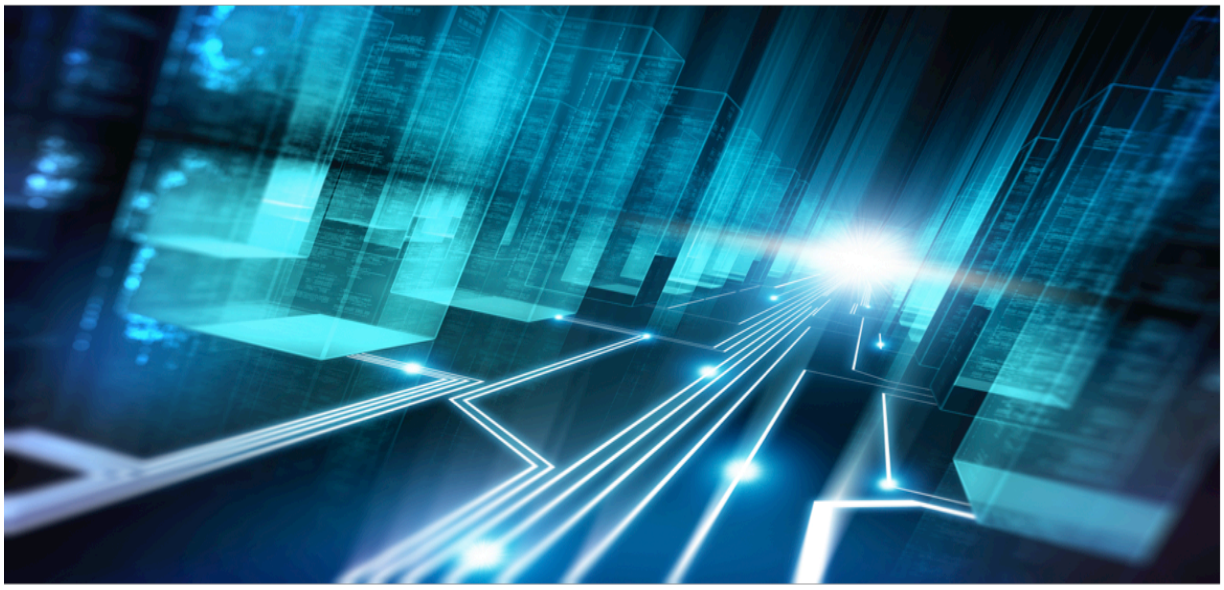


QRadar Security Intelligence Client Study

Sponsored by IBM

Independently conducted by Ponemon Institute LLC

Publication Date: December 2018

QRadar Security Intelligence Client Study

Ponemon Institute, December 2018

Part 1. Introduction

Ponemon Institute is pleased to present the results of *QRadar Security Intelligence Client Study* sponsored by IBM. The purpose of this research is to develop quantitative statistics documenting the required time, skills and the typical workflow IT security teams utilize to investigate suspected network attacks, security breaches and recognized data loss scenarios.

We surveyed 304 US IT and IT security practitioners in organizations that use QRadar Security Intelligence to monitor and defend their company's network. As part of the research we also surveyed 479 users of other SIEM solutions.

Following are key takeaways from this research.

QRadar helps to reduce the headcount associated with daily security incident investigations. Seventy-eight percent of respondents say they were able to reduce the headcount associated with daily security incident investigations by a half full-time equivalent and 19 percent of respondents say their headcount was reduced by one full-time equivalent.

T**he amount of time invested in tuning QRadar decreases following deployment.** Forty percent of respondents say the time to tune QRadar decreased during the first month of deployment. Only 12 percent of respondents say there was no decrease in time since deployment.

Customers benefit from QRadar within days or a week. Most respondents (73 percent) say their organizations recognized the value of QRadar within days (39 percent) or within a week (34 percent).

Out-of-box QRadar correlation rules are considered very valuable and most say bringing logs into QRadar for correlation and analysis is very easy. Fifty-four percent of respondents say it is very easy to bring logs into QRadar for correlation and analysis and 70 percent of respondents say out-of-box QRadar correlation rules are valuable. According to the research, an average of 34 custom correlation rules have been created.

QRadar increases the ability to accurately detect real attacks by 51 percent. Following the deployment of QRadar the average percentage of real attacks that organizations are able to accurately detect increases from 47 percent to 79. An average of only 15 percent of Offenses in QRadar are false positives.

Additional professional services were purchased to assist with QRadar deployment. Sixty-five percent of respondents say their organizations purchased additional professional services to assist with QRadar since it was implemented. An average of five days of professional services were purchased primarily for new module installation (37 percent of respondents), integrations (35 percent of respondents) and for tuning (32 percent of respondents).

Most organizations have a dedicated in-house team to manage their QRadar solution. Forty-three percent of respondents say that their organizations have a dedicated in-house team to maintain the solution, tune rules and manage threats. One-third of respondents say they outsource most QRadar management to a service provider, and 24 percent of respondents say their organization outsources management, but maintains an in-house team to investigate and respond to threats.

QRadar Network Insights is the add-on solution most often used. Fifty-five percent of respondents say their organizations use QRadar Network Insights to gain real-time insight into network packets and metadata and 49 percent use QRadar Vulnerability Manager to prioritize vulnerabilities and correlate asset vulnerabilities against threat intelligence and security events.

Organizations find QRadar features to be very valuable. Respondents especially rate out-of-the-box algorithms for detecting anomalous user and entity behavior as very valuable.

Part 2. Key findings

In this section, we provide a deeper analysis of the key findings. The complete audited findings are presented in the Appendix of this report. Topics in this research include the following:

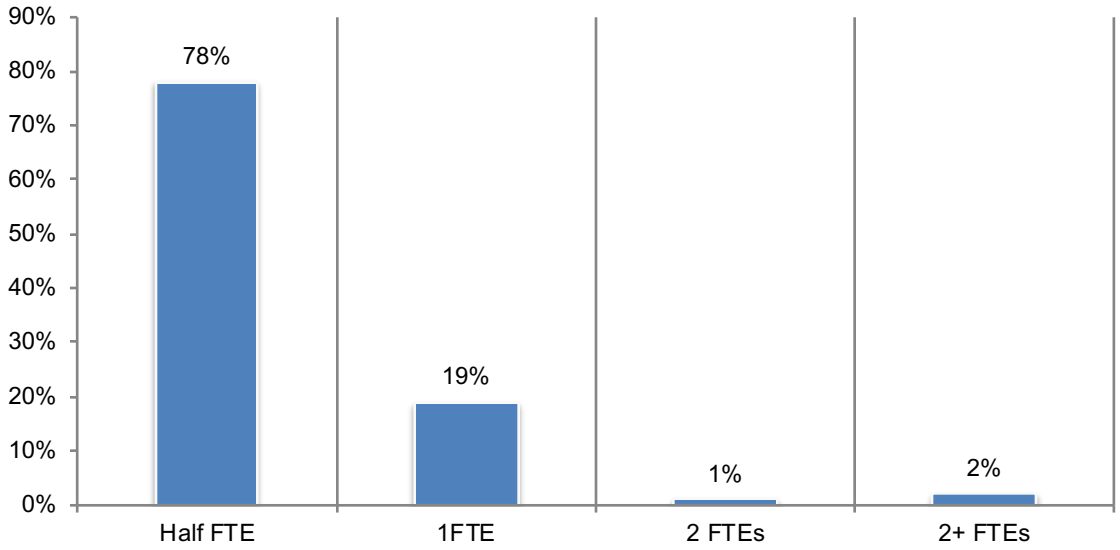
- Operational costs and potential savings
- How companies are deploying QRadar
- Perceptions about QRadar Solutions
- QRadar vs. other SIEM Providers

Operational costs and potential savings

QRadar reduces staffing costs and the use of other point security solutions. On average, organizations represented in this research have 25 employees in security operations dedicated to managing, hunting, investigating and responding to threats. On average, approximately 40 percent of the IT security staff is engaged in proactive security activities. Most organizations represented in this study (75 percent) have between one and two full-time individuals allocated to managing the QRadar solutions. Only 12 percent have more than two full-time employees dedicated to QRadar solutions.

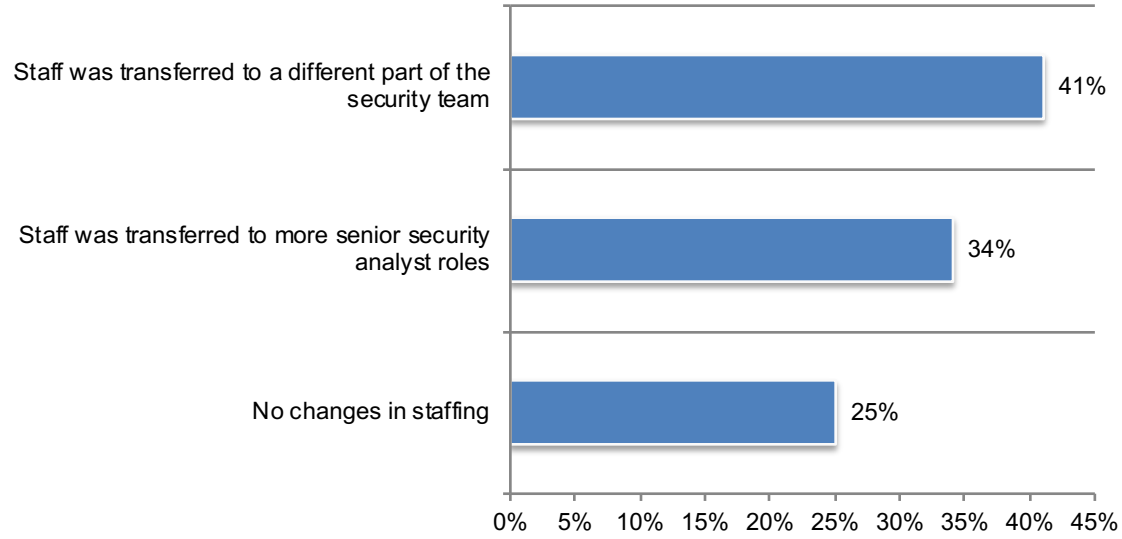
Forty-four percent of respondents say QRadar security intelligence helped to reduce the headcount associated with daily security incident investigations. As shown in Figure 1, 78 percent of respondents say they were able to reduce the headcount associated with daily security incident investigations by a half full-time equivalent and 19 percent of respondents say their headcount was reduced by one full-time equivalent.

Figure 1. What headcount reduction did you experience due to the deployment of QRadar Security Intelligence?



Of the 44 percent of respondents who say organizations were able to reduce the headcount associated with daily security incident investigations, 34 percent of respondents say staff was transferred to more senior security analyst roles, as shown in Figure 2.

