Exabeam SIEM Productivity Study

Sponsored by Exabeam

Independently conducted by Ponemon Institute LLC

Publication Date: July 2019

Exabeam SIEM Productivity Study

Ponemon Institute, July 2019

Part 1. Executive Summary

With sponsorship from Exabeam, Ponemon Institute surveyed 596 IT and IT security practitioners of which 42 self-report that their organization uses Exabeam as its primary SIEM provider. The purpose of this study is to understand how Exabeam's SIEM solution compares to other SIEM solutions in terms of saving time and increasing productivity, realizing value and improving security effectiveness.

SIEM or Security Information and Event Management solutions use rules and statistical correlations to turn log entries and events from security systems into actionable information. This information can help security teams detect threats in real time, manage incident response, perform forensic investigation on past security incidents and prepare audits for compliance purposes. All respondents are familiar with their organization's SIEM deployment and are involved in the detection, investigation and/or remediation of security threats inside its network.

Saving Time and Increasing Productivity

Table 1 compares Exabeam to other SIEM solutions with respect to the time saved for a variety of core cybersecurity activities. According to the findings, following deployment Exabeam users reduced the total time by 51 percent. In contrast, users of other SIEM solutions were able to reduce the total time by less than one-third (31 percent). Please note that results may be skewed because of the participation of organizations with large cybersecurity teams.

Table 1. Exabeam reduces time to complete cybersecurity tasks

Core cybersecurity activities (average hours spent per week)	Exabeam Before	Exabeam After	% Reduced	SIEM* Before	SIEM* After	% Reduced
Organizing and planning the detection and evaluation of suspicious and/or anomalous events	194	88	55%	189	126	33%
Gathering actionable intelligence about cyber threats and vulnerabilities	173	95	45%	185	146	21%
Evaluating actionable intelligence	173	85	51%	169	127	25%
Investigating actionable intelligence and building incident timelines	259	125	52%	250	153	39%
Cleaning, fixing and/or patching networks, applications and devices as a result of an incident	295	157	47%	287	208	28%
Documenting security incidents	126	62	51%	130	82	37%
Chasing alerts or IOCs that are erroneous	441	202	54%	424	286	33%
Totals	1,661	814	51%	1,634	1,128	31%

*Includes all market-leading SIEM solutions (excluding Exabeam)

Realizing Value

A key takeaway from this research is that Exabeam's value is quickly realized. Specifically, 92 percent of Exabeam respondents were able to see its value within a week after deployment versus 53 percent of users of other SIEM solutions. Reduction of operational costs is equally impressive. Ninety percent of Exabeam respondents say Exabeam is highly effective at reducing the operational costs associated with using a SIEM for detection and investigation. This is twice as many as respondents whose organization use other SIEM solutions. Similarly, Exabeam is able to reduce the number of security point products used and the need to buy professional services.

Improving Security Effectiveness

Improvements in the effectiveness of the IT security team is a reason organizations see value in a short period of time. According to the study, Exabeam users are able to significantly improve the effectiveness of their security operations, with 95 percent of Exabeam respondents saying it is an effective solution for detection and investigation. Specifically, Exabeam effectively prioritizes alerts, allowing analysts to investigate 83 percent of daily alerts versus 45 percent for other SIEMs.

Eighty-five percent of respondents also say that Exabeam is effective at reducing the number of false positives. As a result, only 10 percent of alerts in Exabeam are false positives compared to 33 percent for other SIEMs. Exabeam's user-based licensing, model, detection tools (out-of-the box correlation rules and machine learning-based models) and the ability to customize those tools are other notable contributors to the effectiveness of Exabeam compared to other solutions.

