IBM QRadar Security Intelligence: Evidence of Value

Independently conducted by Ponemon Institute LLC

February 2014

IBM QRadar: Evidence of Value

Ponemon Institute: February 2014

Background

Ponemon Institute was engaged by IBM to conduct an independent validation study of its security incident event management (SIEM) solution termed QRadar. The purpose of this study was to better understand the elements of QRadar that bring value to customers and users. We specifically focused interview questions on QRadar's product features as well as enterprise deployment experiences. Another objective of this research was to compare QRadar's value propositions to other market-leading providers of SIEM and network traffic intelligence solutions.[1]

Ponemon Institute independently conducted one-to-one confidential interviews with a learned group of 25 IT and IT security practitioners mostly from larger-sized U.S. companies in seven industry sectors. By design, all participating respondents and companies used another SIEM solution and later switched to IBM's QRadar.

Our interview script included 30 fix-formatted questions. Using a diagnostic interview technique we are able to do additional probes to obtain a deeper understanding about QRadar capabilities and benefits. Following are the four focal points of our interviews.

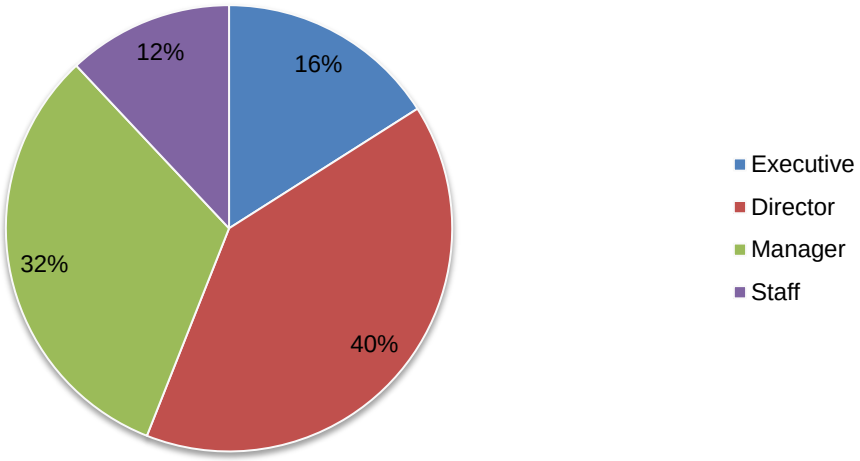
- Rationale for selecting QRadar and switching SIEM providers
- Recent experiences in managing and containing network traffic anomalies
- Recent experiences in deploying SIEM solutions across the enterprise
- Comparison of QRadar features to those of other SIEM providers

About respondents

As noted in Pie Chart 1, a majority of respondents hold positions at or above the director level within their organizations. Most respondents are IT security leaders within their respective companies. In total, nine individuals hold the CISO or equivalent job title. The average relevant experience is 16.5 years (median at 15.0 years).

Pie Chart 1: Position of respondents

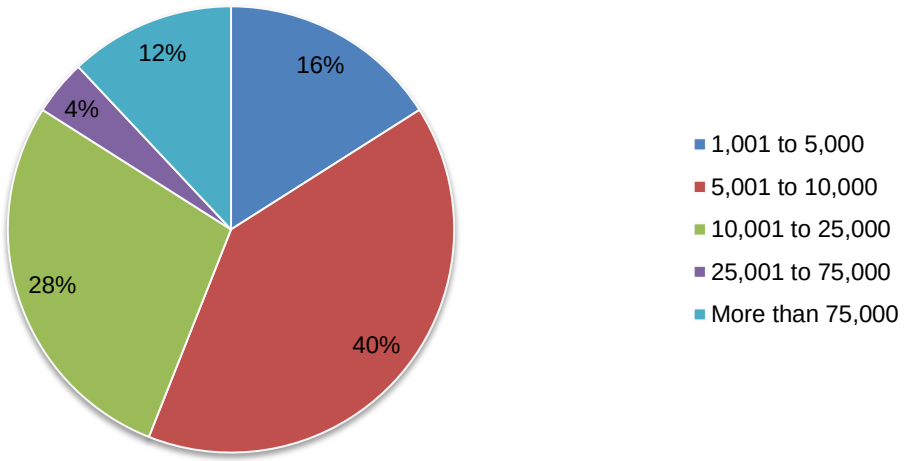
Analysis conducted from 25 confidential interviews of QRadar users



[1] Other marketing-leading SIEM providers include: HP (ArcSight), McAfee (Nitro), Splunk, LogRhythm and RSA (Netwitness).

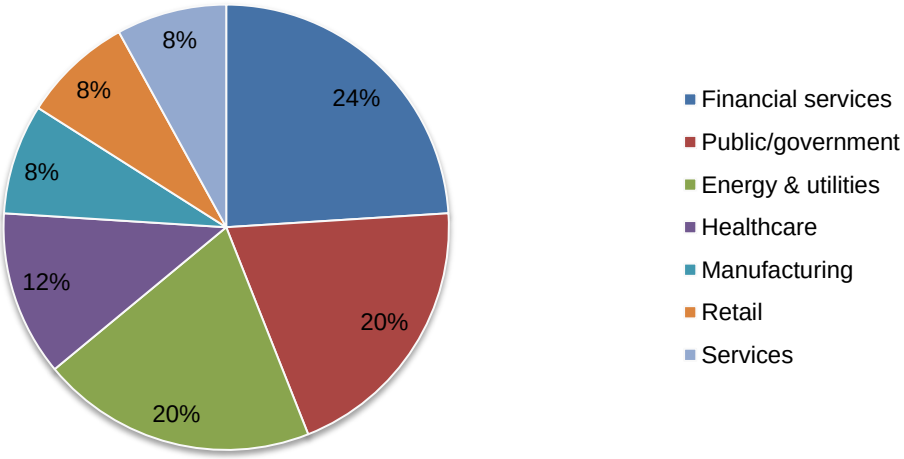
Pie Chart 2 shows the headcount of participating organizations. As can be seen, the vast majority of respondents' organizations have more than 5,000 full time equivalent employees.