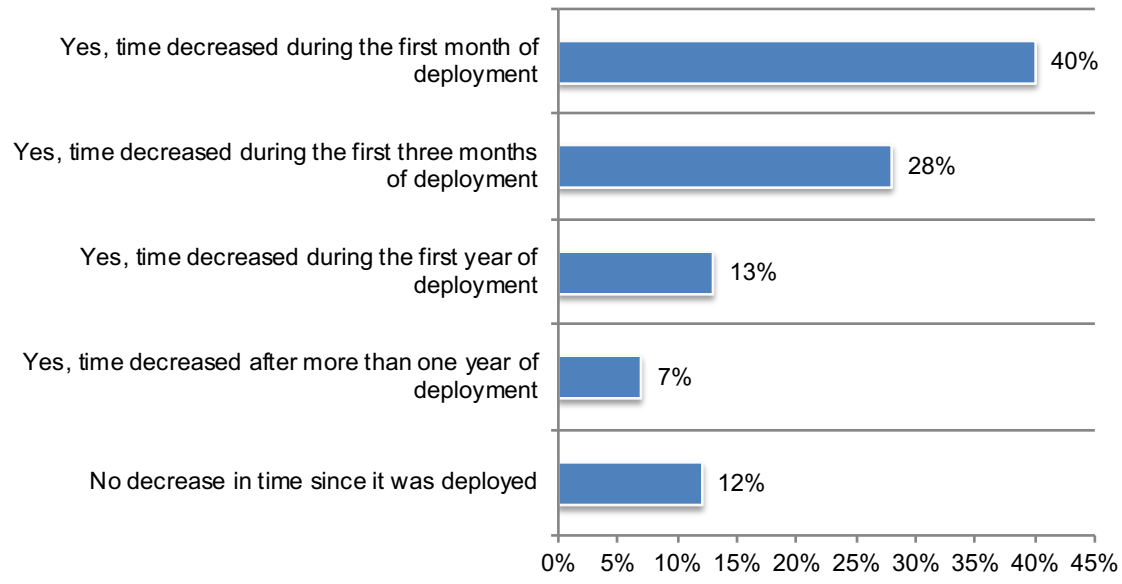
Figure 2. How has reduction impacted staffing of their organization's security team?



T**he amount of time invested in tuning QRadar decreases following deployment.** When asked to rate the difficulty in fine-tuning QRadar on a scale from 1 = not difficult at all to 10 = very difficult, only 37 percent of respondents say it is very difficult to fine-tune QRadar (7+ responses on the 10-point scale). 63 percent of respondents say it average to very easy to fine-tune QRadar.

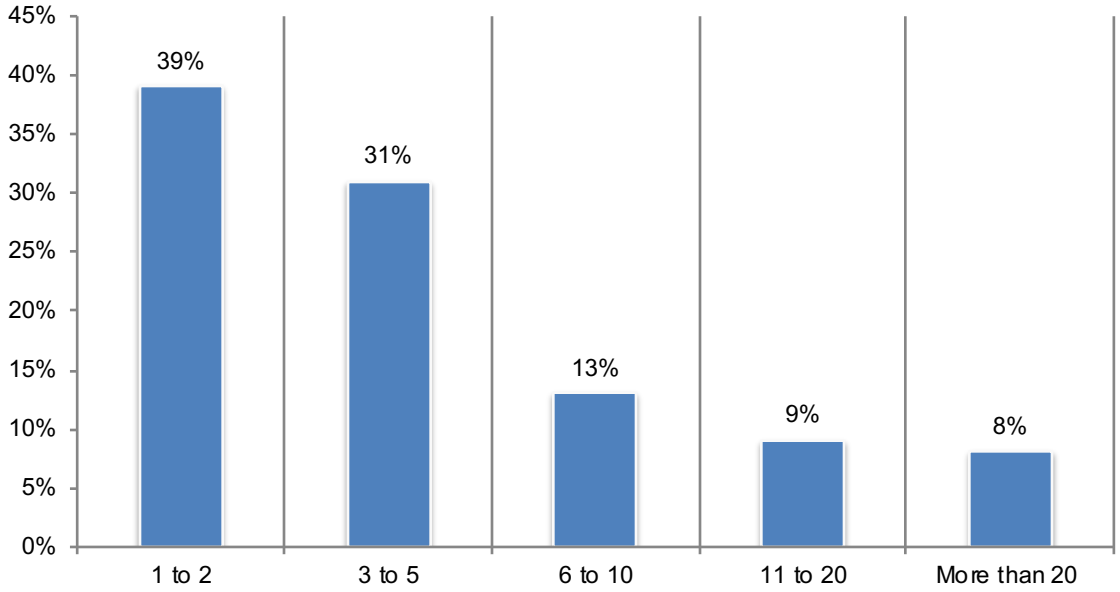
As shown in Figure 3, 40 percent of respondents say the time to tune QRadar decreased during the first month of deployment. Only 12 percent of respondents say there was no decrease in time since deployment.

Figure 3. Has the amount of time invested in tuning QRadar decreased since it was deployed?



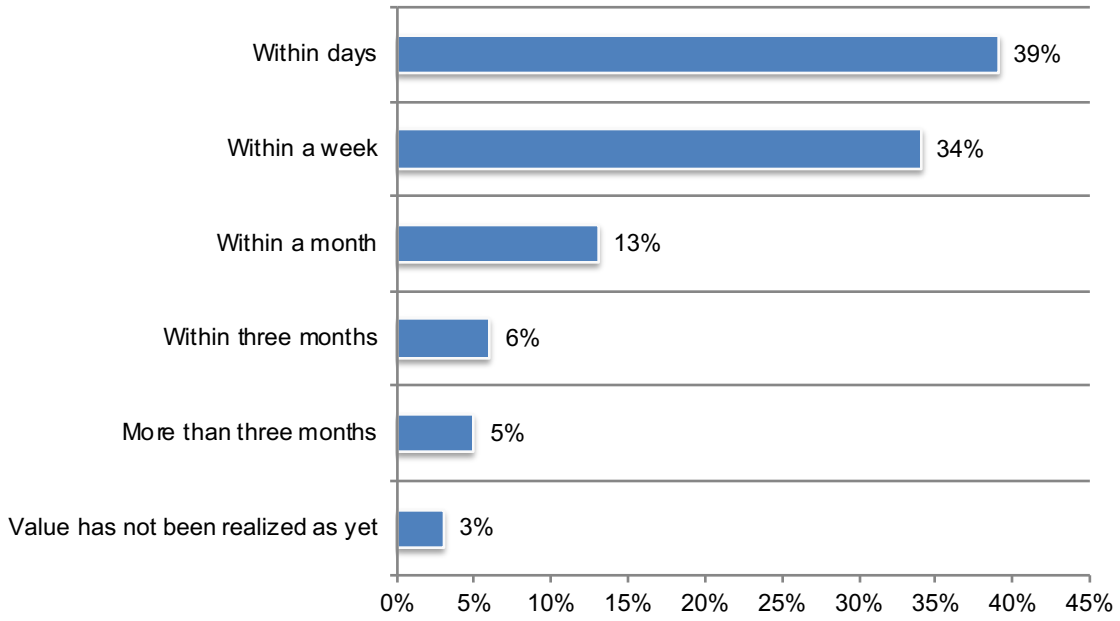
Fifty percent of respondents say their organizations were able to replace point security solution products. As shown in Figure 4, 61 percent of respondents say they have replaced more than three point solutions.

Figure 4. How many point solutions were replaced?
Extrapolated average = 5.87



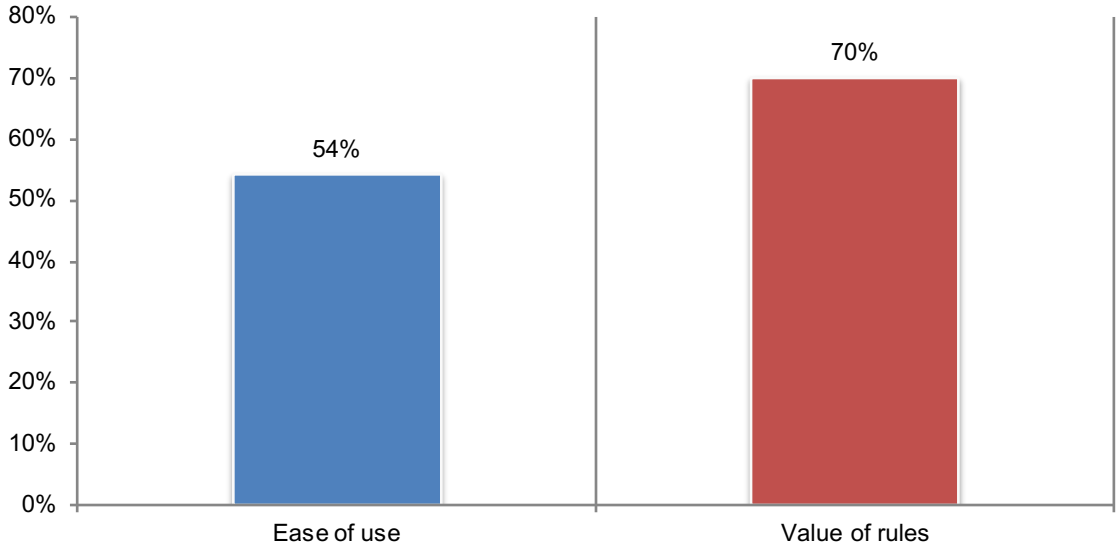
Customers benefit from QRadar within days or a week. Figure 5 shows the length of time it took organizations to recognize value from the QRadar deployment. Most respondents (73 percent) say their organizations recognized the value of QRadar within days (39 percent) or within a week (34 percent).

Figure 5. How long did it take your organization to recognize value from the QRadar deployment?



