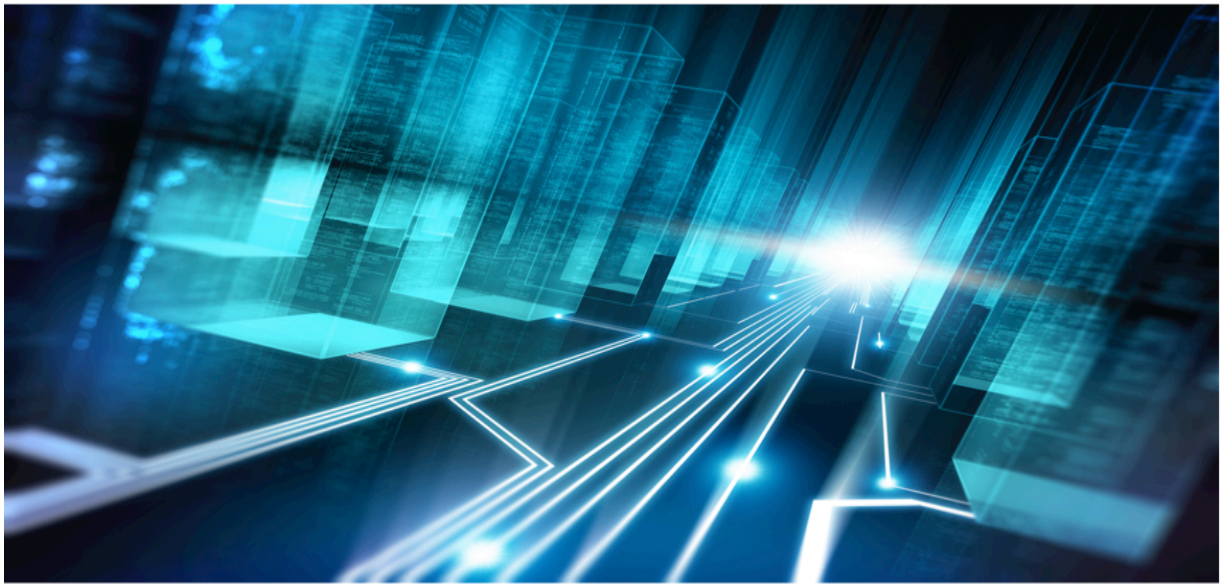


QRadar Security Intelligence Client Study

Sponsored by IBM

Independently conducted by Ponemon Institute LLC

Publication Date: July 2015

QRadar Security Intelligence Client Study

Ponemon Institute, July 2015

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 196 US IT and IT security practitioners in organizations that use QRadar Security Intelligence to monitor and defend their company's network. Topics in this research include the following:

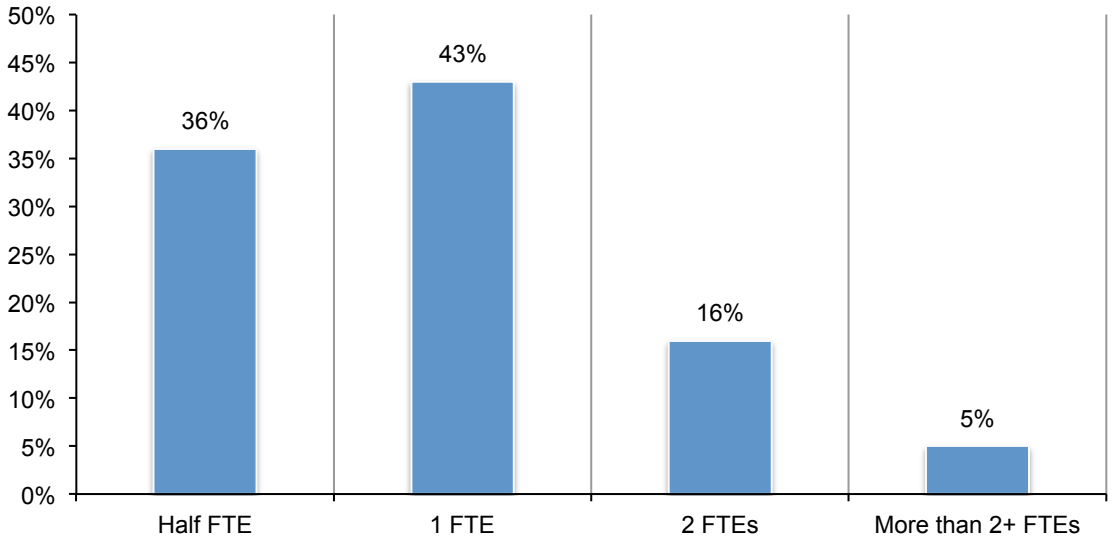
- Operational costs and potential savings
- How companies are deploying QRadar
- Perceptions about QRadar Solutions

Following are the most salient findings from this research:

Operational costs and potential savings

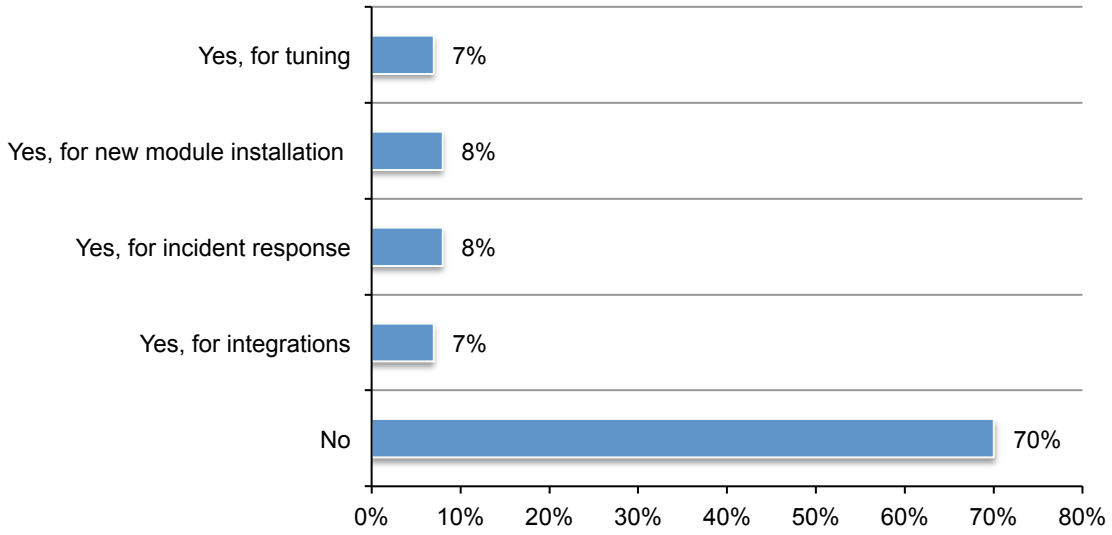
QRadar reduces staffing costs and use of other point security solutions. Most companies (60 percent) have between one and two full-time individuals allocated to security intelligence operations. Only 2 percent have more than two full-time employees dedicated to security intelligence operations. Seventy-nine percent of respondents say they were able to reduce the headcount associated with daily security incident investigations by a half full-time equivalent (36 percent) or one full-time equivalent (43 percent), as shown in Figure 1.

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



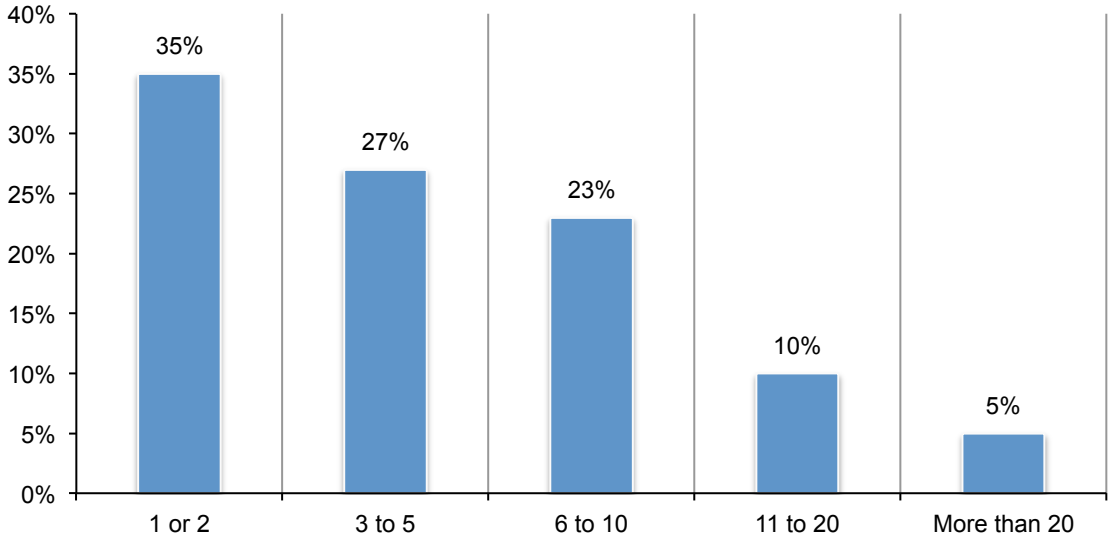
According to Figure 2, 70 percent of respondents say it was not necessary to purchase any additional professional services to help with QRadar since the initial implementation. If they did, on average 2 days were purchased.

Figure 2. Have you purchased any additional professional services to help with QRadar since the initial implementation?