Pie Chart 2: Headcount of participating companies
Analysis conducted from 25 confidential interviews of QRadar users



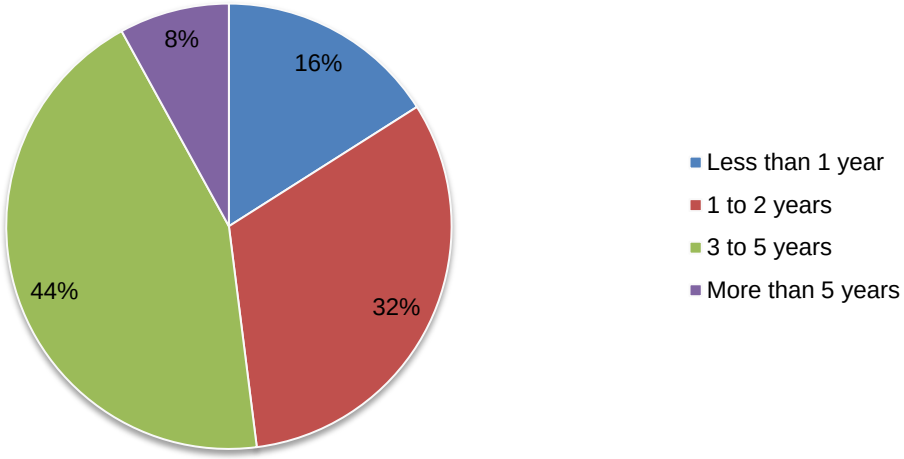
Pie Chart 3 summarizes the primary industry sectors of participants' organizations. The largest sectors are financial services, public sector and energy and utilities.

Pie Chart 3: Industry distribution of respondents' organizations
Analysis conducted from 25 confidential interviews of QRadar users



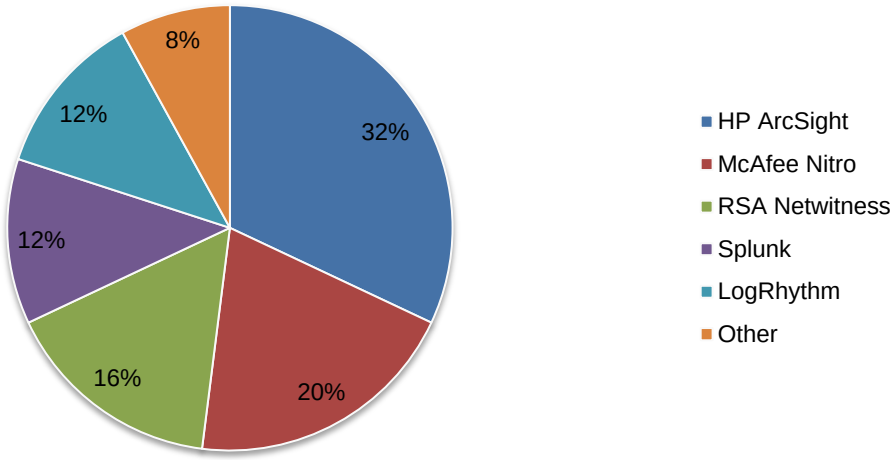
Pie Chart 4 summarizes the length of time interviewees say their organizations have used QRadar. The largest segment says their organizations have three to five years of QRadar experience.

Pie Chart 4: Length of time respondents' organizations used QRadar
Analysis conducted from 25 confidential interviews of QRadar users



Pie Chart 5 summarizes the former SIEM providers utilized by respondents' companies before making the switch to IBM's QRadar product.

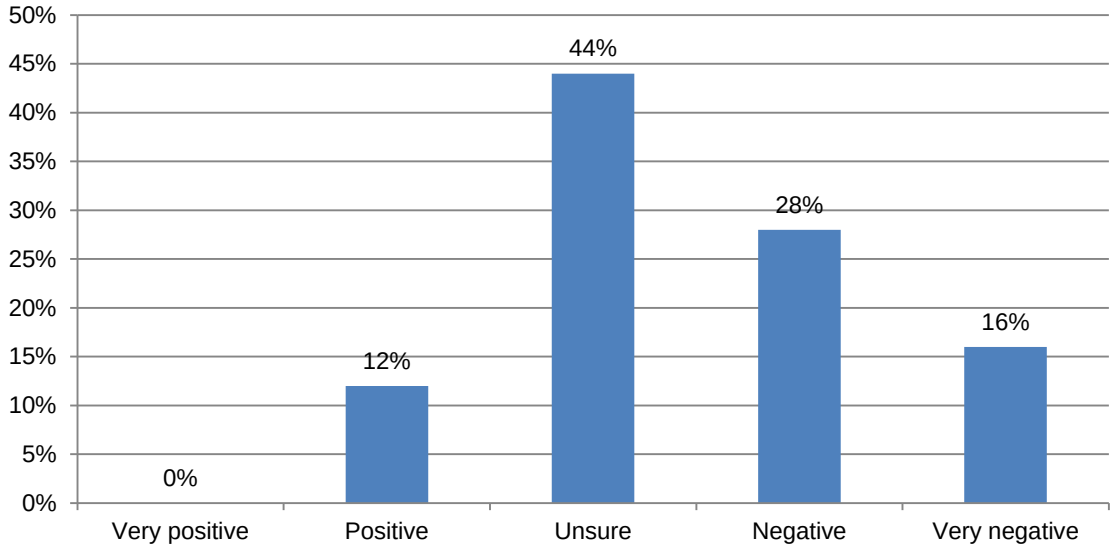
Pie Chart 5: Former SIEM providers before switching to QRadar
Analysis conducted from 25 confidential interviews of QRadar users