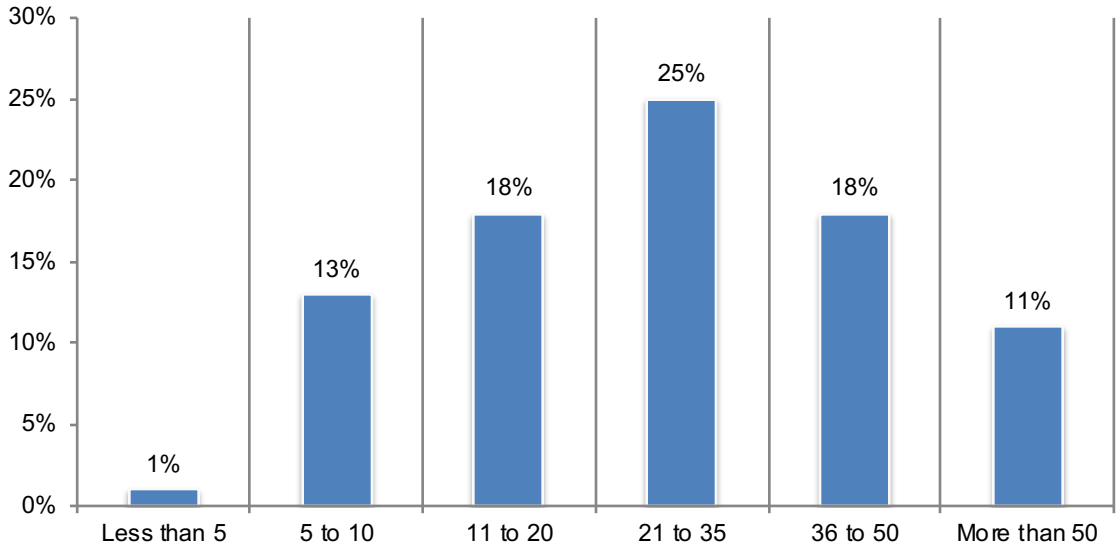
Out-of-box QRadar correlation rules are considered very valuable and most say bringing logs into QRadar for correlation and analysis is very easy. Respondents were asked to rate how easy it was to start bringing logs into QRadar for correlation and analysis and the value of out-of-box QRadar correlation rules on a scale of 1 = not easy/not valuable to 10 = very easy/very valuable. As shown in Figure 6, 54 percent of respondents say it is very easy to bring logs into QRadar for correlation and analysis and 70 percent of respondents say out-of-box QRadar correlation rules are very valuable. According to the research, an average of 34 custom correlation rules have been created.

Figure 6. Ease of bringing logs for correlation and analysis and value of out-of-box QRadar correlation rules 7+ responses on a scale of 1 = not easy/not valuable to 10 = very easy/very valuable



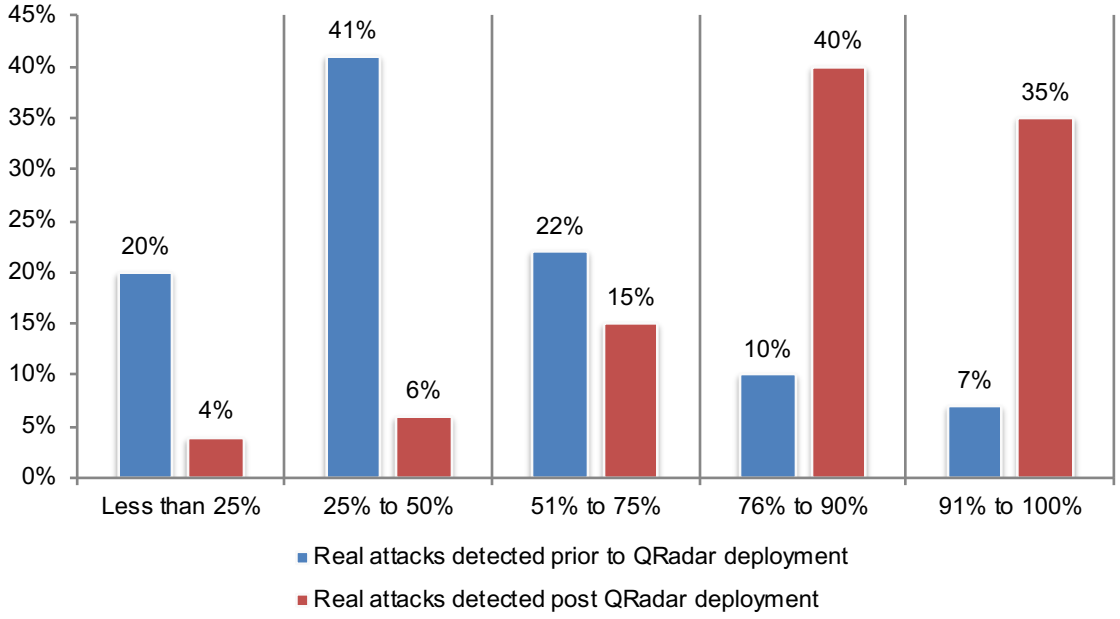
According to Figure 7, respondents see an average of 24 QRadar offenses on a daily basis. Fifty-five percent of respondents say their organizations are able to investigate all the daily offenses generated.

Figure 7. On average, how many QRadar offenses do you see on a daily basis?
Extrapolated average = 24.23 offenses



QRadar increases the ability to accurately detect attacks by 51 percent. According to Figure 8, following the deployment of QRadar the average percentage of real attacks that organizations are able to accurately detect increases from 47 percent to 79. An average of only 15 percent of Offenses in QRadar are false positives.

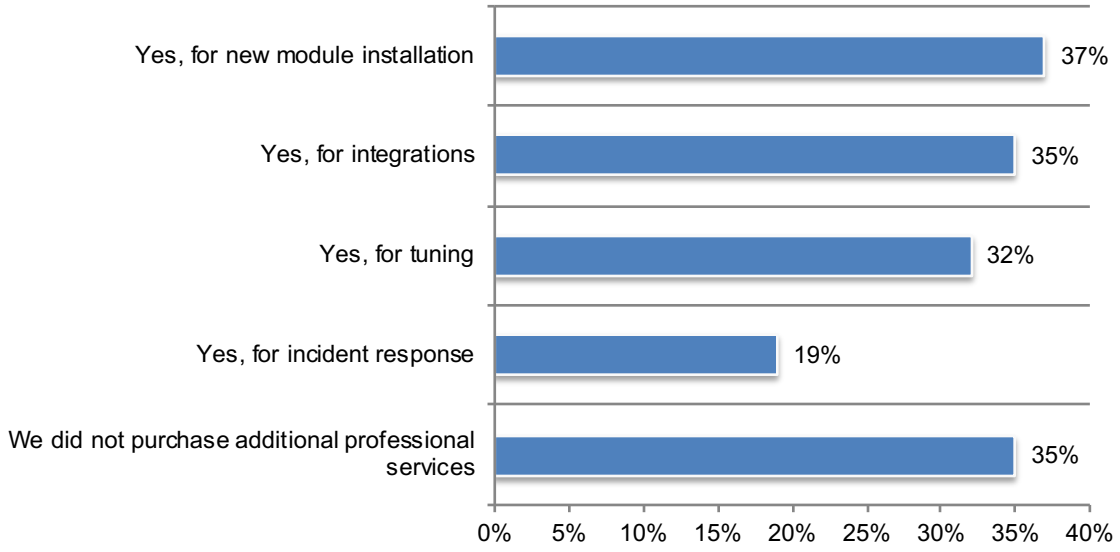
Figure 8. QRadar increases the ability to accurately detect real attacks
Extrapolated averages = 46.61 percent and 78.75 percent



How companies are deploying QRadar

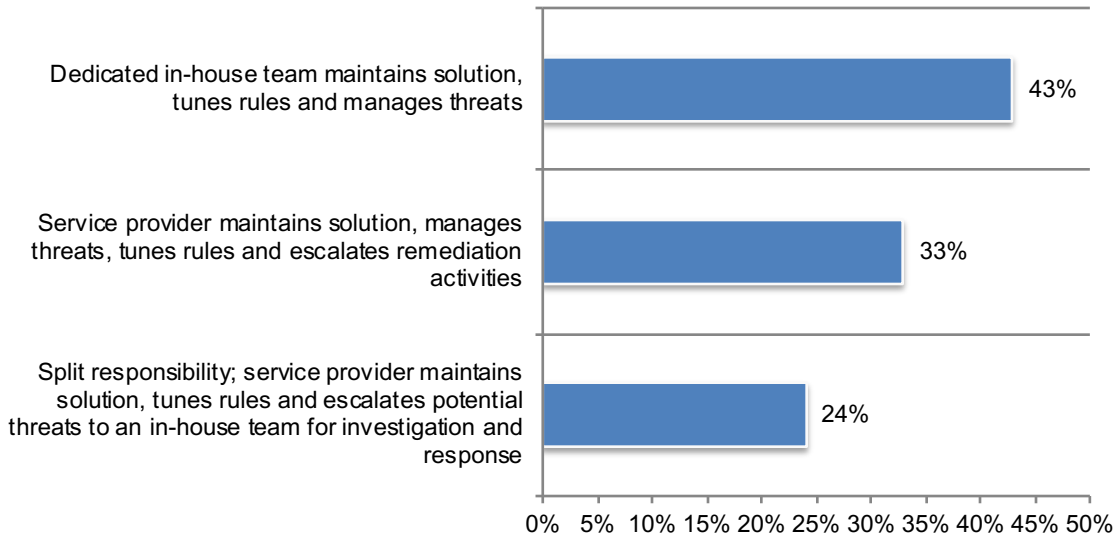
Additional professional services were purchased to assist with QRadar deployment and expansion. 56 percent of respondents purchased professional services to assist with the initial deployment. According to Figure 9, 65 percent of respondents say their organizations purchased additional professional services to assist with QRadar since it was implemented. An average of five days of professional services were purchased primarily for new module installation (37 percent of respondents), integrations (35 percent of respondents) and for tuning (32 percent of respondents).

Figure 9. Have you purchased any additional professional services to help with QRadar since the initial implementation?
More than one response permitted



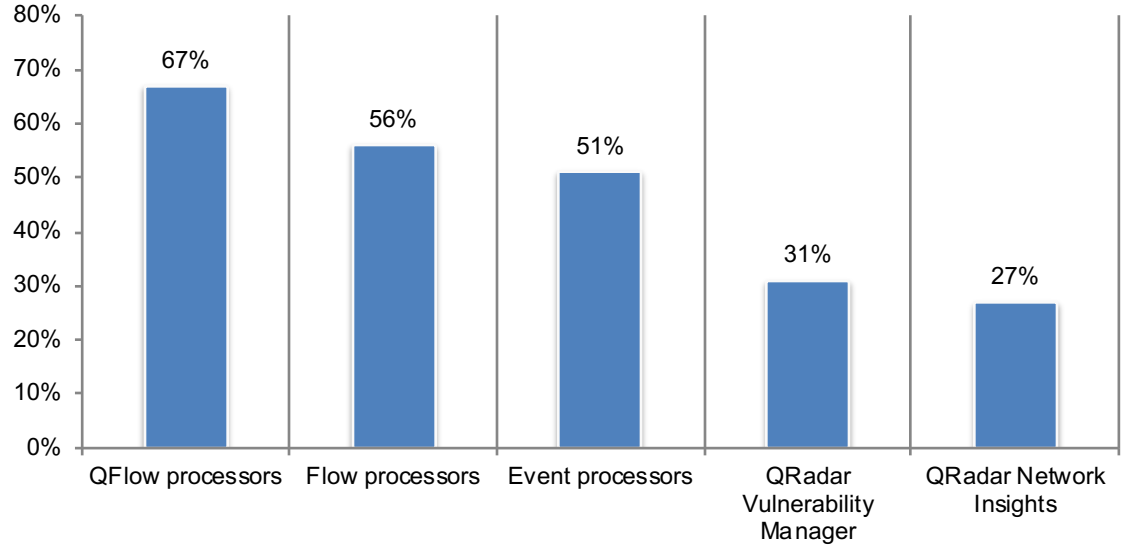
Most organizations have a dedicated in-house team to manage their QRadar solution. As shown in Figure 10, 43 percent of respondents say that their organizations have a dedicated in-house team to maintain the solution, tune rules and manage threats. One-third of respondents say they outsource most QRadar management to a service provider, and 24 percent of respondents say their organization outsources management but maintains an in-house team to investigate and respond to threats.