In addition, 62 percent of respondents say they were able to replace point solutions. On average organizations were able to replace six point security solutions as a result of deploying QRadar, as shown in Figure 3.

Figure 3. How many point solutions were replaced?
Extrapolated value = 6.2 point solutions



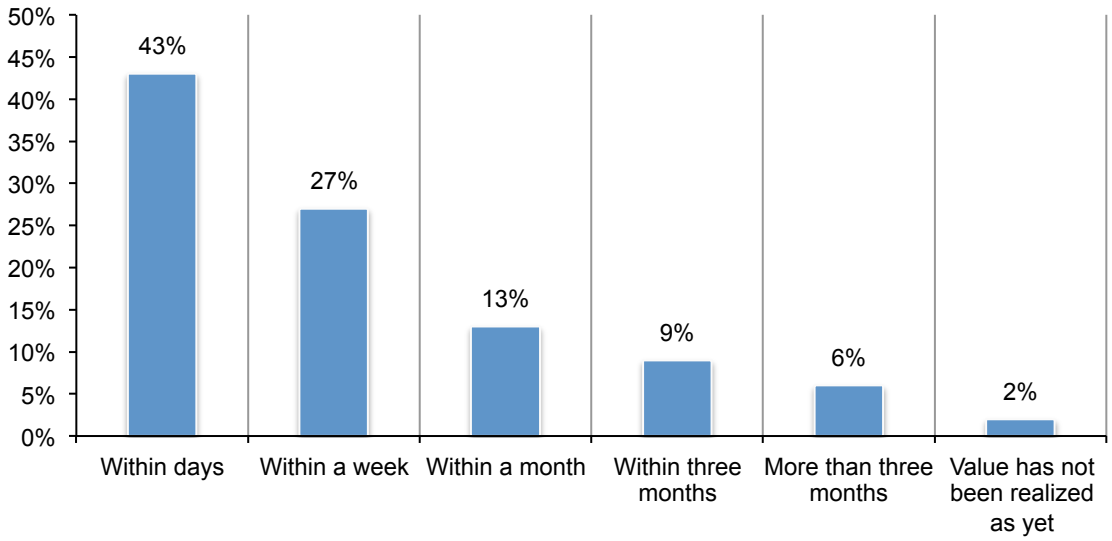
Additional analysis reveals the relationship between the replacement of point solutions and the ability of an organization to reduce costs with a reduction in headcount. As shown in Table 1, the more point solutions replaced the higher the headcount reduction.

Table 1. The impact of point solution replacement on headcount

	How many point solutions were replaced?			
What headcount reduction did you experience?	1 or 2	3 to 5	6 to 10	11 to 20
Half FTE	30%	6%	0%	0%
1 FTE	5%	36%	1%	1%
2 FTEs	0%	2%	12%	2%
More than 2+ FTEs	0%	0%	3%	2%
Total	35%	44%	16%	5%

Forty-three percent of companies represented in this study began recognizing the value from the QRadar deployment within days and 27 percent say it was within a week, as revealed in Figure 4. Only 2 percent say value has not been realized as yet.

Figure 4. How long did it take you to begin recognizing value from the QRadar deployment?



QRadar tuning. Most companies see value in out-of-box correlation rules. As shown in Figure 5, 48 percent of respondents say it is very valuable and 39 percent say it is somewhat valuable. Only 2 percent say it is not very valuable. On average, 29 custom correlation values have been developed.

Figure 5. How valuable are the out-of-box QRadar correlation rules?

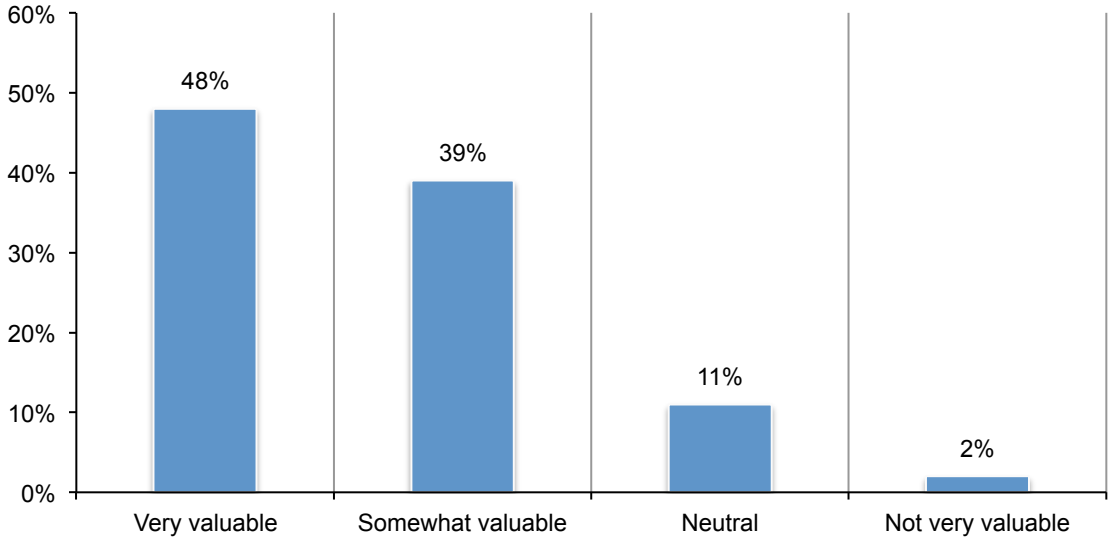
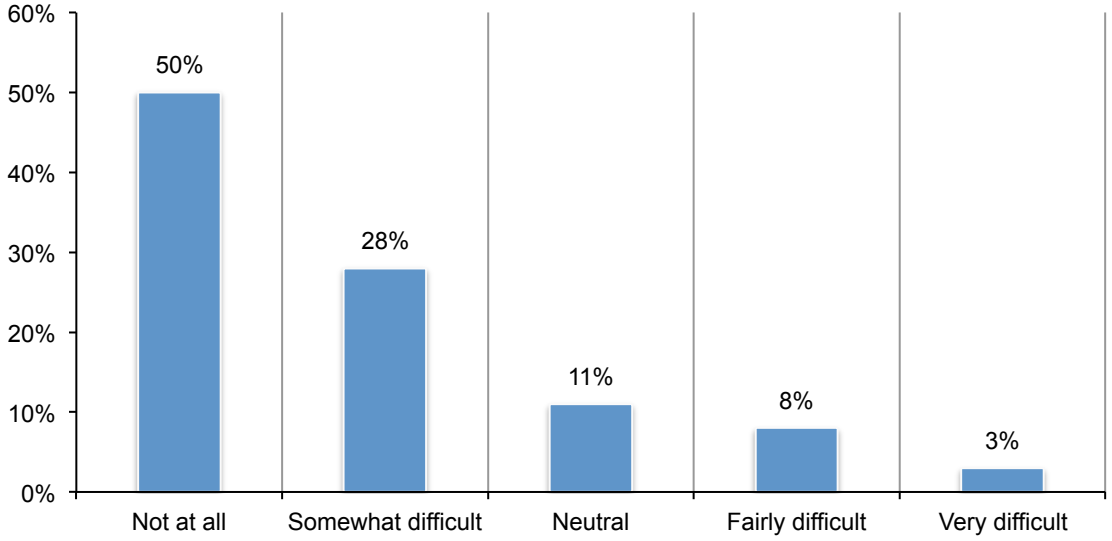


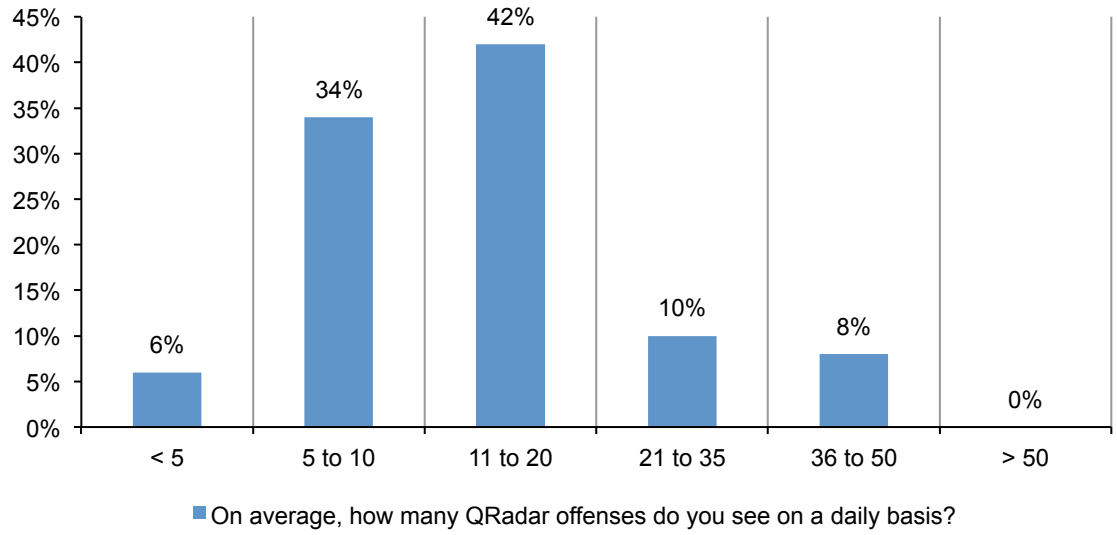
Figure 6 reveals that 50 percent of respondents say it is not at all difficult to fine-tune QRadar and 28 percent say it is somewhat difficult.