Key findings

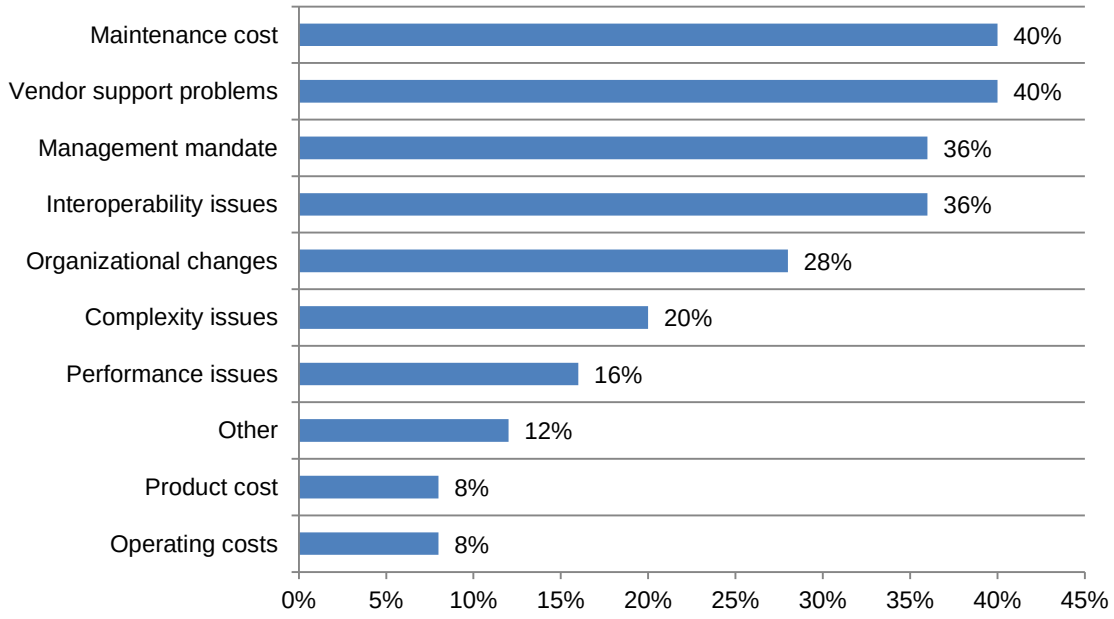
Bar Chart 1 reports the perceptions of QRadar users concerning their former SIEM solution providers. As shown below, a majority of interviewees hold negative impressions of their former providers.

Bar Chart 1: QRadar user perceptions about former SIEM providers
Analysis conducted from 25 confidential interviews of QRadar users



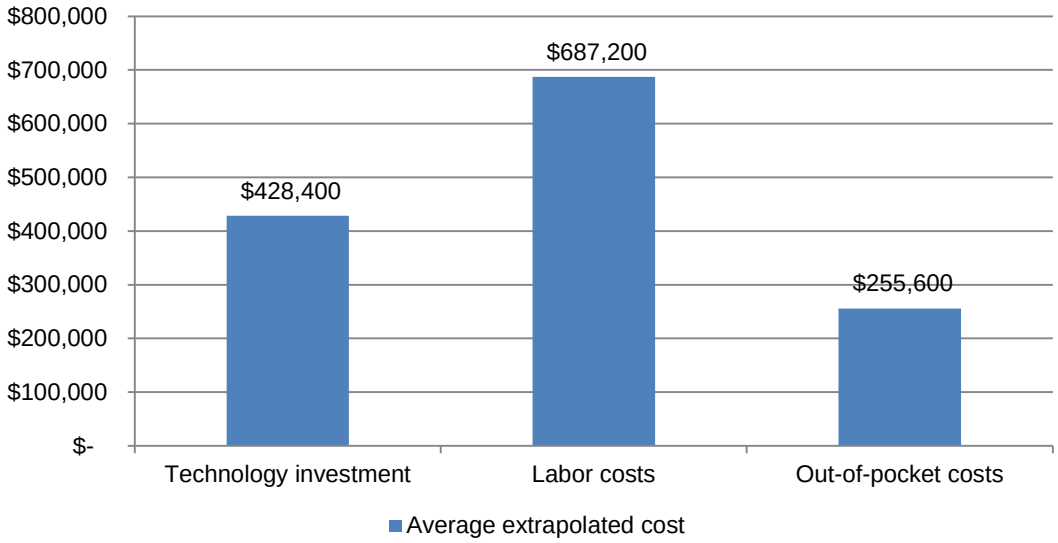
Bar Chart 2 summarizes the main reasons for switching from prior SIEM provider to IBM's QRadar according to interviewees. The top reasons include maintenance cost, vendor support problems, management mandate and interoperability issues.