Figure 10. How do you manage your QRadar solution today?



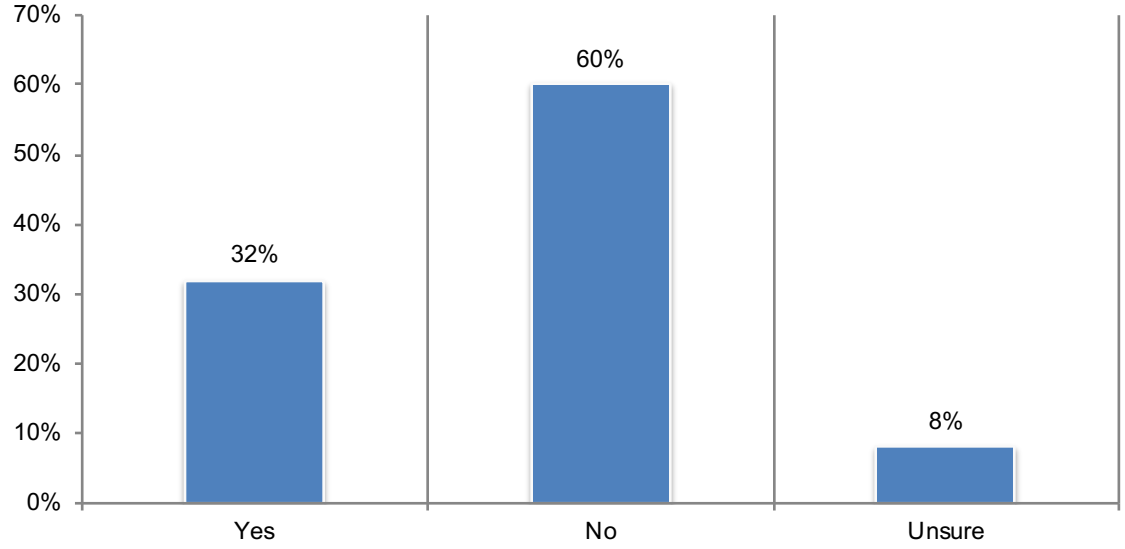
QFlow processors and consoles are the QRadar components most often contained within organizations' security intelligence solution. Figure 11 shows the hardware/software/virtual components contained in their security intelligence solution. Sixty-seven percent of respondents say their organizations use QFlow processors. Many organizations are also using dedicated event and flow processors (51 percent and 56 percent of respondents, respectively).

Figure 11. What QRadar components (hardware/software/virtual) are contained within your security intelligence solution?
More than one response permitted



Licensing for QRadar event & flow processors. According to Figure 12, 60 percent of respondents say they did not have to upgrade their log source license capabilities to accommodate growth. An average of 3,900 log events per second and 6,140 flows per minute are permitted by organizations' licenses.

Figure 12. Have you ever had to upgrade your log source or network flow license capabilities to accommodate growth?

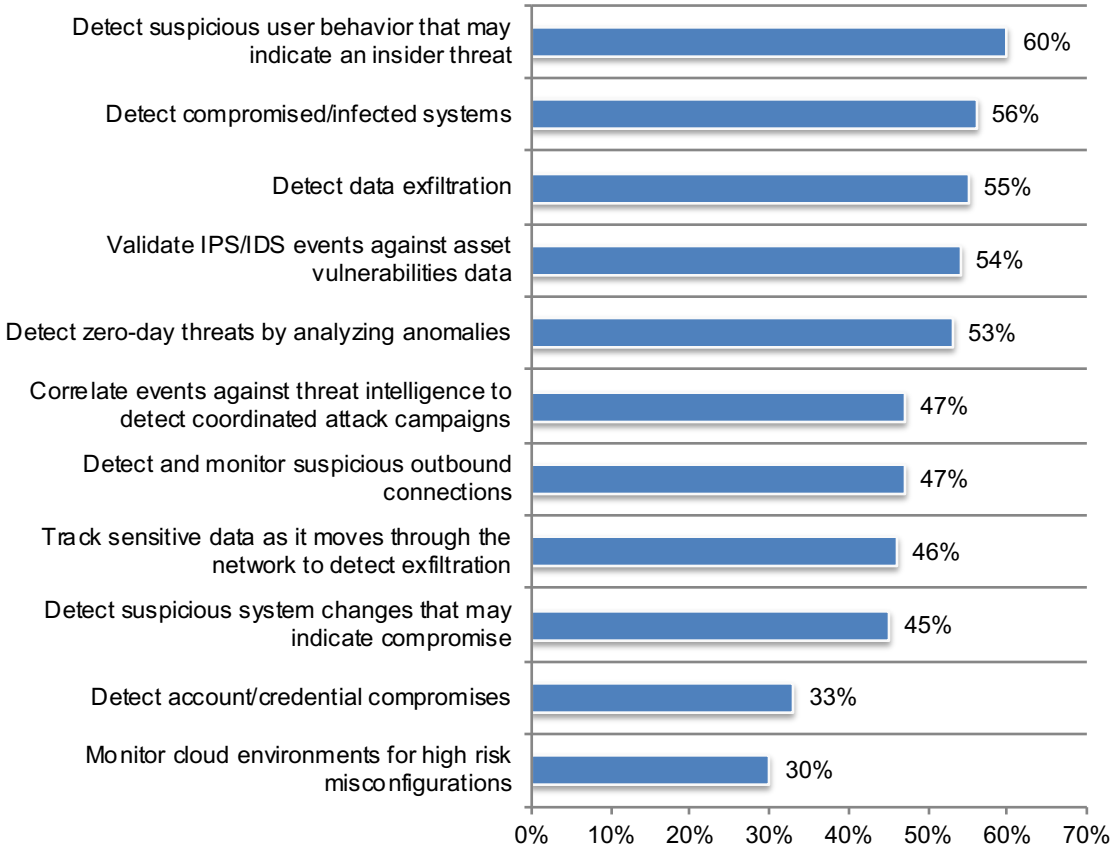


Perceptions about QRadar solutions

QRadar purchasing decisions. Sixty-one percent of respondents say their companies conducted proof of technology or proof of concept trials with competitive solutions. Most often considered in the evaluation were ArcSight (43 percent), Splunk (45 percent) and RSA (27 percent).

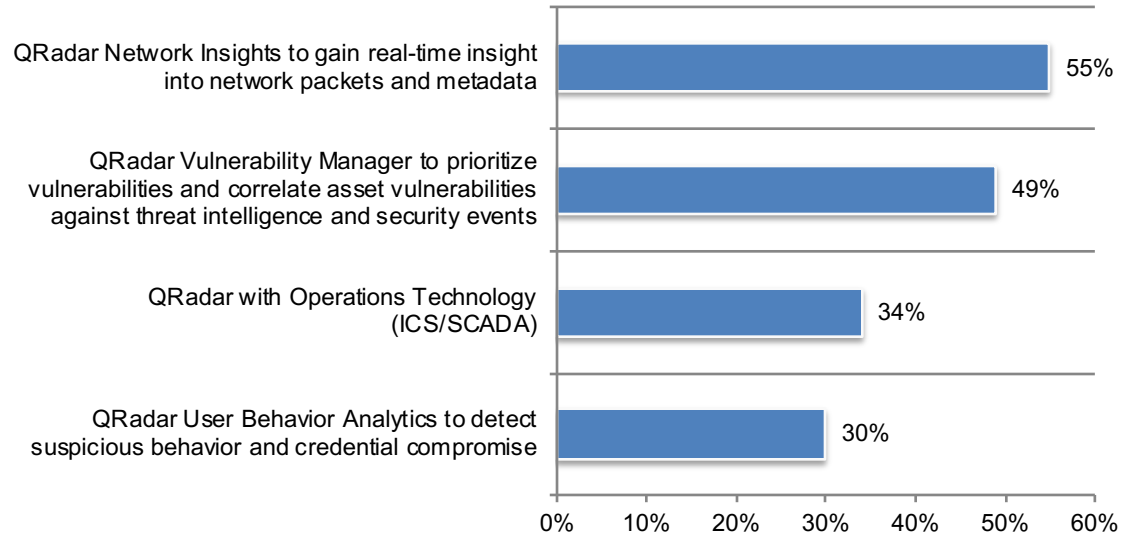
According to Figure 13, the most important use cases in the evaluation and purchase of QRadar were the ability to: detect threats or suspicious changes in behavior (60 percent of respondents), detect compromised/infected systems (56 percent of respondents), detect data exfiltration (55 percent of respondents, validate IPS/IDS events against asset vulnerabilities data (54 percent of respondents) and detect zero-day threats by analyzing anomalies (53 percent of respondents).

Figure 13. What use cases were most important to the evaluation and purchase of QRadar?
More than one response permitted



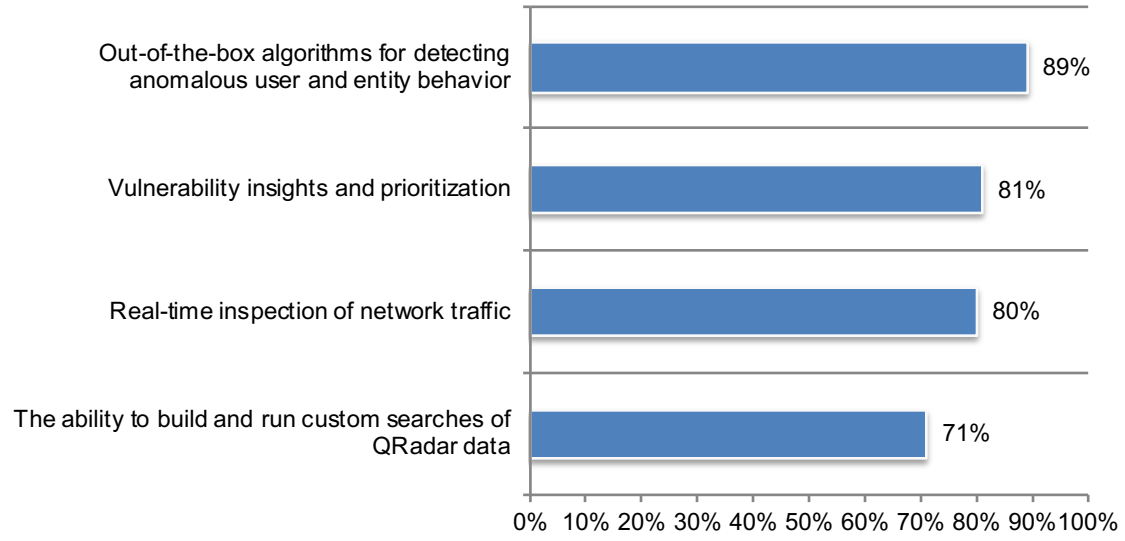
QRadar Network Insights is the add-on solution most often used. According to Figure 14, 55 percent of respondents say their organizations use QRadar Network Insights to gain real-time insight into network packets and metadata and 49 percent use QRadar Vulnerability Manager to prioritize vulnerabilities and correlate asset vulnerabilities against threat intelligence and security events.