Figure 6. Do you consider it difficult to fine-tune QRadar?



According to Figure 7, respondents see an average of 15.4 QRadar offenses on a daily basis. Sixty-four percent say they 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 = 15.4 offenses



On average, respondents say their organizations have developed 29 custom correlation rules. Table 2 shows the relationship between custom correlation rules developed and the QRadar offenses seen on a daily basis. As shown, the more customer correlations the more QRadar offenses shown daily.

Table 2. The relationship between custom correlation rules developed and daily QRadar offenses

	How many custom correlation rules have you developed?					
On average, how many QRadar offenses do you see on a daily basis?	Less than 5	5 to 10	11 to 20	21 to 35	36 to 50	50+
Less than 5	3%	3%	0%	0%	0%	0%
5 to 10	0%	6%	17%	6%	5%	0%
11 to 20	0%	8%	26%	7%	1%	0%
21 to 35	0%	0%	3%	4%	3%	0%
36 to 50	0%	0%	0%	1%	5%	2%
More than 50	0%	0%	0%	0%	0%	0%
Total	3%	17%	46%	18%	14%	2%

How companies are deploying QRadar

According to Figure 8, the majority of respondents (60 percent) of QRadar clients have purchased annual maintenance and support. Only 33 percent of respondents say they purchased professional services to help with initial deployment and on average approximately 3.5 days were needed during the initial deployment.

Figure 8. Did your company purchase annual maintenance & support and professional services to help with initial deployment?

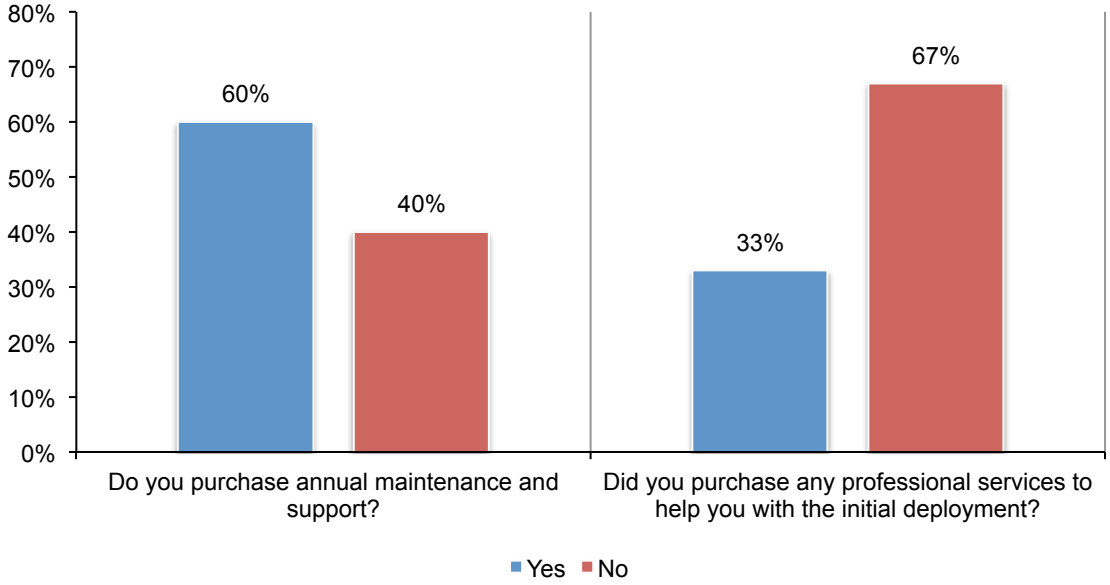
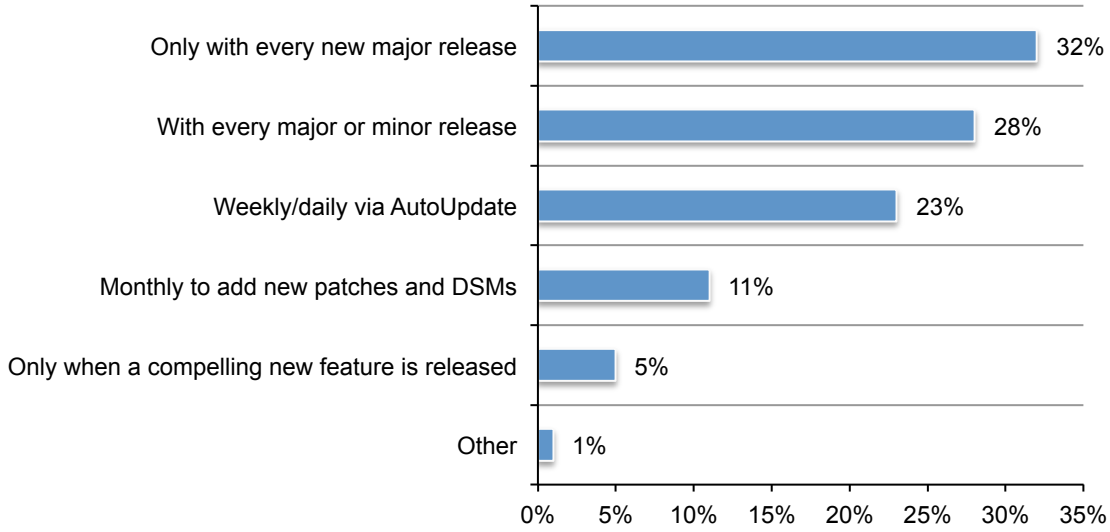


Figure 9 reveals how frequently companies update their QRadar solutions. Most respondents (32 percent) update their QRadar solutions only with every new major release followed by 28 percent of respondents who say they update with every major or minor release and 23 percent of respondents say they use AutoUpdate to update on a weekly or daily basis.

Figure 9. How frequently do you update your QRadar solutions?



As shown in Table 3, companies that purchase annual maintenance and support are more likely to update their QRadar solutions with every major or minor release (24 percent of respondents "yes" response or 10 percent "no" response) or update weekly or daily via AutoUpdate (33 percent of respondents "yes" response vs. 10 percent of respondents "no" response.)

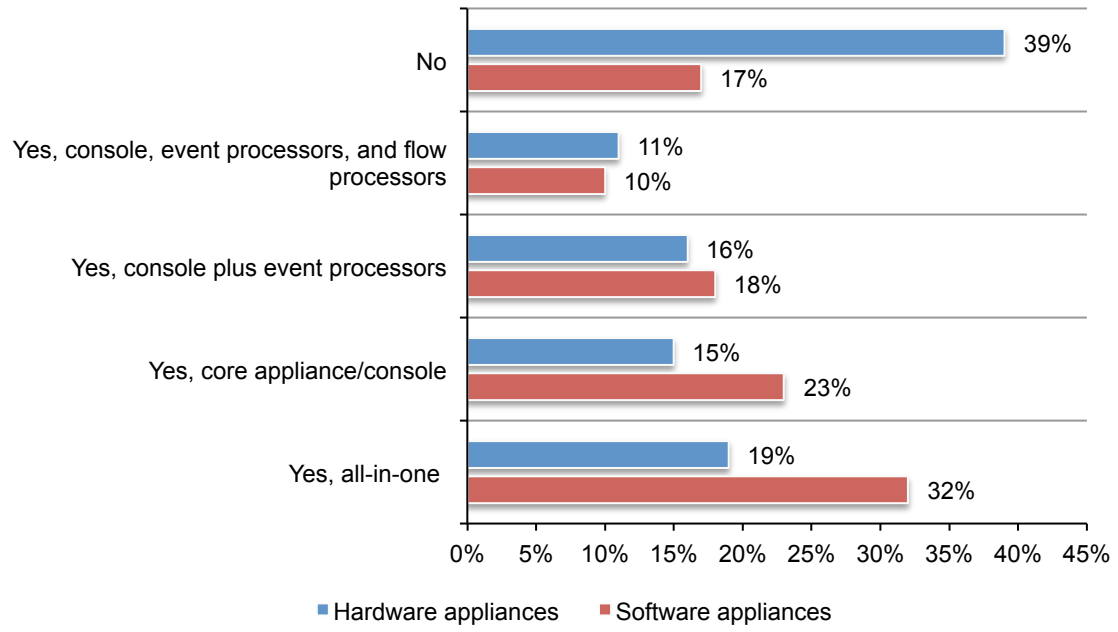
Table 3. If your organization purchases annual maintenance and support, how frequently do you update your QRadar solutions?

	Do you purchase annual maintenance and support?	
How frequently do you update your QRadar solutions?	Yes	No
Only with every new major release	25%	41%
With every major or minor release	24%	10%
Only when a compelling new feature is released	0%	23%
Monthly to add new patches and DSMs	18%	13%
Weekly/daily via AutoUpdate	33%	10%
Other	0%	2%
Total	100%	100%

As shown in Figure 10, 61 percent of respondents say their organizations purchase the following hardware appliances: all-in-one (19 percent), core appliance/console (15 percent), console plus event processors (16 percent) and console, event processors and flow processors (11 percent).