Part 2. Key findings

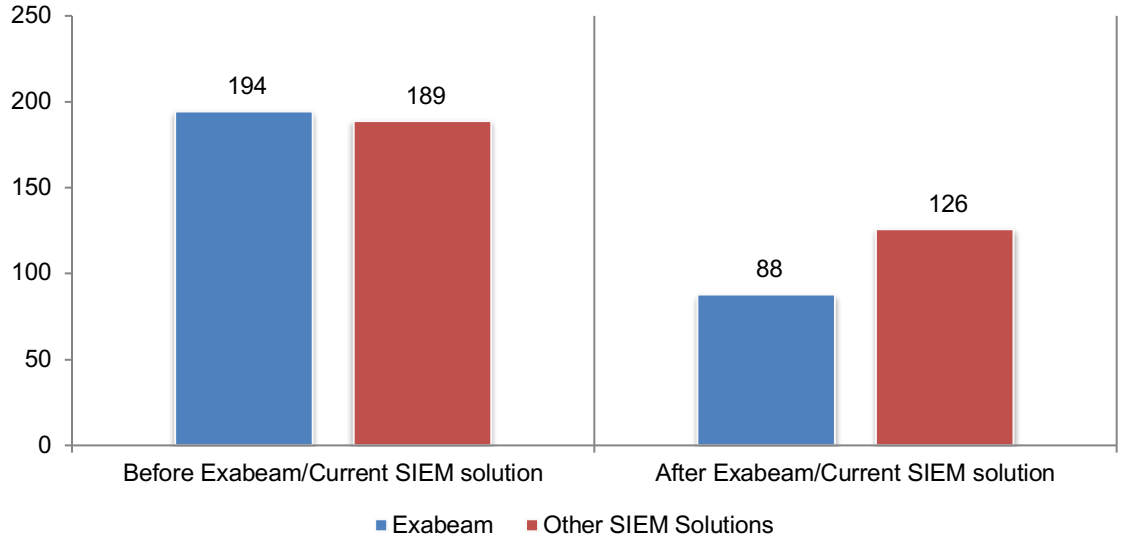
In this section, we provide an analysis of the research findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics:

- Saving Time and Increasing Productivity
- Realizing Value
- Improving Security Effectiveness

Saving Time and Increasing Productivity

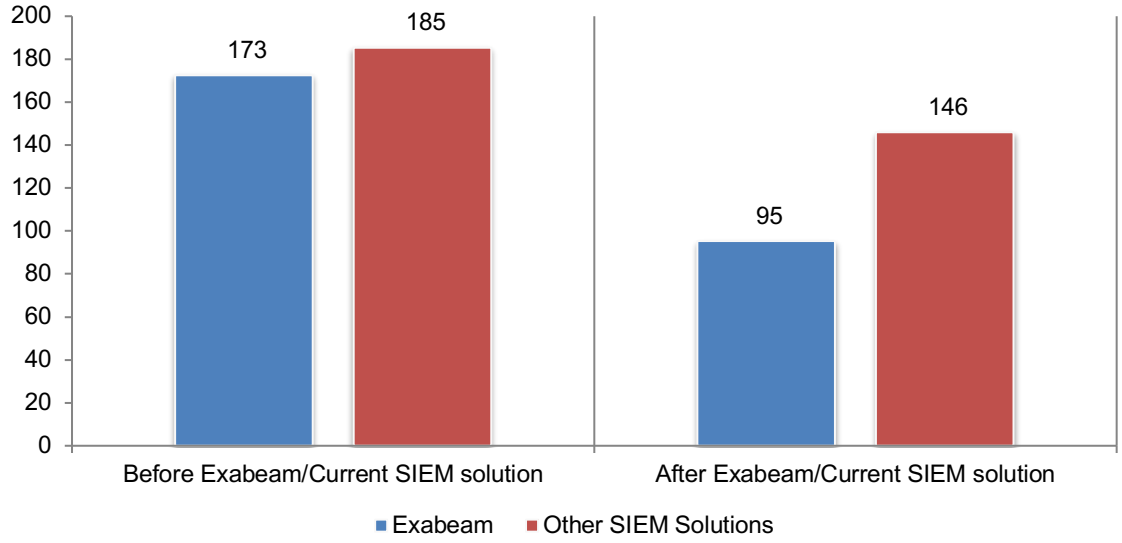
SIEM solutions reduce the average time spent organizing and planning the detection and evaluation of suspicious and/or anomalous events. According to Figure 1, Exabeam users were able to save an average of 106 hours (194-88) and users of other SIEM solutions saved 63 hours (189-126).