Figure 14. The QRadar solutions organizations use
Yes responses presented



Organizations find QRadar features to be very valuable. Respondents were asked to rate QRadar features on a scale from 1 = not valuable at all to 10 = very valuable. Figure 15 shows the very valuable responses (7+ responses on the scale of 1 to 10) for four QRadar features. Respondents give these features very high marks, especially out-of-the-box algorithms for detecting anomalous user and entity behavior.

Figure 15. Value of QRadar solutions
1 = not valuable at all to 10 = very valuable, 7+ responses presented

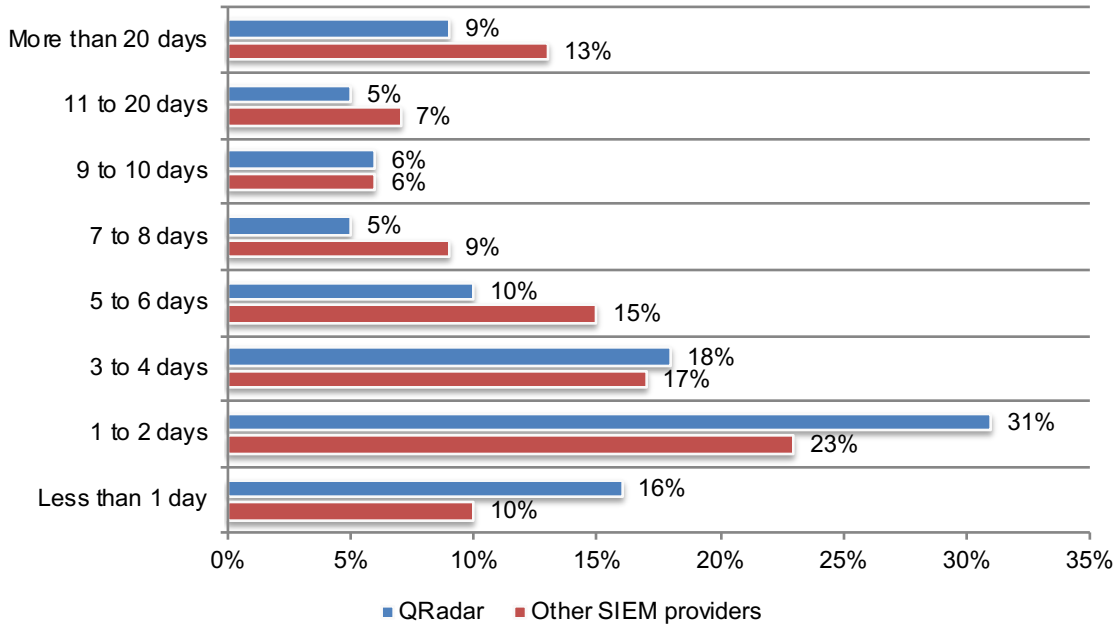


IBM QRadar vs. Other SIEM Providers

As part of this research, we surveyed 479 IT and IT security practitioners whose organizations use other SIEM products. In this section, we compare the responses of IBM QRadar customers to customers of other SIEM providers.

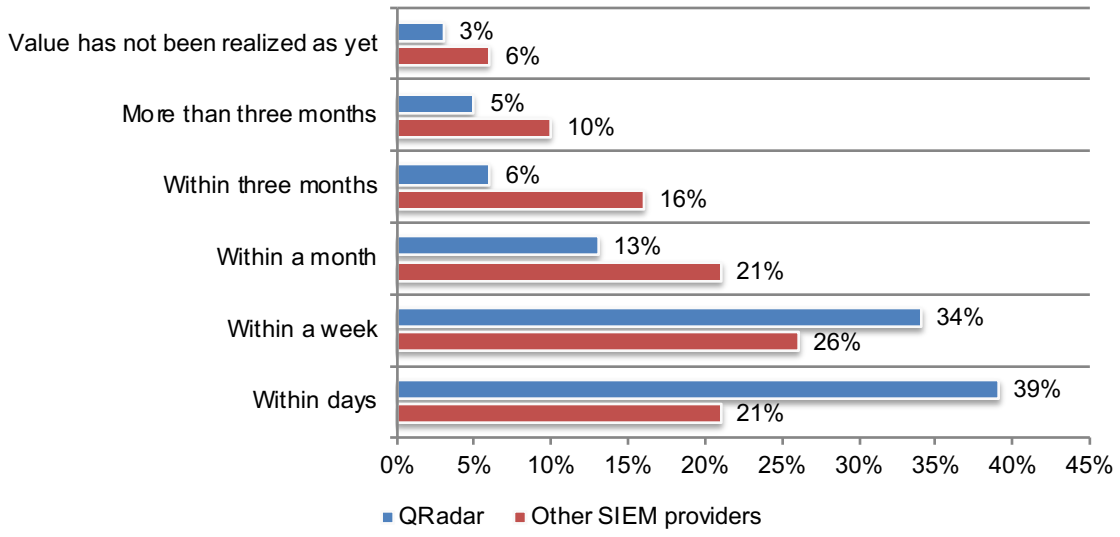
Organizations using other SIEM solutions purchased more days of professional services. According to Figure 16, QRadar customers purchased approximately 5 days of professional service and customers of other solutions purchased an average of 7 days.

Figure 16. How many days of professional services did you purchase with the initial deployment?
Extrapolated averages = 5.49 days and 7.05 days



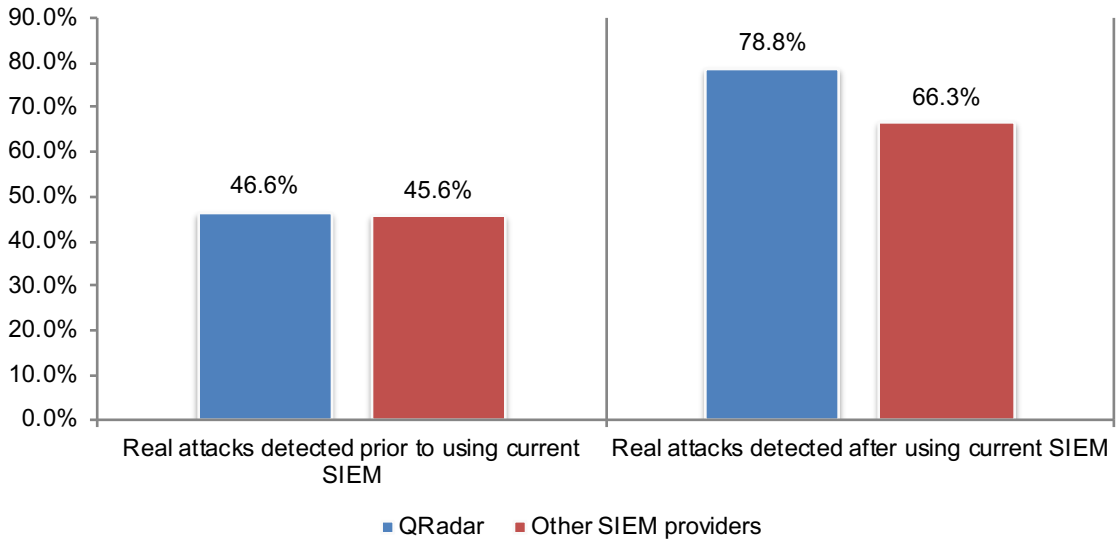
QRadar customers realize its value faster than customers deploying other SIEM solutions. According to Figure 17, 73 percent of QRadar respondents recognized its value within days (39 percent) or within a week (34 percent). In contrast, 47 percent of respondents of other solutions realized its value in the same timeframe.

Figure 17. How long did it take your organization to recognize value from the SIEM deployment?



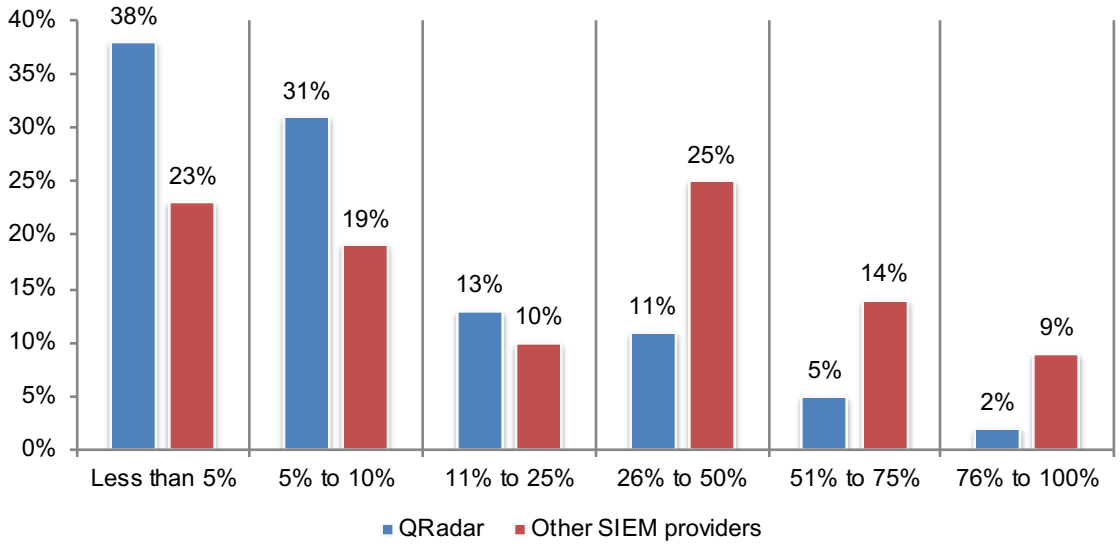
QRadar is better at enabling users to more accurately detect real attacks. According to Figure 18, the differences in the ability to accurately detect real attacks following deployment of the solution are significant. Following deployment of QRadar, the average percentage of attacks detected increased from approximately 47 percent to 79 percent. Other SIEM respondents say detection improved from an average of approximately 46 percent to 66 percent.

