<tr>
<td>Integration with brand monitoring automation</td>
<td>17%</td>
</tr>
<tr>
<td>Total</td>
<td>300%</td>
</tr>
</tbody>
</table>

Q17. How do threat analysts prioritize their work in the threat intelligence platform?

<table>
<thead>
<tr>
<th>Method</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>First-in first-out</td>
<td>42%</td>
</tr>
<tr>
<td>Using tools within the threat intelligence platform</td>
<td>45%</td>
</tr>
<tr>
<td>Using an external task management system (e.g. JIRA)</td>
<td>36%</td>
</tr>
<tr>
<td>Information from the SOC team</td>
<td>44%</td>
</tr>
<tr>
<td>Using a ticket system (e.g. RT)</td>
<td>35%</td>
</tr>
<tr>
<td>Unstructured data (such as email)</td>
<td>12%</td>
</tr>
<tr>
<td>Bulletins from the threat intelligence platform vendor</td>
<td>48%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>264%</td>
</tr>
</tbody>
</table>

Q18a. Does your organization share/disseminate threat intelligence using standardized communication protocols?

<table>
<thead>
<tr>
<th>Answer</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>44%</td>
</tr>
<tr>
<td>No</td>
<td>56%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q18b. If yes, what communication protocols are used? Please select all that apply.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAXII/STIX/CyBOX</td>
<td>48%</td>
</tr>
<tr>
<td>Open IOC</td>
<td>35%</td>
</tr>
<tr>
<td>Unstructured PDF or CSV</td>
<td>59%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>5%</td>
</tr>
<tr>
<td>Total</td>
<td>147%</td>
</tr>
</tbody>
</table>

Q19. What best describes the level of alignment between your organization’s threat analysts and its security operations team?

<table>
<thead>
<tr>
<th>Alignment Status</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully aligned</td>
<td>21%</td>
</tr>
<tr>
<td>Partially aligned</td>
<td>37%</td>
</tr>
<tr>
<td>Not aligned</td>
<td>42%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q20. Does threat intelligence drive decision-making within your organization’s security operations center (SOC)?

<table>
<thead>
<tr>
<th></th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>57%</td>
</tr>
<tr>
<td>No</td>
<td>43%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q21. Do your organization’s IT (CIO/CTO) and/or IT security (CISO/CSO) leaders receive and read threat intelligence reports?

<table>
<thead>
<tr>
<th></th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>51%</td>
</tr>
<tr>
<td>No</td>
<td>34%</td>
</tr>
<tr>
<td>Unsure</td>
<td>15%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q22. Do your organization’s non-IT management receive and read intelligence reports?

<table>
<thead>
<tr>
<th></th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>25%</td>
</tr>
<tr>
<td>No</td>
<td>55%</td>
</tr>
<tr>
<td>Unsure</td>
<td>20%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q23. How often are these intelligence reports issued and disseminated?

<table>
<thead>
<tr>
<th></th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hourly</td>
<td>2%</td>
</tr>
<tr>
<td>Daily</td>
<td>5%</td>
</tr>
<tr>
<td>Weekly</td>
<td>10%</td>
</tr>
<tr>
<td>Monthly</td>
<td>19%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>17%</td>
</tr>
<tr>
<td>Semi-annually</td>
<td>7%</td>
</tr>
<tr>
<td>Annually</td>
<td>9%</td>
</tr>
<tr>
<td>No regular intervals (on demand)</td>
<td>32%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q24. Is threat intelligence used to educate/brief your organization’s senior executives about cyber risks?

<table>
<thead>
<tr>
<th></th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>32%</td>
</tr>
<tr>
<td>No</td>
<td>44%</td>
</tr>
<tr>
<td>Unsure</td>
<td>24%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q25. Is threat intelligence used to educate/brief your organization’s board of directors about cyber risks?

<table>
<thead>
<tr>
<th></th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>30%</td>
</tr>
<tr>
<td>No</td>
<td>42%</td>
</tr>
<tr>
<td>Unsure</td>
<td>28%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q26. Using the following 10-point scale, please rate the value of threat intelligence to your organization’s overall security mission. 1 = low value to 10 = high value.

<table>
<thead>
<tr>
<th></th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2</td>
<td>2%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>8%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>14%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>31%</td>
</tr>
<tr>
<td>9 or 10</td>
<td>46%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
<tr>
<td>Extrapolated average</td>
<td>7.70</td>
</tr>
</tbody>
</table>
### Part 3. Attributions

Please rate each statement using the agreement scale provided below each item. % Strongly Agree and Agree response.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q27. SIEM integration is necessary to maximize the value of threat intelligence data.</td>
<td>62%</td>
</tr>
<tr>
<td>Q28. Threat data is often too voluminous and/or complex to provide actionable intelligence.</td>
<td>70%</td>
</tr>
<tr>
<td>Q29. A threat intelligence platform is necessary to maximize the value of threat intelligence data.</td>
<td>79%</td>
</tr>
<tr>
<td>Q30. A qualified threat analyst is essential to maximize the value of threat intelligence data.</td>
<td>52%</td>
</tr>
<tr>
<td>Q31. Paid threat feeds provide more actionable intelligence than free sources of threat data.</td>
<td>46%</td>
</tr>
<tr>
<td>Q32. The integration of a threat intelligence platform with other security technologies/tools is a difficult and time-consuming task.</td>
<td>64%</td>
</tr>
<tr>
<td>Q33. In my organization, threat analyst activities are often not aligned with operational security events.</td>
<td>55%</td>
</tr>
<tr>
<td>Q34. In my organization, incident responders utilize threat data when deciding how to respond to threats.</td>
<td>46%</td>
</tr>
</tbody>
</table>

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

---

**Ponemon Institute**

*Advancing Responsible Information Management*

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

As a member of the Council of American Survey Research Organizations (CASRO), 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.