Bar Chart 2: Reasons for switching to QRadar
Analysis conducted from 25 confidential interviews of QRadar users



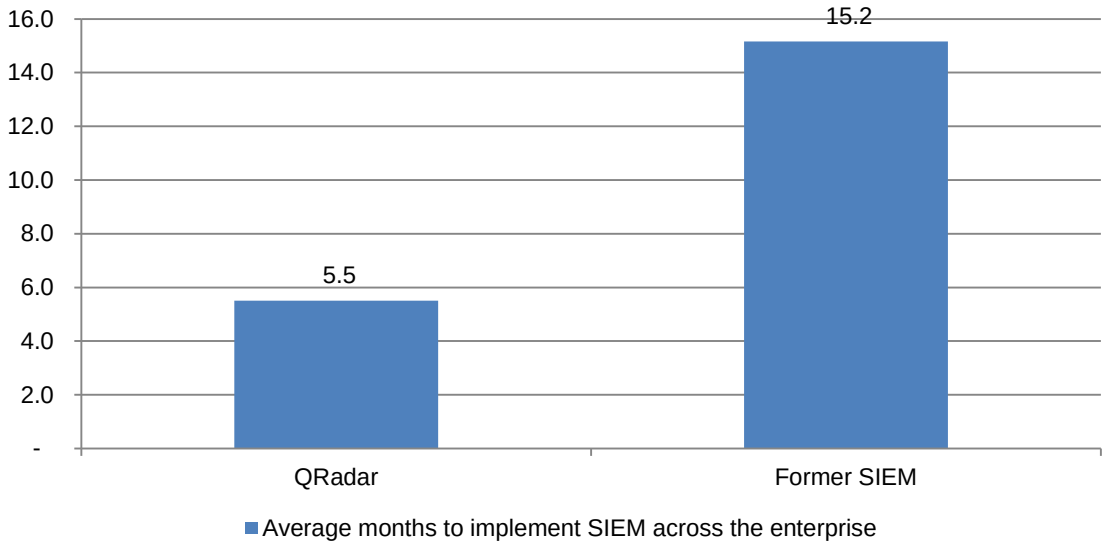
Bar Chart 3 reports the extrapolated average cost incurred by interviewees' companies to deploy QRadar across the enterprise. As shown, the most significant cost category concerns labor cost to implement and maintain SIEM solution.

Bar Chart 3: Extrapolated average cost spent on SIEM
Analysis conducted from 25 confidential interviews of QRadar users



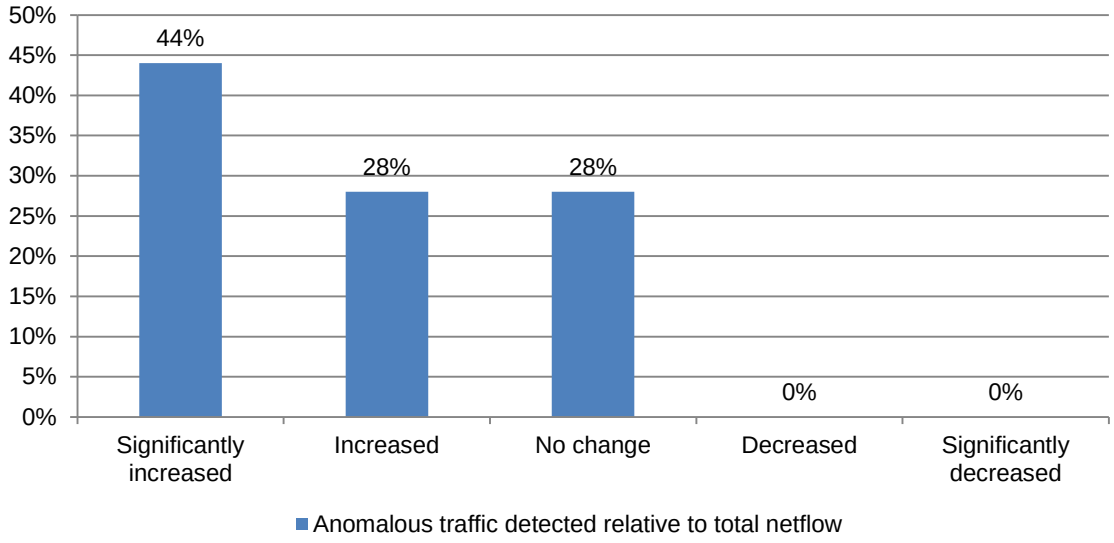
Bar Chart 4 reports the extrapolated average length of time to fully implement SIEM across the enterprise measured in months. This chart compares the interviewees' experience implementing their former SIEM solution to the QRadar implementation experience. Albeit only an estimate, the results suggest marked differences in the implementation experience (i.e., 3 X difference).

Bar Chart 4: Extrapolated average length of time (months) to implement SIEM
Analysis conducted from 25 confidential interviews of QRadar users



Bar Chart 5 compares anomalous traffic detection rates between former SIEM providers and QRadar. As can be seen, 72 percent of interviewees say the detection rate has increased or significantly increased as a result of the switch to QRadar. In contrast, virtually no interviewee said the detection rate decreased after the switch to QRadar.