Figure 18. Ability to accurately detect real attacks
Extrapolated values presented



QRadar is more effective in reducing false positives. According to Figure 19, an average of only 15 percent of Offenses are false positives. However, with other providers an average of 30 percent are false positives.

Figure 19. On average, what percentage of Offenses in your SIEM are false positives?
Extrapolated averages = 14.7 percent and 30 percent



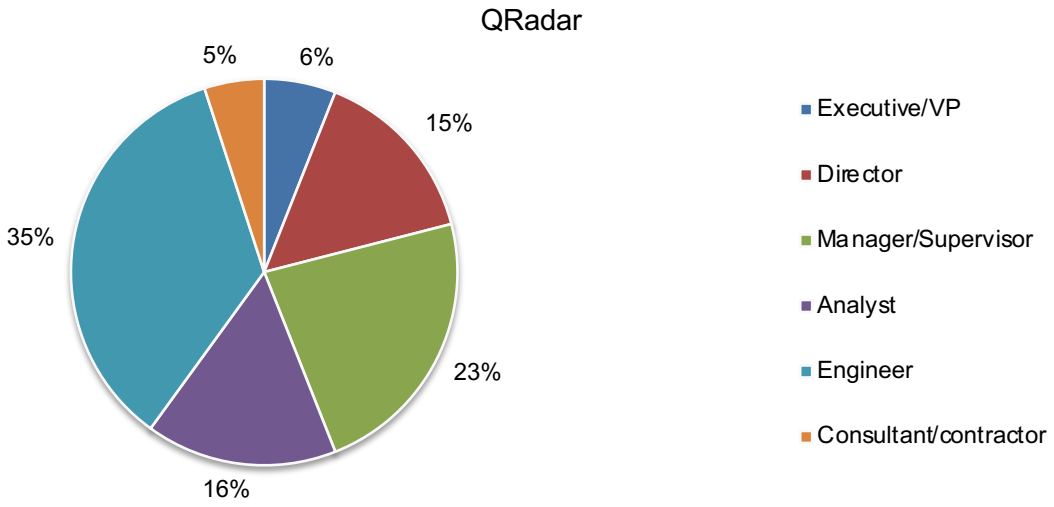
Part 3. Demographics

The sampling frame is composed of 19,650 IT and IT security practitioners in the United States that use QRadar Security Intelligence and 16,881 that use other SIEM providers to monitor and defend their company's network. As shown in Table 1, 323 QRadar respondents and 505 other respondents completed the survey. Screening removed 19 surveys and 26 surveys respectively. The final sample for QRadar users is 304 surveys (or a 1.5 percent response rate) and 470 surveys for other SIEM users (or a 2.8 percent response rate).

Table 1. Sample response	QRadar	Other SIEM providers
Total sampling frame	19,650	16,881
Total returns	323	505
Rejected or screened surveys	19	26
Final sample	304	479
Response rate	1.5%	2.8%

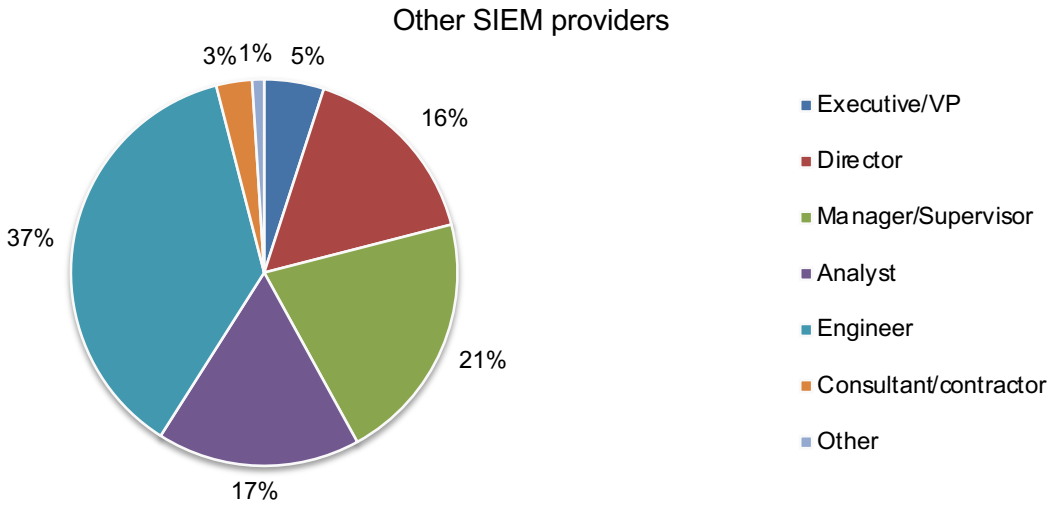
Pie Chart 1a reports the current position or organizational level of the respondents. Thirty-five percent of respondents using QRadar reported their current position level as engineer, 23 percent of respondents reported their current position level is manager/supervisor, 16 percent of respondents are at the analyst level and 15 percent are at the director level.

Pie Chart 1a. Position level within the organization



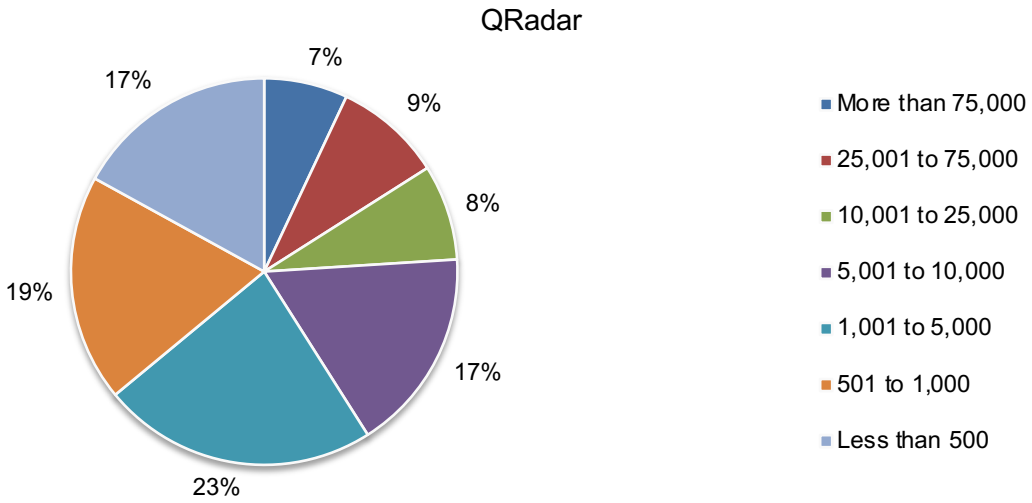
Pie Chart 1b reports the current position or organizational level of respondents using other SIEM providers. Thirty-seven percent of respondents reported their current position level as engineer, 21 percent of respondents reported their current position level is manager/supervisor, 17 percent of respondents are at the analyst level and 16 percent are at the director level.

Pie Chart 1b. Position level within the organization



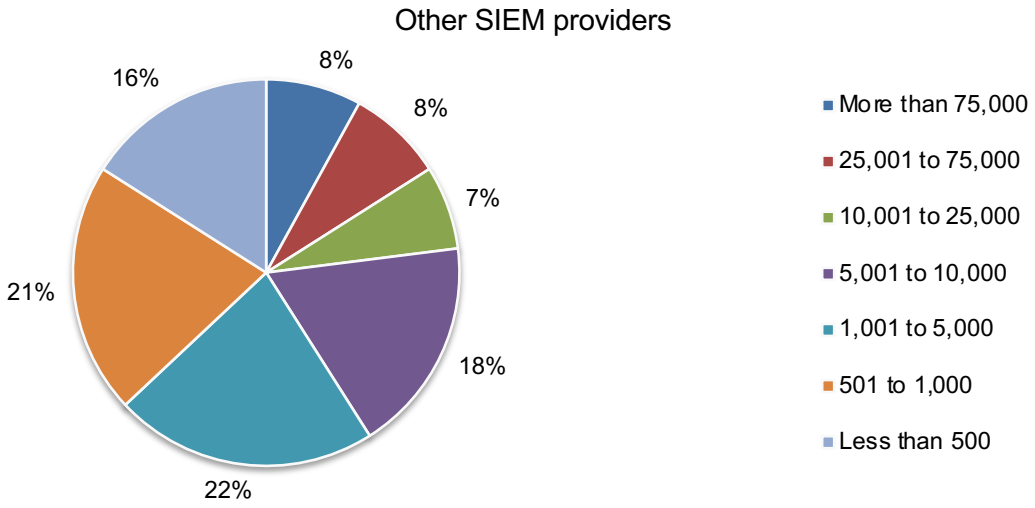
According to Pie Chart 2a, more than half of the QRadar respondents (64 percent) are from organizations with a global head count of more than 1,000 employees, and 36 percent of respondents are from organizations with a global headcount of 1,000 or fewer full-time employees.

Pie Chart 2a. Full-time headcount



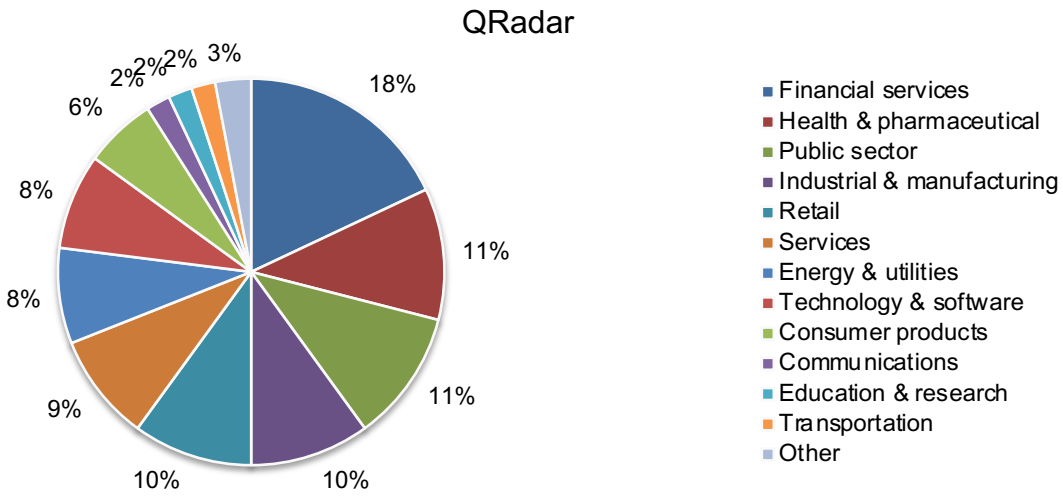
According to Pie Chart 2b, more than half of the respondents (63 percent) in the other SIEM providers sample are from organizations with a global head count of more than 1,000 employees, and 37 percent of respondents are from organizations with a global headcount of 1,000 or fewer full-time employees.