Figure 1. Average hours spent each week organizing and planning the detection and evaluation of suspicious and/or anomalous events
Extrapolated values presented



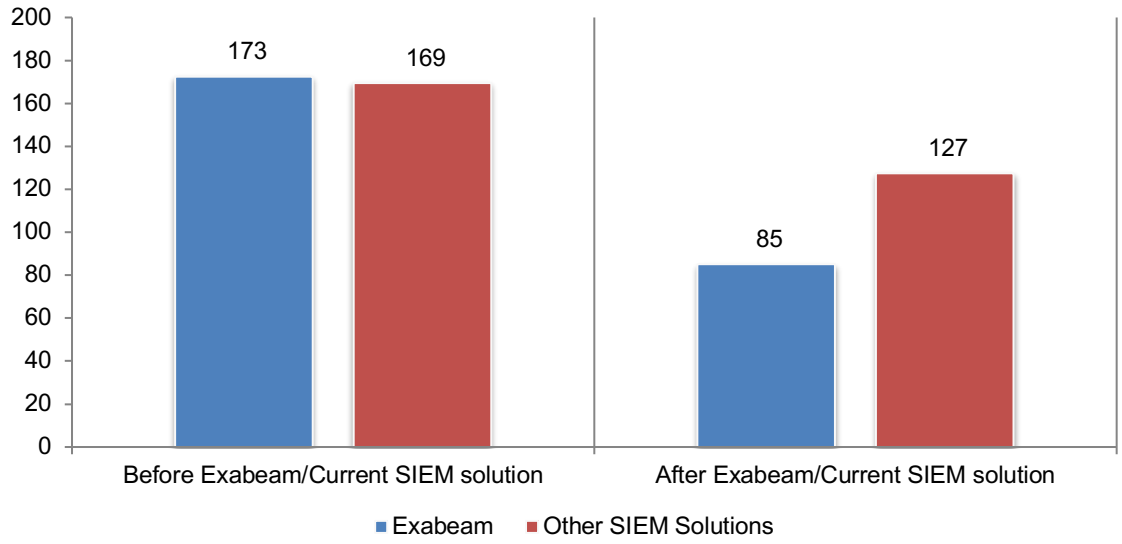
Exabeam users saved an average of 78 hours (173-95) gathering actionable intelligence about cyber threats and vulnerabilities and users of other SIEM solutions saved 39 hours each week (185-146), as shown in Figure 2.

Figure 2. Average hours spent each week gathering actionable intelligence about cyber threats and vulnerabilities
Extrapolated values presented



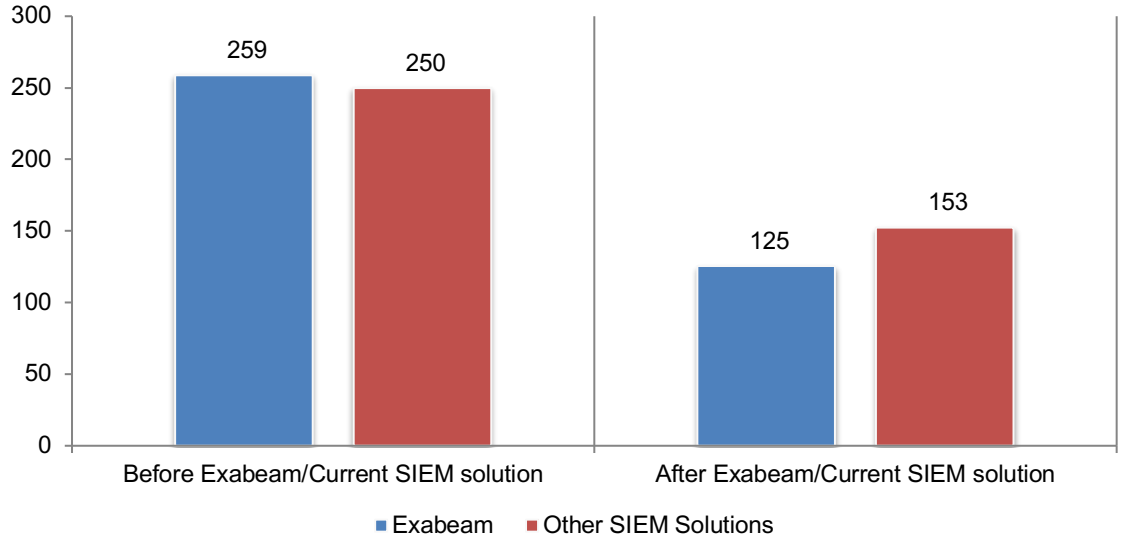
Exabeam users saved a significant amount of time evaluating actionable intelligence. As shown in Figure 3, Exabeam users saved an average of 88 hours per week evaluating actionable intelligence (173-85). The average hours saved by users of other SIEM solutions is 42 hours (169-127).