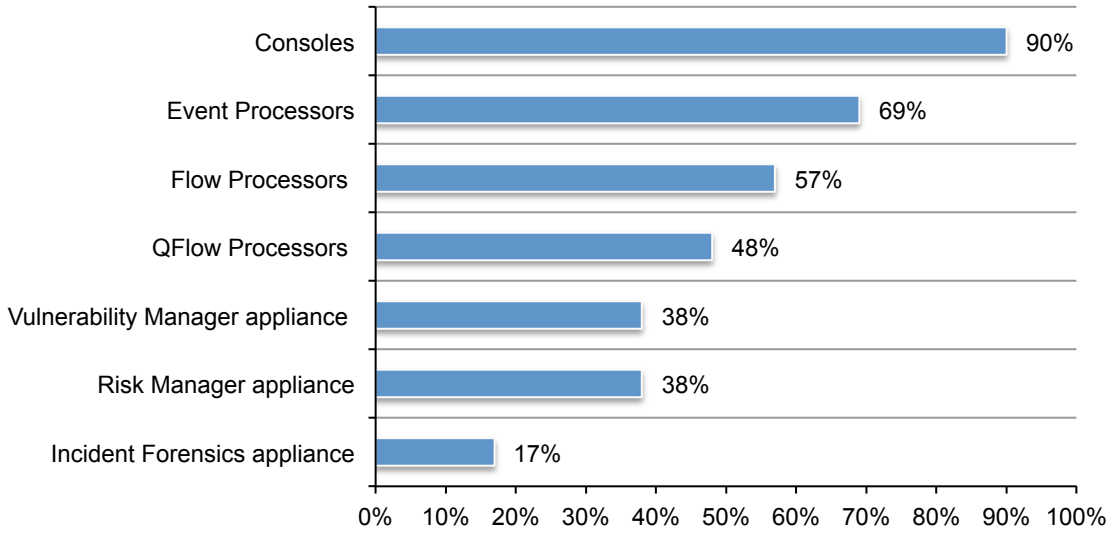
More companies represented in this research (83 percent) purchase software appliances for QRadar. These are: all-in-one (32 percent), core appliance/console (23 percent), console plus event processors (18 percent) and console, event processors and flow processors (10 percent).

Figure 10. Do you purchase any QRadar components as hardware or software appliances?



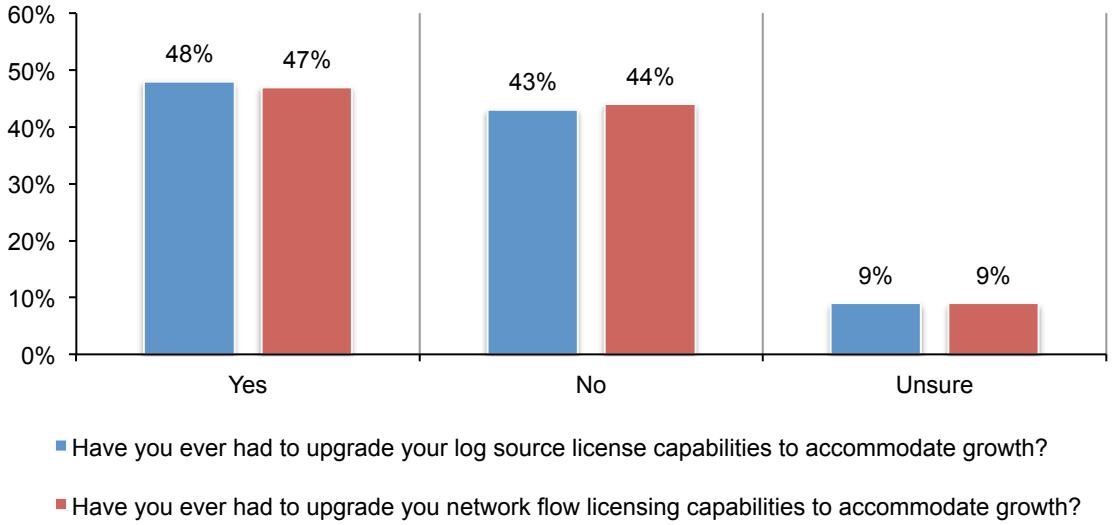
According to Figure 11, most of the appliances contained within the security intelligence solution are consoles (90 percent of respondents), event processors (69 percent of respondents) and flow processors (57 percent of respondents).

Figure 11. What QRadar appliances are contained within your security intelligence solution More than one response permitted



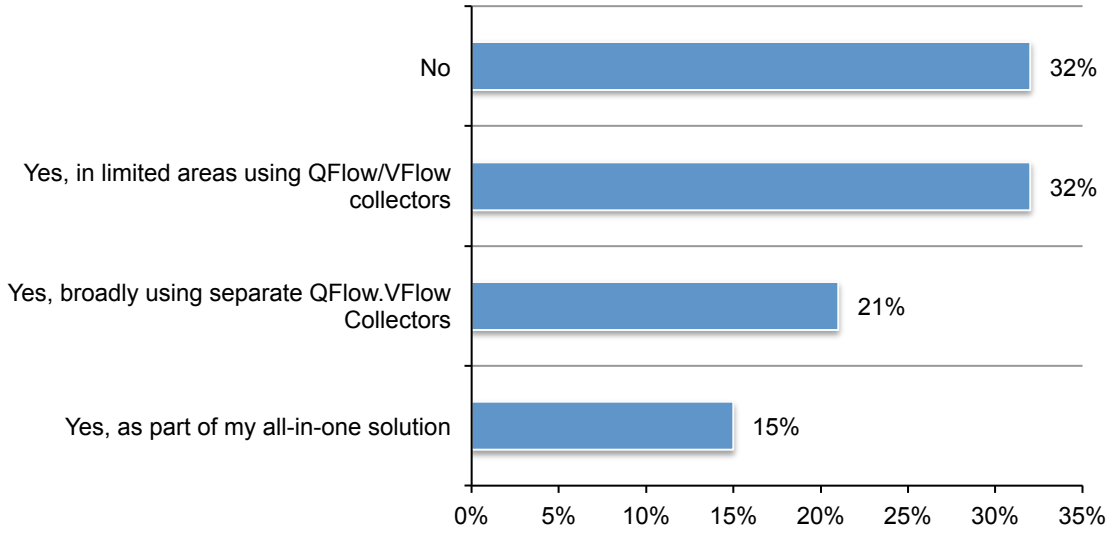
Licensing for QRadar event & flow processors. According to Figure 12, 43 percent of respondents say they did not have to upgrade their log source license capabilities to accommodate growth and 44 percent say they have not had to upgrade their network flow licensing capabilities to accommodate growth. Fifty-two percent of respondents have not had any dropped events due to licensing issues.

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



As shown in Figure 13, 68 percent use QFlow or VFlow Collectors to obtain Layer 7 insights: as part of their all-in-one solutions (15 percent), broadly using separate QFlow/VFlow Collectors (21 percent), in limited areas using QFlow/VFlow Collectors (32 percent).

Figure 13. Do you use QFlow or VFlow Collectors to obtain Layer 7 insights?

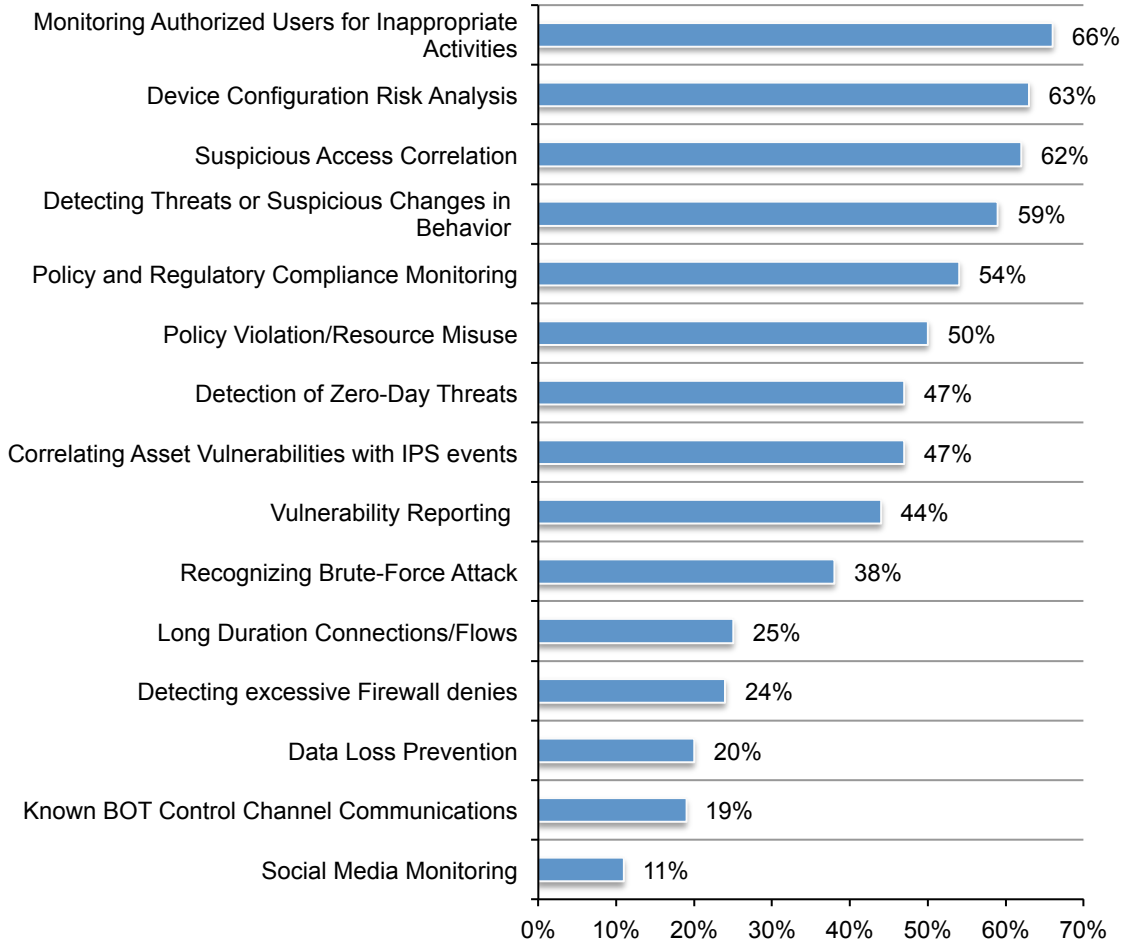


Perceptions about QRadar solutions

QRadar purchasing decisions. Fifty-five 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 (26 percent), Splunk (21 percent) and RSA (17 percent).