Pie Chart 2b. Full-time headcount



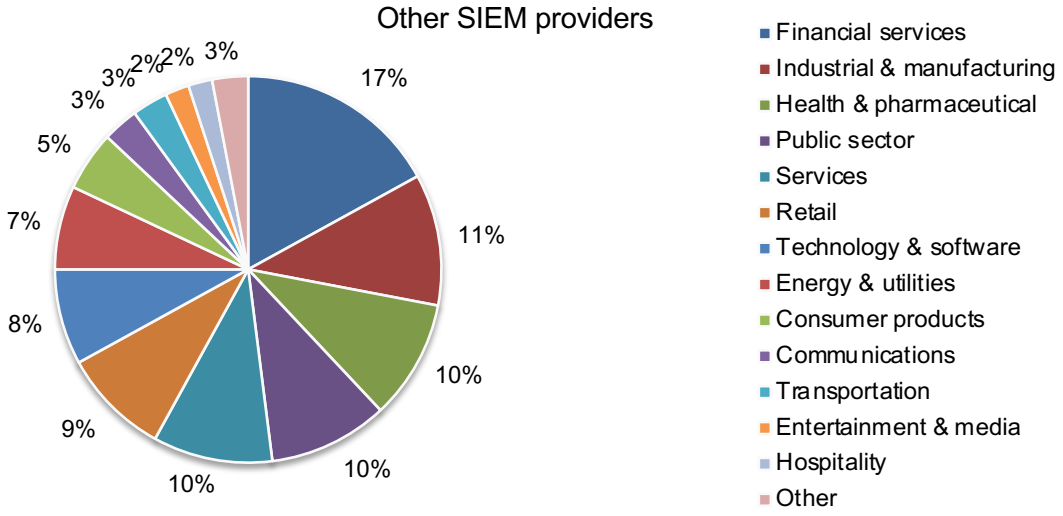
Pie Chart 3a reports the primary industry classification of QRadar respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, followed by health and pharmaceutical (11 percent of respondents), public sector (11 percent of respondents), industrial and manufacturing (10 percent of respondents), retail sector (10 percent of respondents) and services sector (9 percent of respondents).

Pie Chart 3a. The primary industry classification



Pie Chart 3b reports the primary industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by industrial and manufacturing (11 percent of respondents), health and pharmaceutical (10 percent of respondents), public sector (10 percent of respondents), services sector (10 percent of respondents) and retail sector (9 percent of respondents).

Pie Chart 3b. The primary industry classification



Part 4. Caveats

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

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

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners in the United States who use QRadar Security Intelligence to monitor and defend their company's network. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

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 1: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between August 15, 2018 and September 3, 2018.

Survey response	Freq
Total sampling frame	19,650
Total returns (QRadar users)	323
Rejected surveys	19
Final sample	304
Response rate	1.5%

Part 1. Background

Q1. How long has your organization used QRadar to monitor and defend your company's network?	Pct%
Less than 1 year	11%
1 to 2 years	26%
3 to 4 years	39%
5 to 6 years	17%
More than 6 years	7%
Total	100%
Extrapolated value	3.28

Q2. What QRadar release does your organization currently run?	Pct%
v7.2.7 or earlier	6%
v7.2.8	19%
v7.2.9	29%
v7.3.0	27%
v7.3.1	15%
Other	4%
Total	100%

Q3. Do you purchase annual maintenance and support?	Pct%
Yes	59%
No	41%
Total	100%

Q4. How did you purchase the QRadar console?	Pct%
Hardware appliance	19%
Virtual appliance	26%
Software package	38%
SaaS offering (QRadar on Cloud)	17%
Total	100%

Q5. How did you purchase QRadar event and/or flow processors?	Pct%
Hardware appliance(s)	15%
Virtual appliance(s)	16%
Software package(s)	33%
Combination of hardware, software and virtual	21%
Not applicable; use All-in-one appliance	15%
Total	100%

Q6. How many log events per second does your license permit?	Pct%
500	24%
1,000	28%
5,000	24%
10,000	9%
20,000	7%
Other	0%
Not sure	8%
Total	100%
Extrapolated value	3,900

Q7. How many flows per minute does your license permit?	Pct%
100,000	10%
200,000	19%
300,000	24%
600,000	17%
900,000	15%
1,200,000	6%
Not sure	0%
None	9%
Total	100%
Extrapolated value	6,140

Q8. What QRadar components (hardware/software/virtual) are contained within your security intelligence solution? Please select all that apply.	Pct%
Consoles	66%
Event processors	51%
Flow processors	56%
QFlow processors	67%
QRadar Network Insights	27%
QRadar Vulnerability Manager	31%
Total	298%

Q9. Have you ever had to upgrade your log source license capabilities to accommodate growth?	Pct%
Yes	32%
No	60%
Unsure	8%
Total	100%

Q10. How do you manage your QRadar solution today?	Pct%
Dedicated in-house team maintains solution, tunes rules and manages threats	43%
Service provider maintains solution, manages threats, tunes rules and escalates remediation activities	33%
Split responsibility; service provider maintains solution, tunes rules and escalates potential threats to an in-house team for investigation and response	24%
Total	100%

Part 2. Deployment experience

Q11a. Did you purchase any professional services to help you with the initial deployment?	Pct%
Yes	56%
No	44%
Total	100%

Q11b. If yes, how many days of professional services were provided during the initial deployment?	Pct%
Less than 1 day	16%
1 to 2 days	31%
3 to 4 days	18%
5 to 6 days	10%
7 to 8 days	5%
9 to 10 days	6%
11 to 20 days	5%
More than 20 days	9%
Total	100%
Extrapolated value	5.49

Please rate the following statement using the 10-point scale from 1 = not easy at all to 10 = very easy.

Q12. How easy was it to start bringing logs into QRadar for correlation and analysis?	Pct%
1 or 2	12%
3 or 4	9%
5 or 6	25%
7 or 8	28%
9 or 10	26%
Total	100%
Extrapolated value	6.44

Q13. How long did it take your organization to recognize value from the QRadar deployment?	Pct%
Within days	39%
Within a week	34%
Within a month	13%
Within three months	6%
More than three months	5%
Value has not been realized as yet	3%
Total	100%

Part 3. Quality of detection and analytics

Please rate the following statement using the 10-point scale from 1 = not valuable at all to 10 = very valuable.

Q14. How valuable are the out-of-box QRadar correlation rules?	Pct%
1 or 2	6%
3 or 4	3%
5 or 6	21%
7 or 8	34%
9 or 10	36%
Total	100%
Extrapolated value	7.32

Q15. How many custom correlation rules have you developed?	Pct%
None	5%
1 to 10	23%
11 to 25	25%
26 to 50	26%
51 to 100	15%
More than 100	6%
Total	100%
Extrapolated value	34.17

Please rate the following statement using the 10-point scale from 1 = not difficult at all to 10 = very difficult.

Q16. How difficult is it to fine-tune QRadar?	Pct%
1 or 2	13%
3 or 4	19%
5 or 6	31%
7 or 8	21%
9 or 10	16%
Total	100%
Extrapolated value	5.66

Q17. On average, how many QRadar offenses do you see on a daily basis?	Pct%
Less than 5	1%
5 to 10	13%
11 to 20	18%
21 to 35	25%
36 to 50	18%
More than 50	11%
Extrapolated value	24.23

Q18. Are you able to investigate all the daily offenses generated?	Pct%
Yes	55%
No	45%
Total	100%

Q19. Prior to using QRadar, what percentage of real attacks were you able to accurately detect?	Pct%
Less than 25%	20%
25% to 50%	41%
51% to 75%	22%
76% to 90%	10%
91% to 100%	7%
Total	100%
Extrapolated value	46.61

Q20. Following your QRadar deployment, what percentage of real attacks is your organization able to accurately detect?	Pct%
Less than 25%	4%
25% to 50%	6%
51% to 75%	15%
76% to 90%	40%
91% to 100%	35%
Total	100%
Extrapolated value	78.75

Q21a. Did your organization use a competitive solution prior to deployment of QRadar?	Pct%
Yes	53%
No	47%
Total	100%

Q21b. If yes, what percentage of attacks was your organization able to accurately detect?	Pct%
Less than 5%	6%
5% to 10%	7%
11% to 25%	8%
26% to 50%	37%
51% to 75%	30%
76% to 100%	12%
Total	100%
Extrapolated value	45.58%

Q22. On average, what percentage of Offenses in QRadar are false positives?	Pct%
Less than 5%	38%
5% to 10%	31%
11% to 25%	13%
26% to 50%	11%
51% to 75%	5%
76% to 100%	2%
Total	100%
Extrapolated value	14.7%

Please rate the following statement using the 10-point scale from 1 = not valuable at all to 10 = very valuable.

Q23. How valuable is the aggregation of events and flows into single, prioritized Offenses?	Pct%
1 or 2	6%
3 or 4	9%
5 or 6	7%
7 or 8	38%
9 or 10	40%
Total	100%
Extrapolated value	7.44

Please rate the following statement using the 10-point scale from 1 = not valuable at all to 10 = very valuable.

Q24. How valuable is the ability to build and run custom searches of QRadar data?	Pct%
1 or 2	7%
3 or 4	11%
5 or 6	11%
7 or 8	36%
9 or 10	35%
Total	100%
Extrapolated value	7.12

Part 4. Value of QRadar platform solutions

Q25a. Does your organization use QRadar User Behavior Analytics to detect suspicious behavior and credential compromise?	Pct%
Yes	30%
No	70%
Total	100%

If yes, please rate the following statement using the 10-point scale from 1 = not valuable at all to 10 = very valuable.

Q25b. How valuable are the out-of-the-box algorithms for detecting anomalous user and entity behavior?	Pct%
1 or 2	0%
3 or 4	3%
5 or 6	8%
7 or 8	41%
9 or 10	48%
Total	100%
Extrapolated value	8.18

Q26a. Do you use QRadar Network Insights to gain real-time insight into network packets and metadata?	Pct%
Yes	55%
No	45%
Total	100%

If yes, please rate the following statement using the 10-point scale from 1 = not valuable at all to 10 = very valuable.

Q26b. How valuable is real-time inspection of network traffic?	Pct%
1 or 2	5%
3 or 4	5%
5 or 6	10%
7 or 8	35%
9 or 10	45%
Total	100%
Extrapolated value	7.70

Q27a. Do you use QRadar Vulnerability Manager to prioritize vulnerabilities and correlate asset vulnerabilities against threat intelligence and security events?	Pct%
Yes	49%
No	51%
Total	100%

If yes, please rate the following statement using the 10-point scale from 1 = not valuable at all to 10 = very valuable.