Figure 3. Average hours spent each week evaluating actionable intelligence
Extrapolated values presented



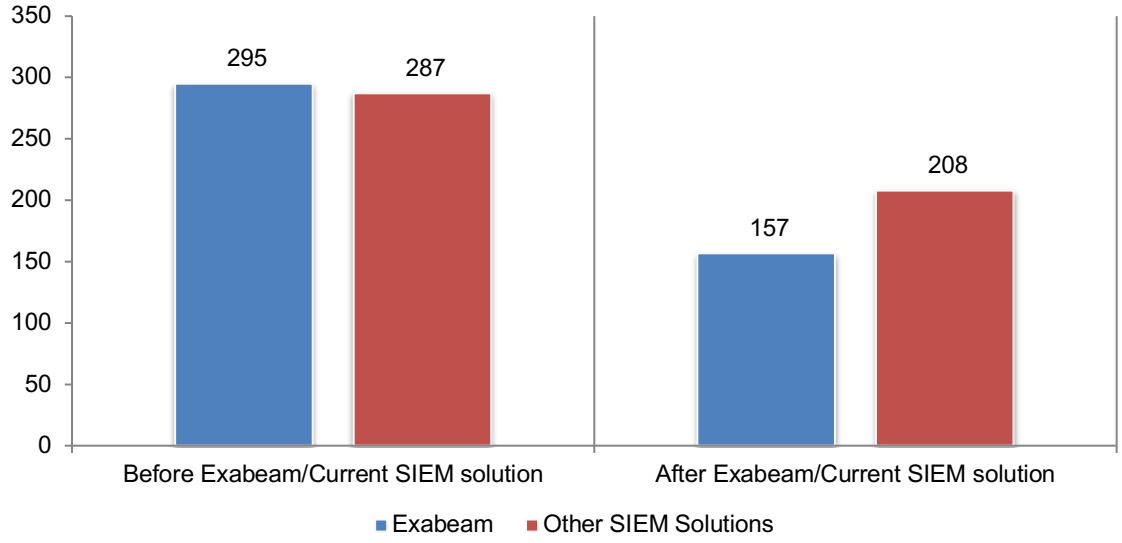
SIEM reduces the hours spent each week investigating actionable intelligence and building incident timelines. According to Figure 4, Exabeam and users of other SIEM solutions saved an average of 134 hours (259-125) and 97 hours (250-153), respectively.

Figure 4. Average hours spent each week investigating actionable intelligence and building incident timelines
Extrapolated values presented