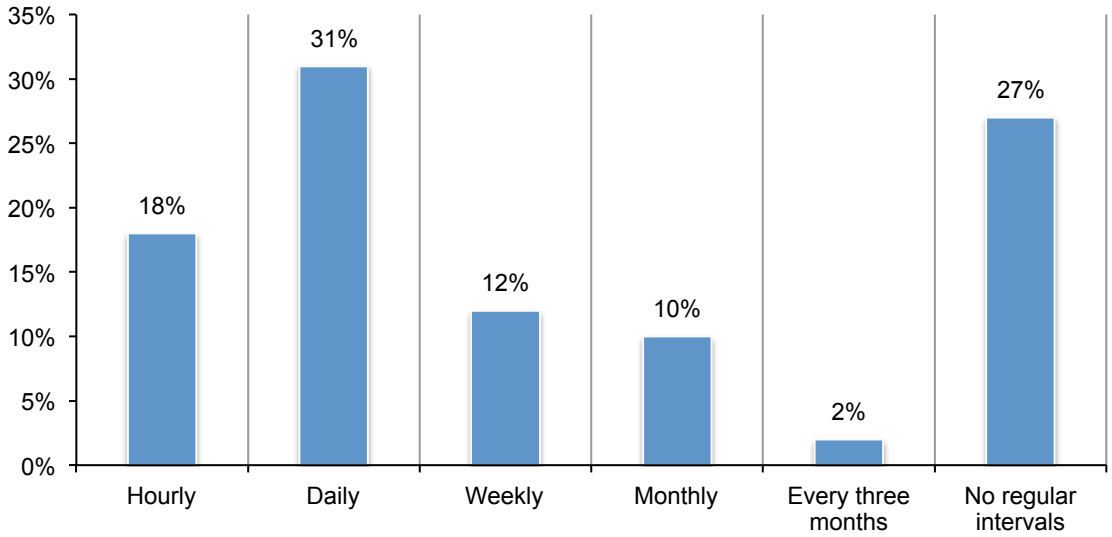
According to Figure 14, the most important use cases in the evaluation and purchase of QRadar were: monitoring authorized users for inappropriate activities (66 percent), device configuration risk analysis (63 percent), suspicious access correlation (62 percent), detecting threats or suspicious changes in behavior (59 percent), policy and regulatory compliance monitoring (54 percent) and policy violation/resource misuse (50 percent).

Figure 14. What use cases were most important to the evaluation and purchase of QRadar? More than one response permitted



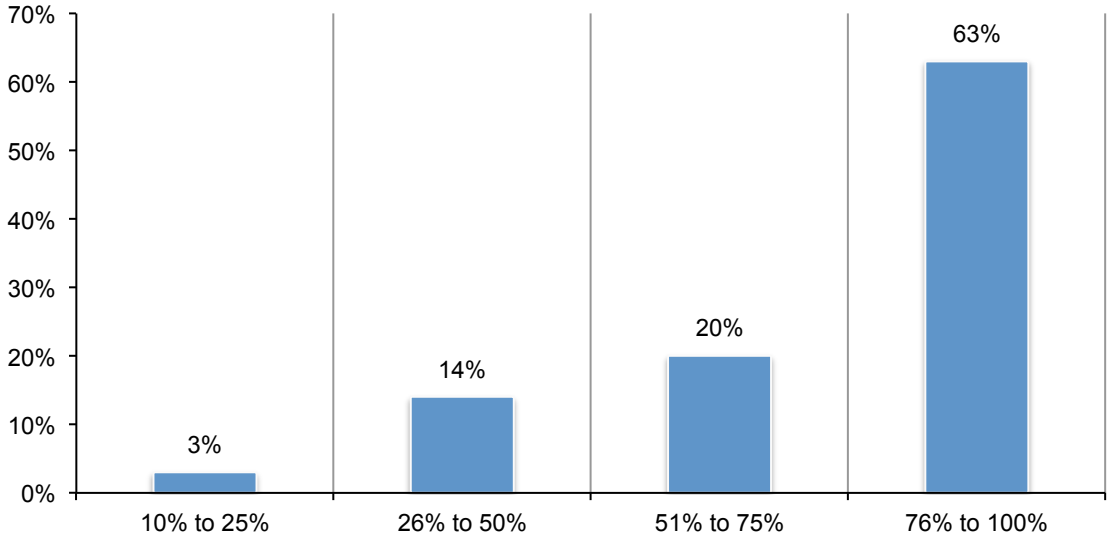
Security intelligence practices and problems. An average of 65 percent of staff bandwidth is allocated to reactive vs. proactive security activities. According to Figure 15, the majority of companies in this study (49 percent) perform a network scan for vulnerabilities hourly (18 percent) or daily (31 percent). Twenty-two percent scan weekly (12 percent) or monthly (10 percent). Twenty-seven percent do not scan at regular intervals.

Figure 15. How often do you perform a network scan for vulnerabilities?



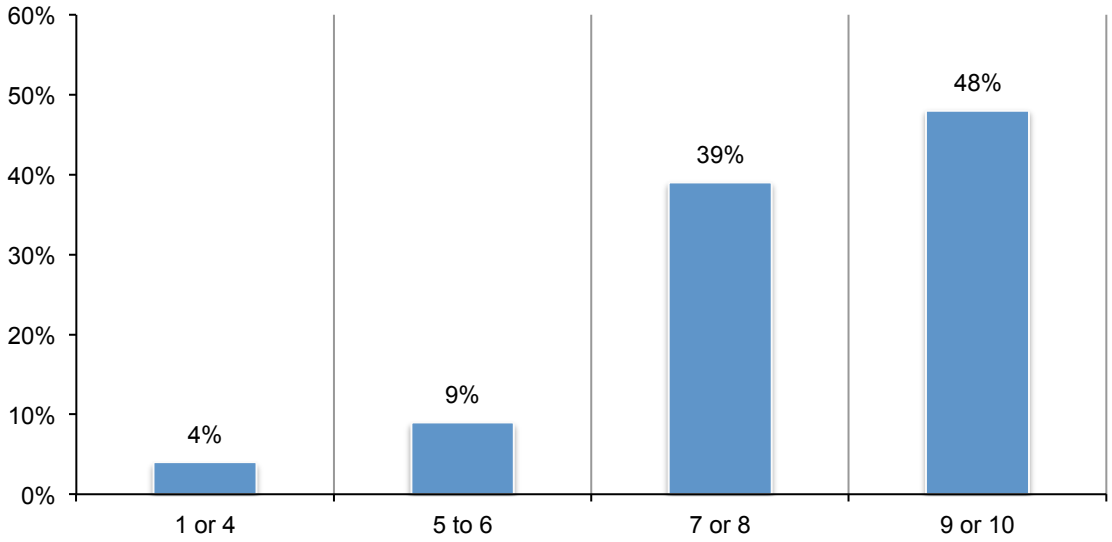
Thirty-five percent of respondents say their organizations have trouble prioritizing vulnerabilities. As shown in Figure 16, an average of 73 percent of discovered vulnerabilities are patched. Respondents report that an average of nine attacks occur each week and 35 network breaches were discovered over the past year.

Figure 16. What percentage of discovered vulnerabilities can you periodically patch?
Extrapolated average = 73 percent



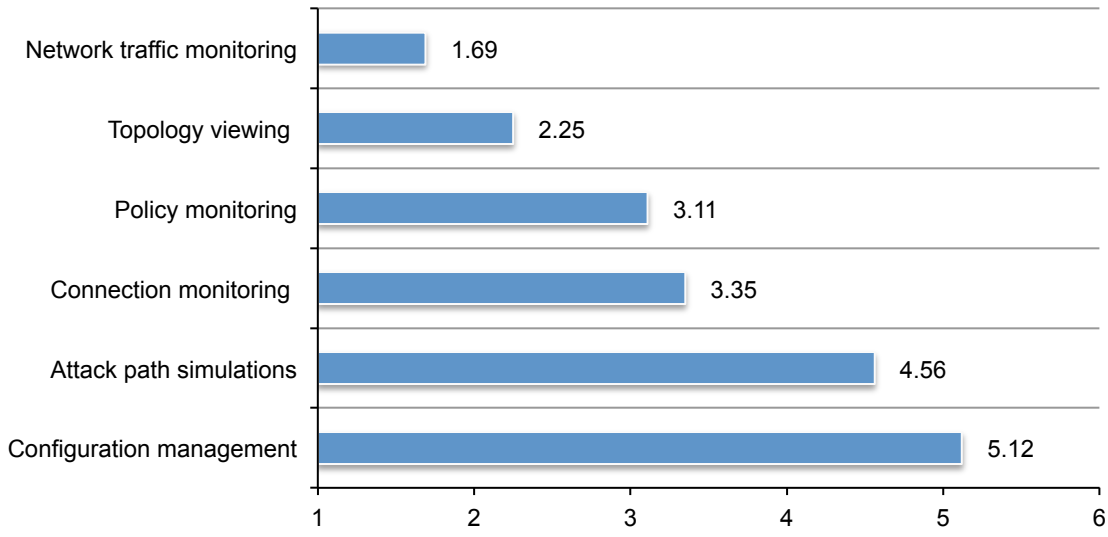
Companies rate satisfaction with QRadar as high or very high. Almost all (87 percent of respondents) rate their satisfaction as high (39 percent) or very high (48 percent), as shown in Figure 17. More detail about satisfaction with these solutions is presented below.