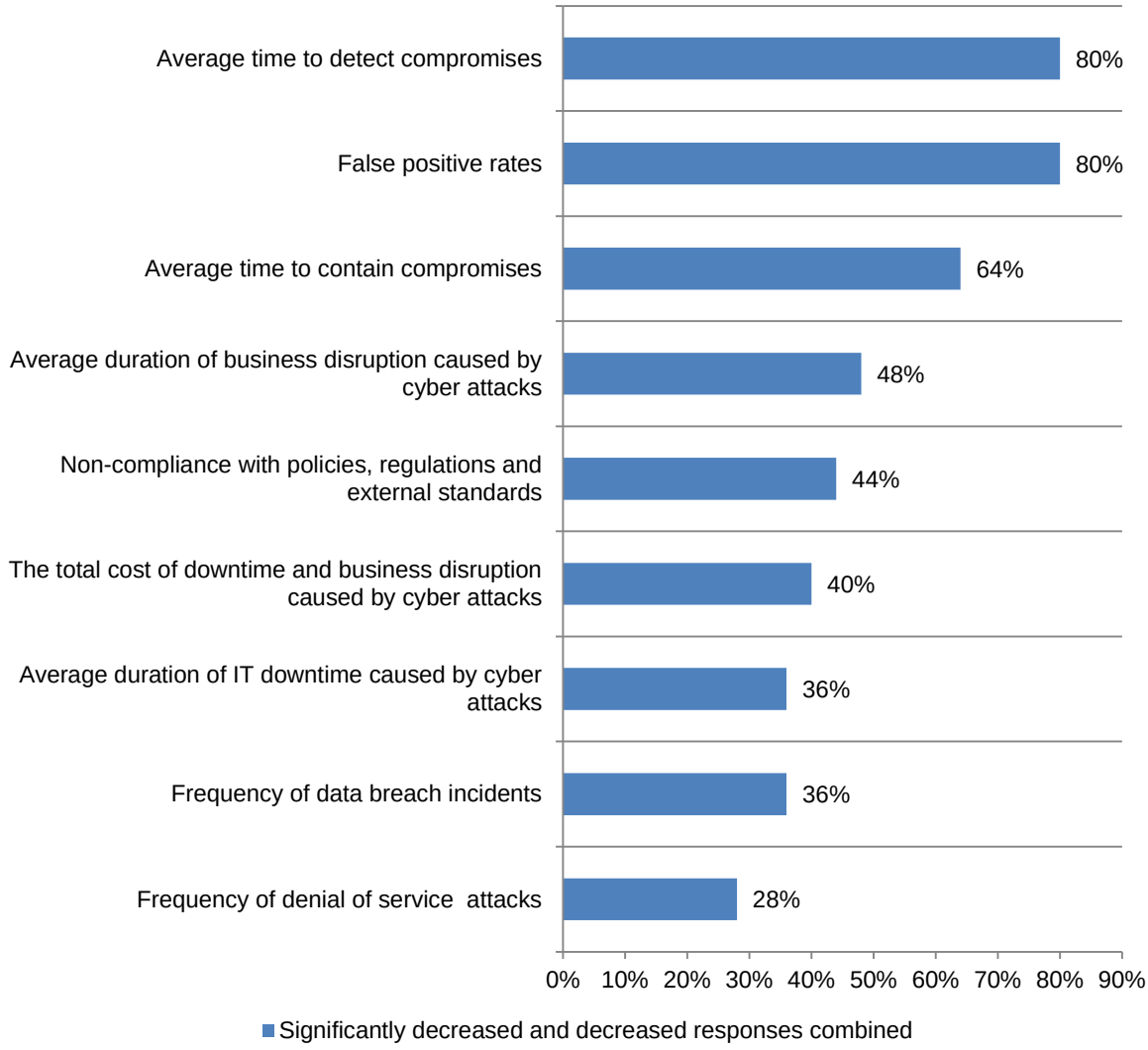
Bar Chart 5: Comparison of anomalous traffic detection relative to total netflow
Analysis conducted from 25 confidential interviews of QRadar users



Bar Chart 6 provides the QRadar experience according to nine normatively important attributes. Interviewees rated each attribute using a five-point scale ranging from significantly increased to significantly decreased. Please note that each percentage represents the significantly decreased and decreased response combined.

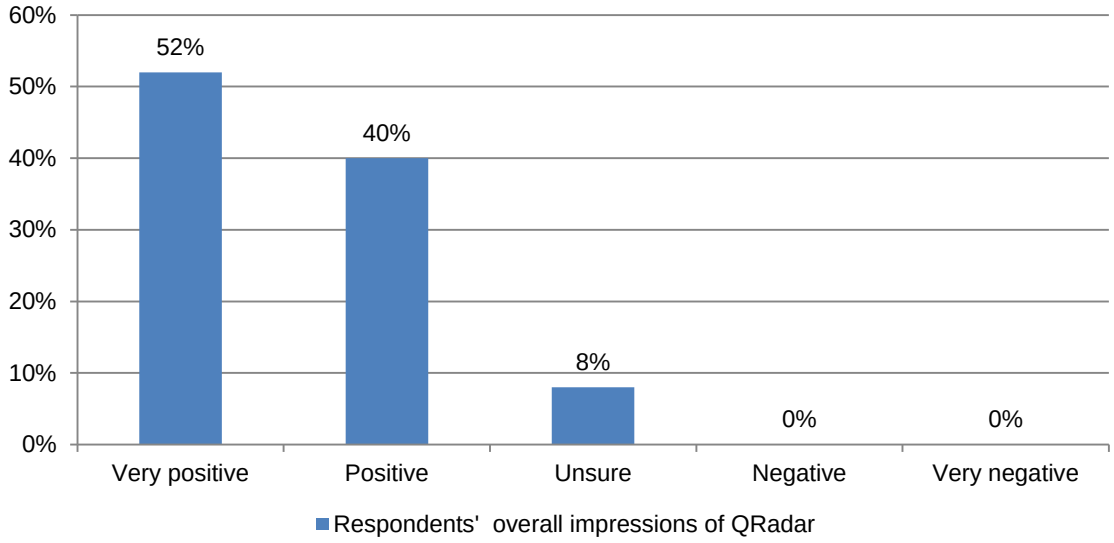
The most salient findings concern the average time to detect compromises, false positive rates, average time to contain compromises and average duration of business disruptions caused by cyber attacks. According to many interviewees, all of these attributes either decreased or significantly decreased as a result of effective deployment of QRadar across the enterprise.