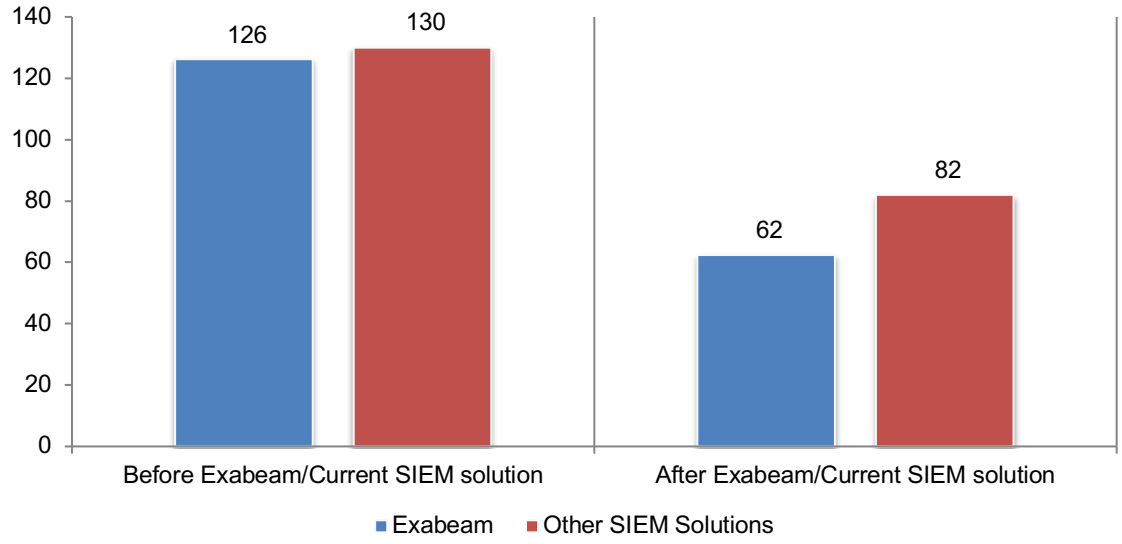
Exabeam significantly reduces the time spent cleaning fixing and/or patching networks. According to Figure 5, Exabeam users report that following the deployment their organizations were able to save 138 hours weekly (295-157). Other SIEM solutions reduced the time by an average of 79 hours (287-207).

Figure 5. Average hours spent each week cleaning, fixing and/or patching networks, applications and devices as a result of an incident
Extrapolated values presented



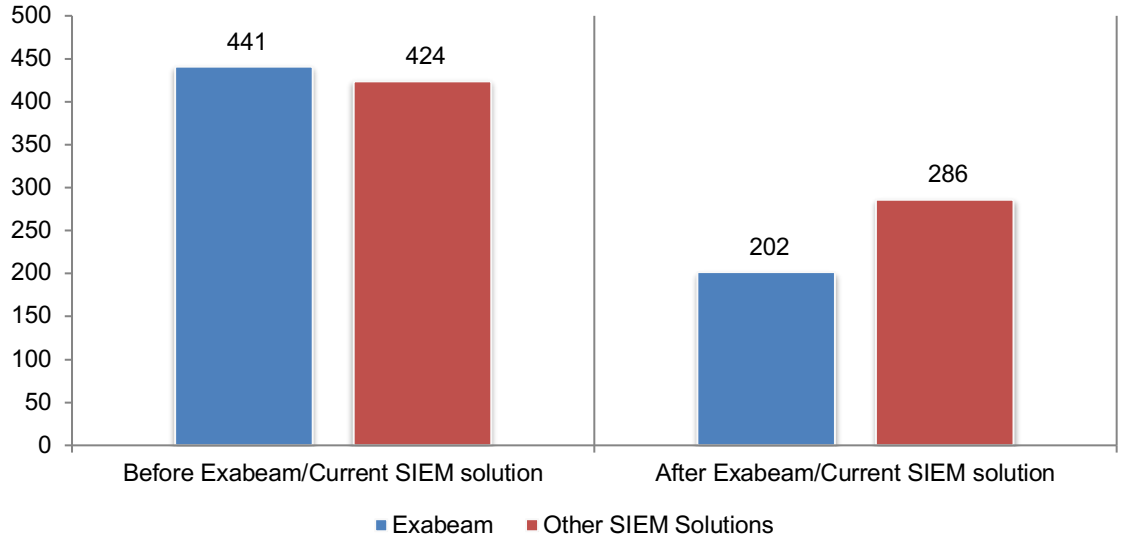
The average time spent each week documenting security incidents was reduced by an average of 64 hours (126-62) and 48 hours (130-82), as shown in Figure 6.

Figure 6. Average hours spent each week documenting security incidents
Extrapolated values presented



Security personnel are more efficient following deployment of Exabeam and other SIEM solutions. According to Figure 7, security teams using Exabeam and other SIEM solutions reduce the amount of wasted time spent chasing erroneous alerts or IOCs (Exabeam 239 hours saved and other SIEM solutions 138 hours).