Figure 17. How satisfied are you with the QRadar solution used in your organization?
1 = low to 10 = high



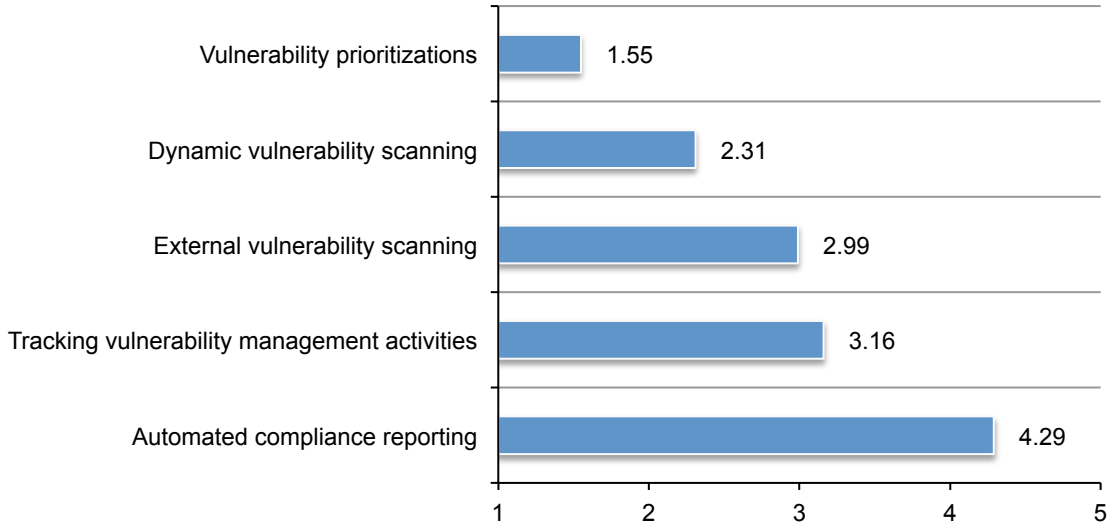
QRadar platform solutions. Only 38 percent of respondents purchased QRadar Risk Manager. Of those companies that deployed platform solutions, 30 percent say it is fully deployed, 33 percent say it was partially deployed and 37 percent have yet to deploy. The most valuable features are network traffic monitoring, topology viewing and policy monitoring, as shown in Figure 18.

Figure 18. How do you rank the QRadar Risk Manager features?
1 = most valuable to 5 = least valuable



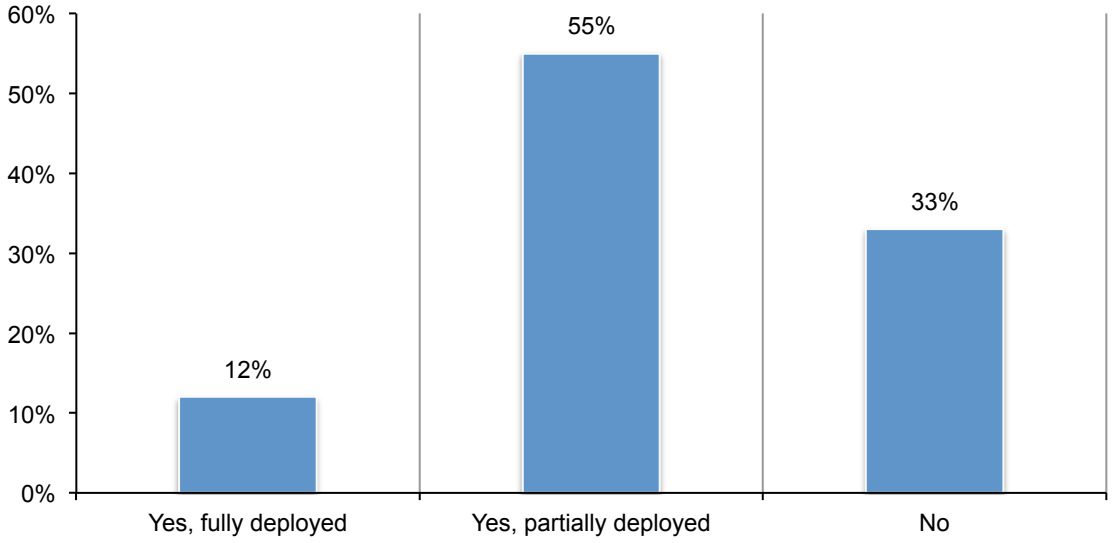
QRadar Vulnerability Manager was purchased by 35 percent of the companies in this study. Of those companies that purchased this solution, 36 percent have fully deployed it and 31 percent have partially deployed it. Approximately one-third (33 percent) of companies have yet to deploy Vulnerability Manager. As shown in Figure 19, the best features are vulnerability prioritizations, dynamic vulnerability scanning and external vulnerability scanning.

Figure 19. How do you rank the QRadar Vulnerability Manager Features
1 = most valuable to 5 = least valuable



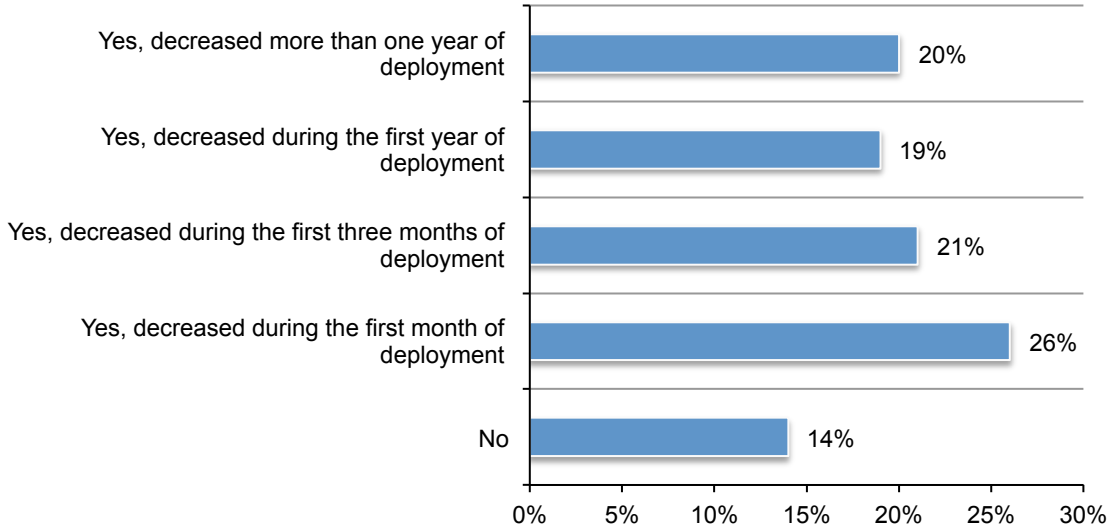
QRadar Incident Forensics was purchased by only 19 percent of companies in this study. Of those companies that have this solution only 12 percent are fully deployed and 55 percent have partially deployed Incident Forensics. Thirty-three percent have not deployed it, as shown in Figure 20.

Figure 20. Have you deployed QRadar Incident Forensics?



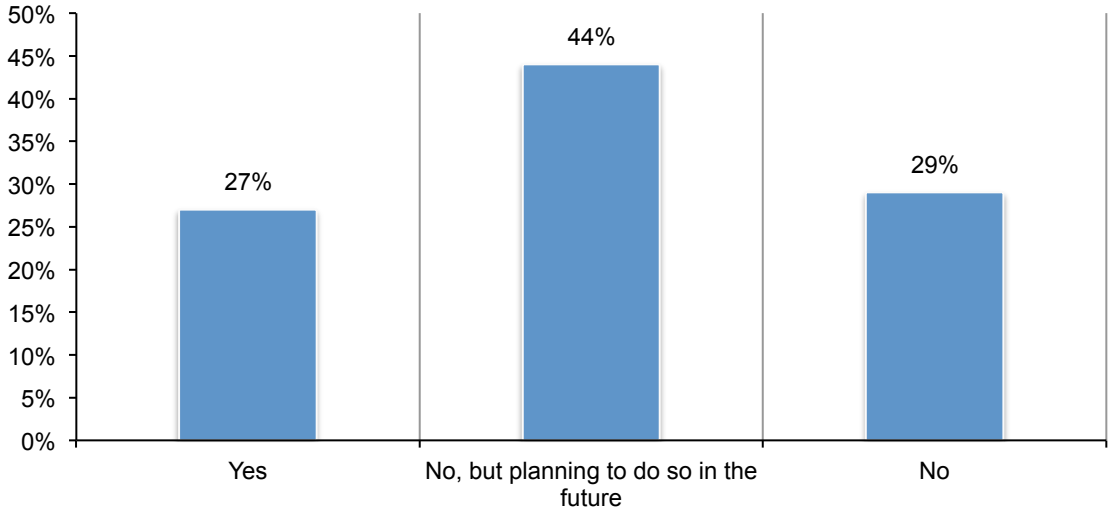
Most companies (86 percent) say the amount of time invested in tuning QRadar has decreased since its initial deployment, according to Figure 21. Twenty-six percent say it happened during the first month of deployment and 21 percent say it decreased during the first three months of deployment.