Q27b. How valuable are the vulnerability insights and prioritization?	Pct%
1 or 2	0%
3 or 4	3%
5 or 6	16%
7 or 8	33%
9 or 10	48%
Total	100%
Extrapolated value	8.02

Part 5. Post-deployment operational benefits

Q28. Has the amount of time invested in tuning QRadar decreased since it was deployed?	Pct%
Yes, time decreased during the first month of deployment	40%
Yes, time decreased during the first three months of deployment	28%
Yes, time decreased during the first year of deployment	13%
Yes, time decreased after more than one year of deployment	7%
No decrease in time since it was deployed	12%
Total	100%

Q29. How many full or partial headcount are allocated to managing the QRadar solution?	Pct%
Half FTE	13%
1FTE	40%
2 FTEs	35%
2+ FTEs	12%
Total	100%
Extrapolated value	1.53

Q30. How many security operations employees are dedicated to managing, hunting, investigating and responding to threats?	Pct%
1 to 4	8%
5 to 10	16%
11 to 25	36%
26 to 50	31%
50+	9%
Total	100%
Extrapolated value	25.1

Q31a. Did QRadar Security Intelligence help you reduce the headcount associated with daily security incident investigations?	Pct%
Yes	44%
No	56%
Total	100%

Q31b. If yes, how much headcount was reduced?	Pct%
Half FTE	78%
1FTE	19%
2 FTEs	1%
2+ FTEs	2%
Total	100%
Extrapolated value	1.3

Q31c. If yes, how has reduction impacted staffing of your organization's security team?	Pct%
Staff was transferred to more senior security analyst roles	34%
Staff was transferred to a different part of the security team	41%
No changes in staffing	25%
Total	100%

Q32a. Has your organization purchased any additional professional services to assist with QRadar since it was implemented? Please select all that apply.	Pct%
Yes, for tuning	32%
Yes, for new module installation	37%
Yes, for incident response	19%
Yes, for integrations	35%
We did not purchase additional professional services	35%
Total	158%

Q32b. If yes, how many days of professional services were purchased?	Pct%
Less than 1 day	16%
1 to 2 days	28%
3 to 4 days	18%
5 to 6 days	11%
7 to 8 days	9%
9 to 10 days	7%
11 to 20 days	5%
More than 20 days	6%
Total	100%
Extrapolated value	5.23

Q33a. Was your organization able to replace any point security solution products as a result	Pct%
Yes	50%
No	50%
Total	100%

Q33b. If yes, how many point solutions were replaced?	Pct%
1 to 2	39%
3 to 5	31%
6 to 10	13%
11 to 20	9%
More than 20	8%
Total	100%
Extrapolated value	5.87

Part 6. Solution evaluation insight

Q34a. As part of the QRadar initial evaluation, did your organization conduct a proof of technology or proof of concept with competitive solutions?	Pct%
Yes	61%
No	39%
Total	100%

Q34b. If yes, which competitive solutions were considered in the evaluation process? Please select all that apply?	Pct%
ArcSight	43%
Splunk	45%
RSA	27%
McAfee	18%
LogRhythm	21%
Other	8%
Total	162%

Q35. What use cases were most important to the evaluation and purchase of QRadar? Please select all that apply.	Pct%
Detect account/credential compromises	33%
Detect compromised/infected systems	56%
Validate IPS/IDS events against asset vulnerabilities data	54%
Detect and monitor suspicious outbound connections	47%
Detect suspicious system changes that may indicate compromise	45%
Detect suspicious user behavior that may indicate an insider threat	60%
Monitor cloud environments for high risk misconfigurations	30%
Track sensitive data as it moves through the network to detect exfiltration	46%
Detect data exfiltration	55%
Correlate events against threat intelligence to detect coordinated attack campaigns	47%
Detect zero-day threats by analyzing anomalies	53%
Total	526%

Q36. What percentage of your staff is engaged in proactive security activities?	Pct%
Less than 10%	7%
10% to 25%	28%
26% to 50%	35%
51% to 75%	21%
76% to 100%	9%
Total	100%
Extrapolated value	39.6%

Q37. On average, how many attacks does your organization see in a week?	Pct%
Less than 5	4%
5 to 10	13%
11 to 20	16%
21 to 30	23%
31 to 40	18%
41 to 50	12%
51 to 100	9%
More than 100	5%
Total	100%
Extrapolated value	34.07

Q38. How many network breaches did your organization have in the past 12 months?	Pct%
Less than 5	38%
5 to 10	31%
11 to 20	16%
21 to 30	8%
31 to 40	4%
41 to 50	3%
51 to 100	0%
More than 100	0%
Total	100%
Extrapolated value	10.58

Q39. Do you use QRadar with Operations Technology (ICS/SCADA)	Pct%
Yes	34%
No	66%
Total	100%

Q40. Did you acquire QRadar through an IBM Business Partner?	Pct%
Yes	65%
No	35%
Total	100%

Q41. How satisfied is your organization with QRadar solutions?	Pct%
1 or 2	0%
3 or 4	4%
5 or 6	12%
7 or 8	38%
9 or 10	46%
Total	100%
Extrapolated value	8.02

Part 7. Demographics

D1. What best describes your position within the organization?	Pct%
Executive/VP	6%
Director	15%
Manager/Supervisor	23%
Analyst	16%
Engineer	35%
Consultant/contractor	5%
Other	0%
Total	100%

D2. What range best describes the full-time headcount of your global organization?	Pct%
Less than 500	17%
501 to 1,000	19%
1,001 to 5,000	23%
5,001 to 10,000	17%
10,001 to 25,000	8%
25,001 to 75,000	9%
More than 75,000	7%
Total	100%

D3. What best describes your organization's primary industry classification?	Pct%
Communications	2%
Consumer products	6%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	8%
Entertainment & media	1%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	1%
Industrial & manufacturing	10%
Public sector	11%
Retail	10%
Services	9%
Technology & software	8%
Transportation	2%
Other	0%
Total	100%

Appendix 2: Detailed Survey Results

Survey response	Other SIEM providers
Total sampling frame	16,881
Total returns (QRadar users)	505
Rejected surveys	26
Final sample	479
Response rate	2.8%

Part 2. Deployment experience

Q12a. Did you purchase any professional services to help you with the initial SIEM deployment?	Other SIEM providers
Yes	65%
No	35%
Total	100%

Q12b. If yes, how many days of professional services were provided during the initial deployment?	Other SIEM providers
Less than 1 day	10%
1 to 2 days	23%
3 to 4 days	17%
5 to 6 days	15%
7 to 8 days	9%
9 to 10 days	6%
11 to 20 days	7%
More than 20 days	13%
Total	100%
Extrapolated value	7.05

Please rate the following statement using the 10-point scale from 1 = not easy at all to 10 = very easy.

Q13. How easy was it to start bringing logs into the SIEM for correlation and analysis?	Other SIEM providers
1 or 2	4%
3 or 4	7%
5 or 6	16%
7 or 8	36%
9 or 10	37%
Total	100%
Extrapolated value	7.40

Q14. How long did it take your organization to recognize value from the SIEM deployment?	Other SIEM providers
Within days	21%
Within a week	26%
Within a month	21%
Within three months	16%
More than three months	10%
Value has not been realized as yet	6%
Total	100%

Part 3. Quality of detection and analytics

Please rate the following statement using the 10-point scale from 1 = not valuable at all to 10 = very valuable.

Q15. How valuable are the out-of-box SIEM correlation rules?	Other SIEM providers
1 or 2	5%
3 or 4	5%
5 or 6	18%
7 or 8	32%
9 or 10	40%
Total	100%
Extrapolated value	7.44

Q16. How many custom correlation rules have you developed?	Other SIEM providers
None	4%
1 to 10	20%
11 to 25	21%
26 to 50	30%
51 to 100	20%
More than 100	5%
Total	100%
Extrapolated value	37.38

Please rate the following statement using the 10-point scale from 1 = not difficult at all to 10 = very difficult.

Q17. How difficult is it to fine-tune your SIEM?	Other SIEM providers
1 or 2	11%
3 or 4	9%
5 or 6	17%
7 or 8	35%
9 or 10	28%
Total	100%
Extrapolated value	6.70

Q18. On average, how many SIEM offenses do you see on a daily basis?	Other SIEM providers
Less than 5	10%
5 to 10	25%
11 to 20	20%
21 to 35	26%
36 to 50	13%
More than 50	6%
Total	100%
Extrapolated value	21.05

Q19. Are you able to investigate all the daily offenses generated?	Other SIEM providers
Yes	46%
No	54%
Total	100%

Q20. Prior to using your present SIEM, what percentage of real attacks were you able to accurately detect?	Other SIEM providers
Less than 25%	18%
25% to 50%	44%
51% to 75%	26%
76% to 90%	7%
91% to 100%	5%
Total	100%
Extrapolated value	45.6%

Q21. Following your present SIEM deployment, what percentage of real attacks is your organization able to accurately detect?	Other SIEM providers
Less than 25%	11%
25% to 50%	12%
51% to 75%	29%
76% to 90%	28%
91% to 100%	20%
Total	100%
Extrapolated value	66.3%

Q22a. Did your organization use a competitive solution prior to deploying your present SIEM?	Other SIEM providers
Yes	51%
No	49%
Total	100%

Q22b. If yes, what percentage of attacks was your organization able to accurately detect?	Other SIEM providers
Less than 5%	5%
5% to 10%	8%
11% to 25%	8%
26% to 50%	35%
51% to 75%	33%
76% to 100%	11%
Total	100%
Extrapolated value	45.9%

Q23. On average, what percentage of Offenses in your SIEM are false positives?	Other SIEM providers
Less than 5%	23%
5% to 10%	19%
11% to 25%	10%
26% to 50%	25%
51% to 75%	14%
76% to 100%	9%
Total	100%
Extrapolated value	30.0%

Q30. How many full or partial headcount are allocated to managing your present SIEM?	Other SIEM providers
Half FTE	8%
1FTE	27%
2 FTEs	26%
2+ FTEs	39%
Total	100%
Extrapolated value	2.00

Part 7. Demographics

D1. What best describes your position within the organization?	Other SIEM providers
Executive/VP	5%
Director	16%
Manager/Supervisor	21%
Analyst	17%
Engineer	37%
Consultant/contractor	3%
Other	1%
Total	100%

D2. What range best describes the full-time headcount of your global organization?	Other SIEM providers
Less than 500	16%
501 to 1,000	21%
1,001 to 5,000	22%
5,001 to 10,000	18%
10,001 to 25,000	7%
25,001 to 75,000	8%
More than 75,000	8%
Total	100%

D3. What best describes your organization's primary industry classification?	Other SIEM providers
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	1%
Energy & utilities	7%
Entertainment & media	2%
Financial services	17%
Health & pharmaceutical	10%
Hospitality	2%
Industrial & manufacturing	11%
Public sector	10%
Retail	9%
Services	10%
Technology & software	8%
Transportation	3%
Other	1%
Total	100%

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

Ponemon Institute

Advancing Responsible Information Management

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

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