Bar Chart 6: Experience after deploying QRadar for nine attributes
Percentage of interviewees that said each attribute either decreased or significantly decreased after the deployment of QRadar. Analysis conducted from 25 confidential interviews of QRadar users



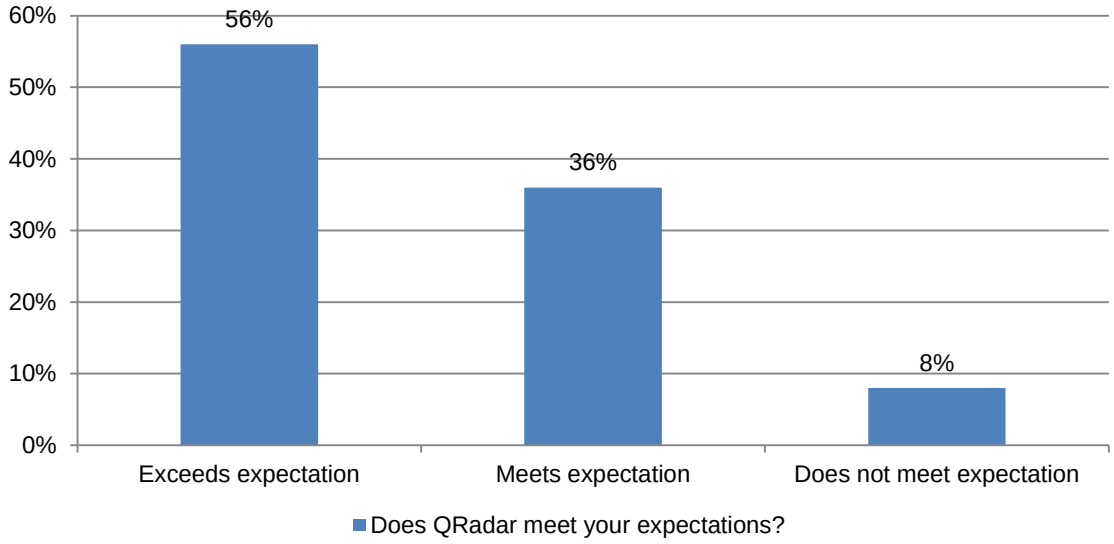
Bar Chart 7 provides very favorable results for QRadar. As can be seen, more than half of the interviewees rate their impression as very positive. In contrast, no interviewee provides a negative rating.

Bar Chart 7: Overall impressions of QRadar
Analysis conducted from 25 confidential interviews of QRadar users



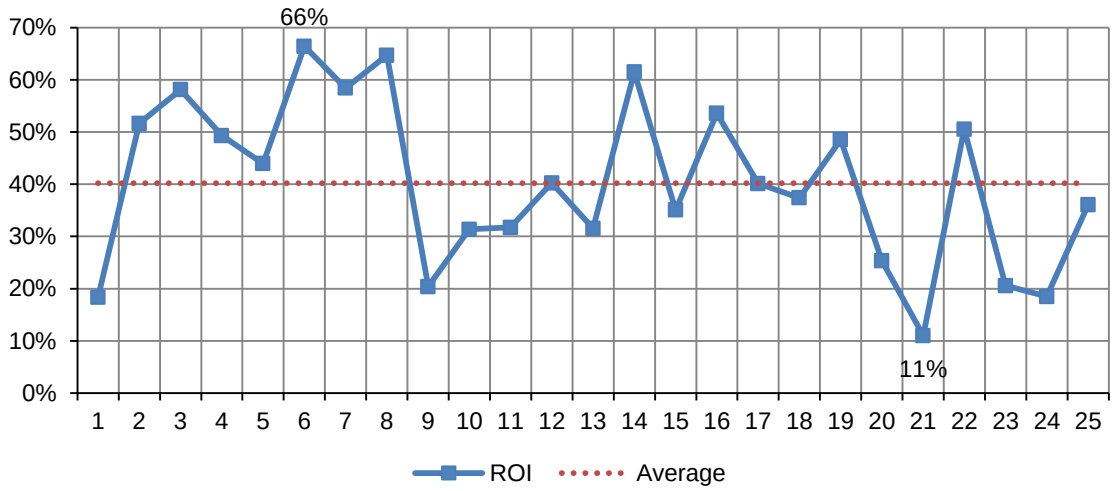
Bar Chart 8 provides more favorable results for QRadar. Fifty-six percent of interviewees say QRadar exceeded their expectations. Another 36 percent say QRadar met expectations and only 8 percent say it did not meet expectations.