Figure 21. Has the amount of time invested in tuning QRadar decreased since its initial deployment?



On average, companies see 15 QRadar offenses on a daily basis. Sixty-four percent of respondents say they are able to investigate all the daily offenses generated. According to Figure 22, to help expedite investigations, 27 percent of respondents say their companies currently use a network forensics/full packet capture product to help expedite investigations.

Figure 22. Do you use a network forensics/full packet capture product to help expedite investigations?



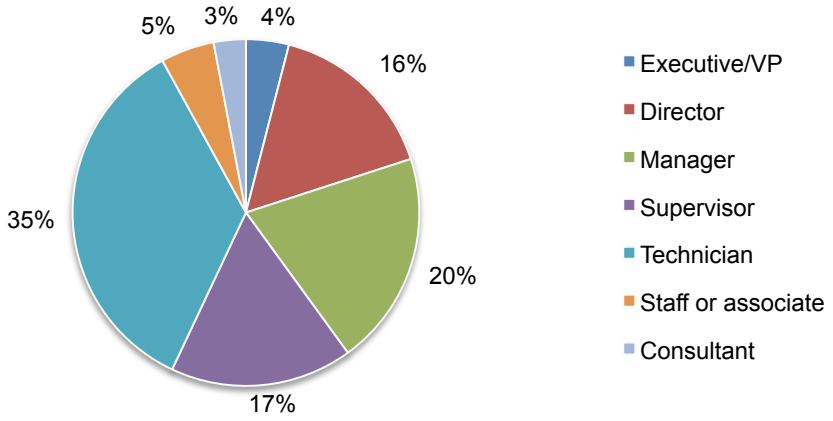
Part 3. Demographics

A sampling frame composed of 19,076 IT and IT security practitioners located in the United States in organizations that use QRadar were selected for participation in this survey. While 440 respondents returned their survey, 244 were removed because of additional screening criteria, as shown in the Table 1. The final sample consisted of 196 surveys from bona fide sources (1.03 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	19,076	100.0%
Total returns	440	2.3%
Rejected or screened surveys	244	1.3%
Final sample	196	1.03%

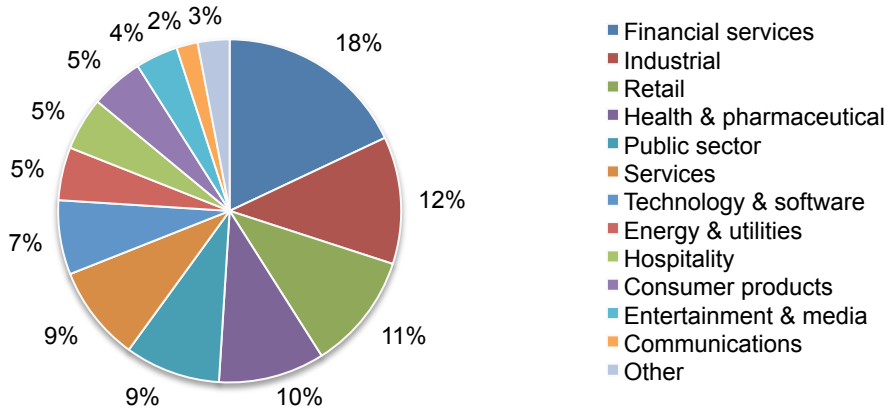
Pie chart 1 reports the current position or organization level of the respondent. More than half (57 percent) of respondents reported their current position is at or above the supervisory level.

Pie Chart 1. Position level within the organization



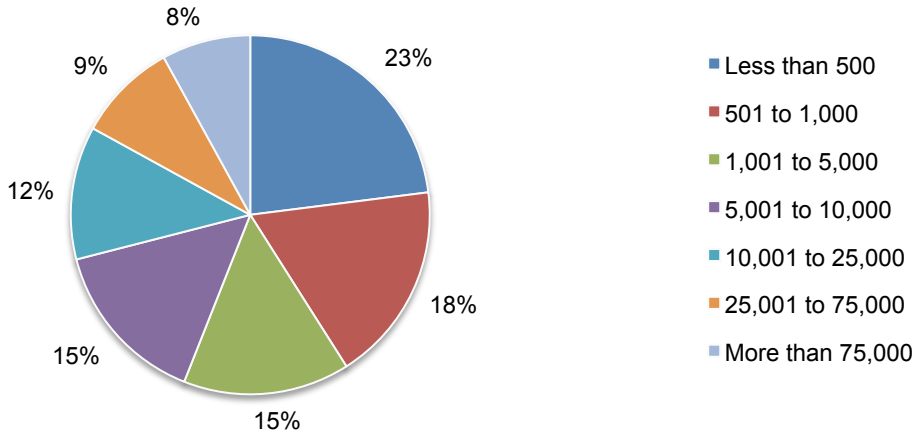
Pie Chart 2 reports the primary industry classification for the respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by industrial (12 percent) and retail (11 percent).

Pie Chart 2. The primary industry classification for the IT respondent



Pie chart 3 reports the full-time headcount of the global organization. More than half (59 percent) of respondents are from organizations with more than 1,000 full-time employees.

Pie Chart 2. Full-time headcount of the global organization



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 March 2015.

Survey response	Freq
Total sampling frame	19076
Total returns	440
Rejected or screened surveys	244
Final sample	196
Response rate	1.03%

Part 1. Questions about Technology Deployment

Q1. How long has your organization used QRadar to monitor and defend your company's network?	Pct%
Less than 1 year	9%
1 or 2 years	25%
3 or 4 years	32%
5 or 6 years	23%
More than 6 years	11%
Total	100%
Extrapolated value	3.61

Q2. What QRadar release are you currently running?	Pct%
V7.0 or earlier	5%
V7.2.1	16%
V7.2.2	20%
V7.2.3	23%
V7.2.4	36%
Total	100%

Q3. Do you purchase annual maintenance and support?	Pct%
Yes	60%
No	40%
Total	100%

Q4. How frequently do you update your QRadar solutions?	Pct%
Only with every new major release	32%
With every major or minor release	28%
Only when a compelling new feature is released	5%
Monthly to add new patches and DSMs	11%
Weekly/daily via AutoUpdate	23%
Other	1%
Total	100%

Q5. Do you use the AutoUpdate service?	Pct%
Yes	40%
No	60%
Total	100%

Q6. Do you purchase any QRadar components as hardware appliances?	Pct%
Yes, all-in-one	19%
Yes, core appliance/console	15%
Yes, console plus event processors	16%
Yes, console, event processors, and flow processors	11%
No	39%
Total	100%

Q7a. Did you purchase any QRadar components as software appliances?	Pct%
Yes, all-in-one	32%
Yes, core appliance/console	23%
Yes, console plus event processors	18%
Yes, console, event processors, and flow processors	10%
No	17%
Total	100%

Q7b. If no, have you deployed QRadar virtual appliances?	Pct%
Yes, exclusively	10%
Yes, in some specific instances	25%
Yes, in order to include cloud service monitoring	18%
No	47%
Total	100%

Q8. What QRadar appliances (hardware/software/virtual) are contained within your security intelligence solution? Please select all that apply.	Pct%
Consoles	90%
Event Processors	69%
Flow Processors	57%
QFlow Processors	48%
Risk Manager appliance	38%
Vulnerability Manager appliance	38%
Incident Forensics appliance	17%
Total	357%

Q9a. Did you purchase any professional services to help you with the initial deployment?	Pct%
Yes	33%
No	67%
Total	100%

Q9b. If yes, how many days of professional services were provided during the initial deployment?	Pct%
Less than 1 day	8%
1 to 2 days	43%
3 to 4 days	21%
5 to 6 days	15%
7 to 8 days	8%
9 to 10 days	3%
11 to 20 days	2%
More than 20 days	0%
Total	100%
Extrapolated value	3.46

Q10. How long did it take you to begin recognizing value from the QRadar deployment?	Pct%
Within days	43%
Within a week	27%
Within a month	13%
Within three months	9%
More than three months	6%
Value has not been realized as yet	2%
Total	100%

Part 2. Questions about licensing for QRadar Event Processors

Q11. How many log source events per second does your license permit?	Pct%
500	11%
1,000	12%
5,000	24%
10,000	25%
20,000	15%
Other	3%
Unsure	10%
Total	100%
Extrapolated value	6,875

Q12. How many log source event devices does your license permit?	Pct%
750	8%
1,000	11%
2,000	12%
5,000	19%
10,000	24%
25,000	11%
50,000	2%
Other	3%
Unsure	10%
Total	100%
Extrapolated value	7,510

Q13. Have you ever had to upgrade your log source license capabilities to accommodate growth?	Pct%
Yes	48%
No	43%
Unsure	9%
Total	100%

Q14. Have you ever had any dropped events due to licensing issues?	Pct%
Yes	39%
No	52%
Unsure	9%
Total	100%

Part 3. Questions about licensing For QRadar Flow Processors

Q15. How many flows per minute does your license permit?	Pct%
100K	6%
200K	14%
300K	14%
600K	26%
900K	19%
1.2M	9%
Other	3%
Unsure	9%
Total	100%

Q16. Have you ever had to upgrade you network flow licensing capabilities to accommodate growth?	Pct%
Yes	47%
No	44%
Unsure	9%
Total	100%

Q17. Do you use QFlow or VFlow Collectors to obtain Layer 7 insights?	Pct%
Yes, as part of my all-in-one solution	15%
Yes, broadly using separate QFlow.VFlow Collectors	21%
Yes, in limited areas using QFlow/VFlow collectors	32%
No	32%
Total	100%

Part 4. Questions about QRadar Platform Solutions

Q18a. Have you purchased QRadar Risk Manager?	Pct%
Yes	38%
No	62%
Total	100%

Q18b. If yes, have you deployed QRadar Risk Manager?	Pct%
Yes, fully deployed	30%
Yes, partially deployed	33%
No	37%
Total	100%

Q18c. If yes, can your rank order the value of the following QRadar Risk Manager features:	Average rank
Configuration management	5.12
Policy monitoring	3.11
Network traffic monitoring	1.69
Connection monitoring	3.35
Topology viewing	2.25
Attack path simulations	4.56

Q19a. Have you purchased QRadar Vulnerability Manager?	Pct%
Yes	35%
No	65%
Total	100%

Q19b. If yes, have you deployed QRadar Vulnerability Manager?	Pct%
Yes, fully deployed	36%
Yes, partially deployed	31%
No	33%
Total	100%

Q19c. If yes, can you rank order the value of the following QRadar Vulnerability Manager features:	Average rank
Dynamic vulnerability scanning	2.31
External vulnerability scanning	2.99
Vulnerability prioritizations	1.55
Automated compliance reporting	4.29
Tracking vulnerability management activities	3.16

Q20a. Have you purchased QRadar Incident Forensics?	Pct%
Yes	19%
No	83%
Total	102%

Q20b. If yes, have you deployed QRadar Incident Forensics?	Pct%
Yes, fully deployed	12%
Yes, partially deployed	55%
No	33%
Total	100%

Part 5. Questions about QRadar Tuning

Q21. How valuable were the out-of-box QRadar correlation rules?	Pct%
Very valuable	48%
Somewhat valuable	39%
Neutral	11%
Not very valuable	2%
No value	0%
Total	100%

Q22. How many custom correlation rules have you developed?	Pct%
None	3%
1 to 10	17%
11 to 25	46%
26 to 50	18%
51 to 100	14%
More than 100	2%
Total	100%
Extrapolated value	28.87

Q23. Do you consider it difficult to fine-tune QRadar?	Pct%
Not at all	50%
Somewhat difficult	28%
Neutral	11%
Fairly difficult	8%
Very difficult	3%
Total	100%

Q24. On average, how many QRadar offenses do you see on a daily basis?	Pct%
Less than 5	6%
5 to 10	34%
11 to 20	42%
21 to 35	10%
36 to 50	8%
More than 50	0%
Total	100%
Extrapolated value	15.41

Q25. Are you able to investigate all the daily offenses generated?	Pct%
Yes	64%
No	36%
Total	100%

Q26. Do you use a network forensics/full packet capture product to help expedite investigations?	Pct%
Yes	27%
No, but planning to do so in the future	44%
No	29%
Total	100%

Part 6. Questions about Operational Costs

Q27. Has the amount of time invested in tuning QRadar decreased since its initial deployment?	Pct%
No	14%
Yes, decreased during the first month of deployment	26%
Yes, decreased during the first three months of deployment	21%
Yes, decreased during the first year of deployment	19%
Yes, decreased more than one year of deployment	20%
Total	100%

Q28. How many full or partial headcount are allocated to security intelligence operations?	Pct%
Half FTE	38%
1 FTE	43%
2 FTEs	17%
More than 2+ FTEs	2%
Total	100%

Q29a. Did QRadar Security Intelligence help you reduce the headcount associated with daily security incident investigations?	Pct%
Yes	77%
No	23%
Total	100%

Q29b. If yes, what headcount reduction did you experience?	Pct%
Half FTE	36%
1 FTE	43%
2 FTEs	16%
More than 2+ FTEs	5%
Total	100%

Q30a. Have you purchased any additional professional services to help with QRadar since the initial implementation? Please select all that apply.	Pct%
Yes, for tuning	7%
Yes, for new module installation	8%
Yes, for incident response	8%
Yes, for integrations	7%
No	70%
Total	100%

Q30b. If yes, how many days of professional services were provided post deployment?	Pct%
Less than 1 day	18%
1 to 2 days	43%
3 to 4 days	29%
5 to 6 days	7%
7 to 8 days	3%
9 to 10 days	0%
11 to 20 days	0%
More than 20 days	0%
Total	100%
Extrapolated value	2.43

Q31a. Were you able to replace any point security solution products as a result of deploying QRadar?	Pct%
Yes	62%
No	38%
Total	100%

Q31b. If yes, how many point solutions were replaced?	Pct%
1 or 2	35%
3 to 5	27%
6 to 10	23%
11 to 20	10%
More than 20	5%
Total	100%
Extrapolated value	6.20

Part 7. General Questions:

Q32a. As part of the QRadar initial evaluation, did you conduct a proof of technology or proof of concept trials with competitive solutions?	Pct%
Yes	55%
No	45%
Total	100%

Q32b. If yes, what competitive solutions were considered in the evaluation process? Please select all that apply.	Pct%
ArcSight	26%
Splunk	21%
RSA	17%
McAfee	15%
LogRhythm	12%
Other	9%
Total	100%

Q33. What use cases were most important to the evaluation and purchase of ORadar? Please select all that apply.	Pct%
Policy and Regulatory Compliance Monitoring	54%
Policy Violation/Resource Misuse	50%
Vulnerability Reporting	44%
Correlating Asset Vulnerabilities with IPS events	47%
Detecting excessive Firewall denies	24%
Detecting Threats or Suspicious Changes in Behavior	59%
Detection of Zero-Day Threats	47%
Recognizing Brute-Force Attack	38%
Data Loss Prevention	20%
Long Duration Connections/Flows	25%
Known BOT Control Channel Communications	19%
Social Media Monitoring	11%
Suspicious Access Correlation	62%
Monitoring Authorized Users for Inappropriate Activities	66%
Device Configuration Risk Analysis	63%
Total	629%

Q34. What percentage of your staff bandwidth is allocated to reactive vs. proactive security activities?	Pct%
Less than 10% is proactive	0%
10% to 25% is proactive	9%
26% to 50% is proactive	23%
51% to 75% is proactive	19%
76% to 100% is proactive	49%
Total	100%
Extrapolated value	65%

Q35. How often do you perform a network scan for vulnerabilities?	Pct%
Hourly	18%
Daily	31%
Weekly	12%
Monthly	10%
Every three months	2%
More than three months	0%
No regular intervals	27%
Total	100%

Q36. Do you have trouble prioritizing discovered vulnerabilities?	Pct%
Yes	35%
No	65%
Total	100%

Q37. What percentage of discovered vulnerabilities can you periodically patch?	Pct%
Less than 10%	0%
10% to 25%	3%
26% to 50%	14%
51% to 75%	20%
76% to 100%	63%
Total	100%
Extrapolated value	73%

Q38. How many attacks do you see on an average basis every week?	Pct%
Less than 5	45%
5 to 10	34%
11 to 20	12%
21 to 30	7%
31 to 40	1%
41 to 50	1%
51 to 100	0%
More than 100	0%
Total	100%
Extrapolated value	8.70

Q39. How many network breaches have you discovered over the past year?	Pct%
Less than 5	0%
5 to 10	8%
11 to 20	19%
21 to 30	30%
31 to 40	15%
41 to 50	12%
51 to 100	11%
More than 100	5%
Total	100%
Extrapolated value	35.35

Q40. Do you use QRadar with Operations Technology (ICS/SCADA)?	Pct%
Yes	15%
No	85%
Total	100%

Q41. Did you acquire QRadar through an IBM Business Partner?	Pct%
Yes	36%
No	64%
Total	100%

Q42. Using the following 10-point scale, please rate your level of satisfaction with the QRadar solutions used in your organization? 1 = low to 10 = high.	Pct%
1 or 2	0%
3 or 4	4%
5 or 6	9%
7 or 8	39%
9 or 10	48%
Total	100%
Extrapolated value	8.12

Part 8. Respondent demographics

D1. Position level	Pct%
Executive/VP	4%
Director	16%
Manager	20%
Supervisor	17%
Technician	35%
Staff or associate	5%
Consultant	3%
Total	100%

D2. Industry segment	Pct%
Financial services	18%
Industrial	12%
Retail	11%
Health & pharmaceutical	10%
Public sector	9%
Services	9%
Technology & software	7%
Energy & utilities	5%
Hospitality	5%
Consumer products	5%
Entertainment & media	4%
Communications	2%
Other	3%
Total	100%

D3. Global headcount	Pct%
Less than 500	23%
501 to 1,000	18%
1,001 to 5,000	15%
5,001 to 10,000	15%
10,001 to 25,000	12%
25,001 to 75,000	9%
More than 75,000	8%
Total	100%

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 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.