Bar Chart 8: Does QRadar meet expectations?
Analysis conducted from 25 confidential interviews of QRadar users



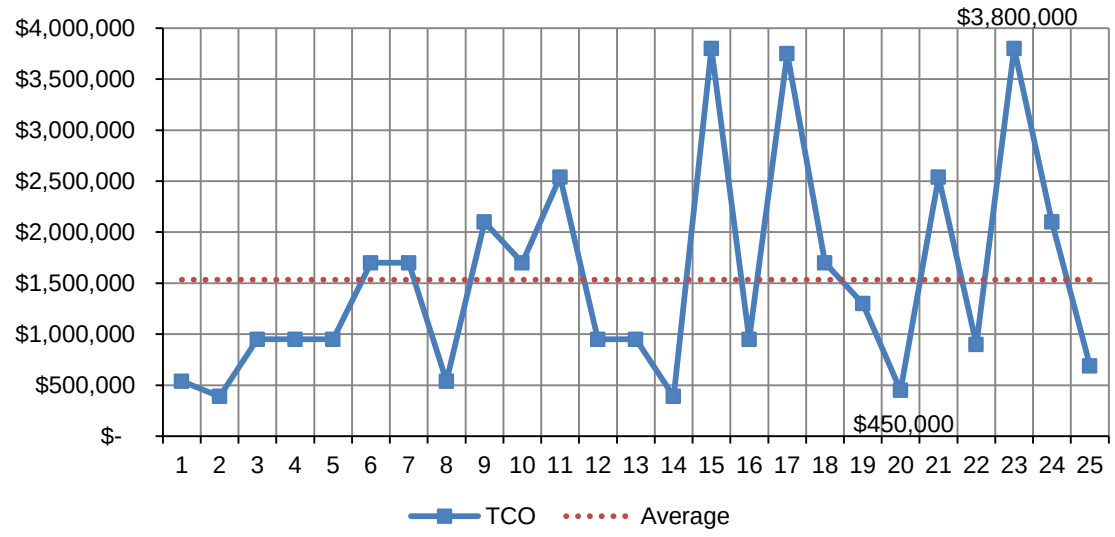
Line Graph 1 reports the individuated return on investment (ROI) estimates for 25 QRadar users. The ROI calculated for each security technology category is defined as: (1) gains from the investment divided by (2) cost of investment (minus any residual value). We estimate a three-year life for all technology categories presented. Hence, investments are simply amortized over three years. The gains are the net present value of cost savings expected over the investment life. From this amount, we subtract conservative estimates for operations and maintenance cost each year. The net present value used the prime plus 2 percent discount rate per year. We also assume no (zero) residual value. As can be seen, ROI results vary considerably from a high of 66 percent to a low of 11 percent. The mean ROI for all cases is 40 percent, which is illustrated by the dotted line in the graph.

Line Graph 1: ROI estimates for 25 cases
Analysis conducted from 25 confidential interviews of QRadar users



Line Graph 2 reports the individuated total cost of ownership (TCO) estimates for 25 QRadar users. Here again, TCO results vary considerably from a high of $3.80 million to a low of $.45 million. The dotted line represents the mean TCO for all cases, which is $1.53 million.

Line Graph 2: TCO estimates for 25 cases
Analysis conducted from 25 confidential interviews of QRadar users



Appendix 1: Diagnostic Interview Results

Fieldwork completed in January 2014

Q1. What best describes your position level within the organization?	Freq	Pct%
Executive	4	16%
Director	10	40%
Manager	8	32%
Technician	3	12%
Other	0	0%
Total	25	100%

Q2. What best describes the full-time headcount of your global organization?	Freq	Pct%
1,001 to 5,000	4	16%
5,001 to 10,000	10	40%
10,001 to 25,000	7	28%
25,001 to 75,000	1	4%
More than 75,000	3	12%
Total	25	100%

Q3. What best describes your organization's primary industry classification?	Freq	Pct%
Financial services	6	24%
Healthcare	3	12%
Manufacturing	2	8%
Public/government	5	20%
Energy & utilities	5	20%
Retail	2	8%
Services	2	8%
Other	0	0%
Total	25	100%

Q5. Former SIEM technology provider	Freq	Pct%
HP ArcSight	8	32%
McAfee Nitro	5	20%
Splunk	3	12%
LogRhythm	3	12%
RSA Netwitness	4	16%
Other	2	8%
Total	25	100%

Q6. Overall impression of your organization's former SIEM or network intelligence solutions	Freq	Pct%
Very positive	0	0%
Positive	3	12%
Unsure	11	44%
Negative	7	28%
Very negative	4	16%
Total	25	100%

Q7. Reason for the change	Freq	Pct%
Operating costs	2	8%
Complexity issues	5	20%
Limited functionality	12	48%
Vendor support problems	10	40%
Performance issues	4	16%
Organizational changes	7	28%
Maintenance cost	10	40%
Interoperability issues	9	36%
Product cost	2	8%
Management mandate	9	36%
Other	3	12%
Total	73	292%

Q8. Approximate length of time as a QRadar customer	Freq	Pct%
Less than 1 year	4	16%
1 to 2 years	8	32%
3 to 5 years	11	44%
More than 5 years	2	8%
Total	25	100%

Q9. The total investment in SIEM technologies	Freq	Pct%
Less than $100,000	2	8%
$100,000 to $200,000	5	20%
$200,001 to $400,000	5	20%
$400,001 to $600,000	4	16%
$600,001 to $800,000	4	16%
$800,001 to $1,000,000	2	8%
More than $1,000,000	3	12%
Total	25	100%

Q10. Fully loaded labor costs associated with the implementation and ongoing maintenance of the SIEM solutions:	Freq	Pct%
Less than $100,000	0	0%
$100,000 to $200,000	3	12%
$200,001 to $400,000	6	24%
$400,001 to $600,000	6	24%
$600,001 to $800,000	3	12%
$800,001 to $1,000,000	2	8%
$1,000,001 to $1,500,000	0	0%
$1,500,001 to $2,000,000	3	12%
More than $2,000,000	2	8%
Total	25	100%

Q11. Out-of-pocket costs paid for services relating to SIEM installation and deployment throughout the enterprise	Freq	Pct%
Less than $100,000	5	20%
$100,000 to $200,000	7	28%
$200,001 to $400,000	8	32%
$400,001 to $600,000	2	8%
$600,001 to $800,000	2	8%
$800,001 to $1,000,000	1	4%
More than $1,000,000	0	0%
Total	25	100%

Q12. Total time in months to install QRadar across the enterprise	Freq	Pct%
Less than 1 month	2	8%
1 to 3 months	8	32%
4 to 6 months	7	28%
7 to 9 months	5	20%
10 to 12 months	1	4%
13 to 15 months	0	0%
16 to 18 months	2	8%
19 to 21 months	0	0%
21 to 24 months	0	0%
More than 24 months	0	0%
Total	25	100%

Q13. Total time in months to install former SIEM across the enterprise	Freq	Pct%
Less than 1 month	0	0%
1 to 3 months	2	8%
4 to 6 months	2	8%
7 to 9 months	5	44%
10 to 12 months	4	16%
13 to 15 months	3	12%
16 to 18 months	3	12%
19 to 21 months	0	0%
21 to 24 months	4	16%
More than 24 months	2	8%
Total	25	100%

Q14. Anomalous traffic detected relative to total netflow	Freq	Pct%
Significantly increased	11	44%
Increased	7	28%
No change	7	28%
Decreased	0	0%
Significantly decreased	0	0%
Total	25	100%

Q15. False positive rates	Freq	Pct%
Significantly increased	0	0%
Increased	0	0%
No change	5	20%
Decreased	10	40%
Significantly decreased	10	40%
Total	25	100%

Q16. Average time to detect compromises	Freq	Pct%
Significantly increased	0	0%
Increased	0	0%
No change	5	20%
Decreased	12	48%
Significantly decreased	8	32%
Total	25	100%

Q17. Average time to contain compromises	Freq	Pct%
Significantly increased	0	0%
Increased	0	0%
No change	9	36%
Decreased	9	36%
Significantly decreased	7	28%
Total	25	100%

Q18. Frequency of data breach incidents	Freq	Pct%
Significantly increased	0	0%
Increased	1	4%
No change	15	60%
Decreased	5	20%
Significantly decreased	4	16%
Total	25	100%

Q19. Frequency of denial of service (DoS/DDoS) attacks	Freq	Pct%
Significantly increased	0	0%
Increased	0	0%
No change	18	72%
Decreased	7	28%
Significantly decreased	0	0%
Total	25	100%

Q20. Average duration of IT downtime caused by cyber attacks	Freq	Pct%
Significantly increased	0	0%
Increased	0	0%
No change	16	64%
Decreased	9	36%
Significantly decreased	0	0%
Total	25	100%

Q21. Average duration of business disruption caused by cyber attacks	Freq	Pct%
Significantly increased	0	0%
Increased	0	0%
No change	13	52%
Decreased	10	40%
Significantly decreased	2	8%
Total	25	100%

Q22. The total cost of downtime and business disruption caused by cyber attacks	Freq	Pct%
Significantly increased	0	0%
Increased	0	0%
No change	15	60%
Decreased	10	40%
Significantly decreased	0	0%
Total	25	100%

Q23. State of compliance with policies, regulations and external standards	Freq	Pct%
Significantly increased	0	0%
Increased	11	44%
No change	14	56%
Decreased	0	0%
Significantly decreased	0	0%
Total	25	100%

Q24. Organizational reputation or brand	Freq	Pct%
Significantly increased	0	0%
Increased	10	40%
No change	15	60%
Decreased	0	0%
Significantly decreased	0	0%
Total	25	100%

Q25. Please record your overall impressions of QRadar	Freq	Pct%
Very positive	13	52%
Positive	10	40%
Unsure	2	8%
Negative	0	0%
Very negative	0	0%
Total	25	100%

Q26. Does QRadar meet your expectations?	Freq	Pct%
Exceeds expectation	14	56%
Meets expectation	9	36%
Does not meet expectation	2	8%
Total	25	100%

Following are 25 separately compiled ROI and TCO estimates for QRadar

Case	ROI	TCO
C1	18%	$540,000
C2	52%	$390,000
C3	58%	$950,000
C4	49%	$950,000
C5	44%	$950,000
C6	66%	$1,700,000
C7	58%	$1,700,000
C8	65%	$540,000
C9	20%	$2,100,000
C10	31%	$1,700,000
C11	32%	$2,540,000
C12	40%	$950,000
C13	32%	$950,000
C14	61%	$390,000
C15	35%	$3,800,000
C16	54%	$950,000
C17	40%	$3,750,000
C18	37%	$1,700,000
C19	49%	$1,300,000
C20	25%	$450,000
C21	11%	$2,540,000
C22	51%	$900,000
C23	21%	$3,800,000
C24	18%	$2,100,000
C25	36%	$690,000
Average	40%	$1,533,200

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 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.