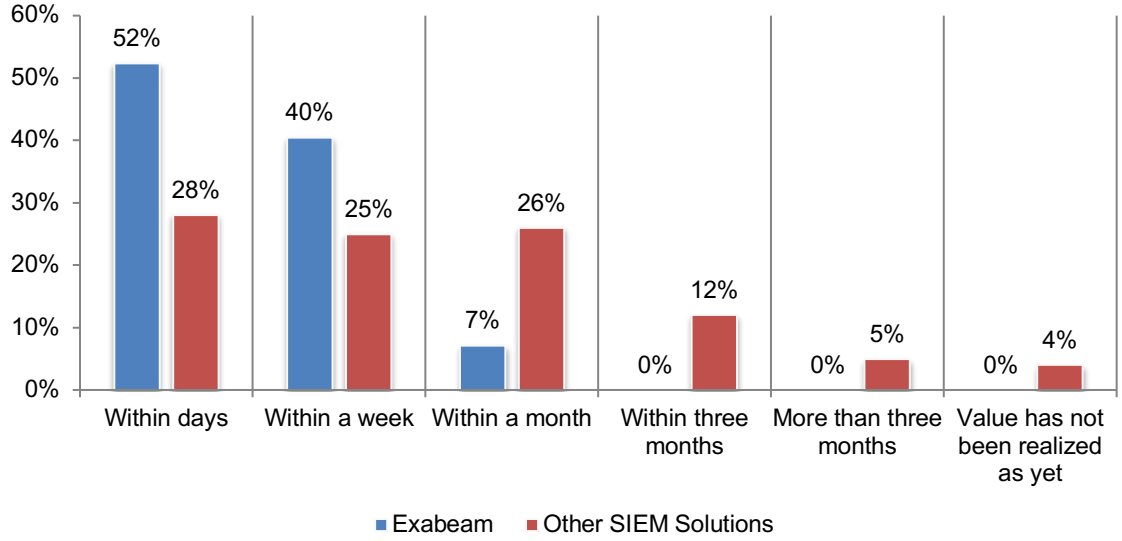
Figure 7. Average hours wasted by security personnel because alerts or IOCs they chase are erroneous
Extrapolated values presented



Realizing Value

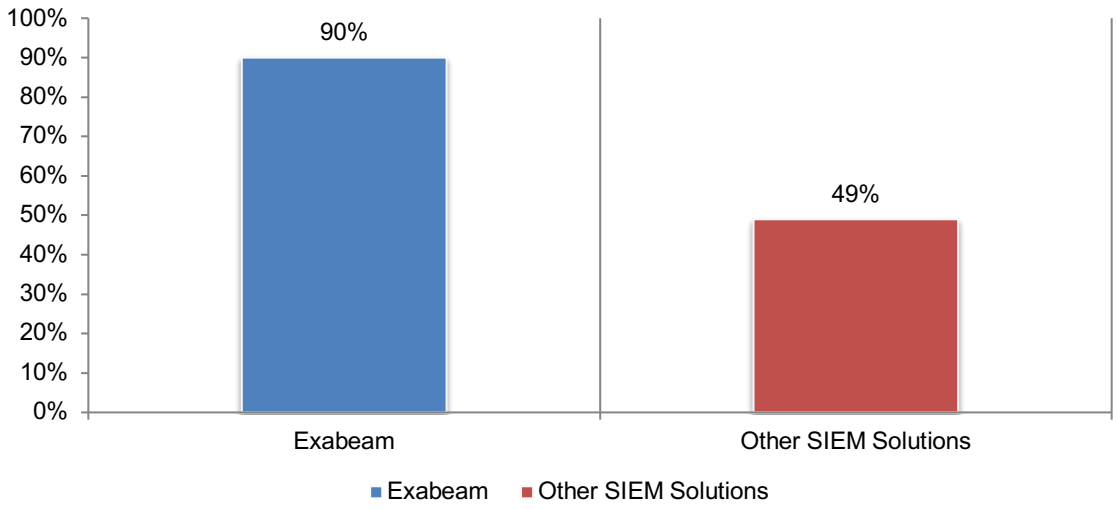
The value of Exabeam is seen within a week. Following deployment, 92 percent of respondents say the time to realize the value of the SIEM is within days (52 percent) or within a week (40 percent). In contrast, 53 percent of users were able to see the value during the same time period.

Figure 8. How long did it take your organization to realize value from its Exabeam solution?



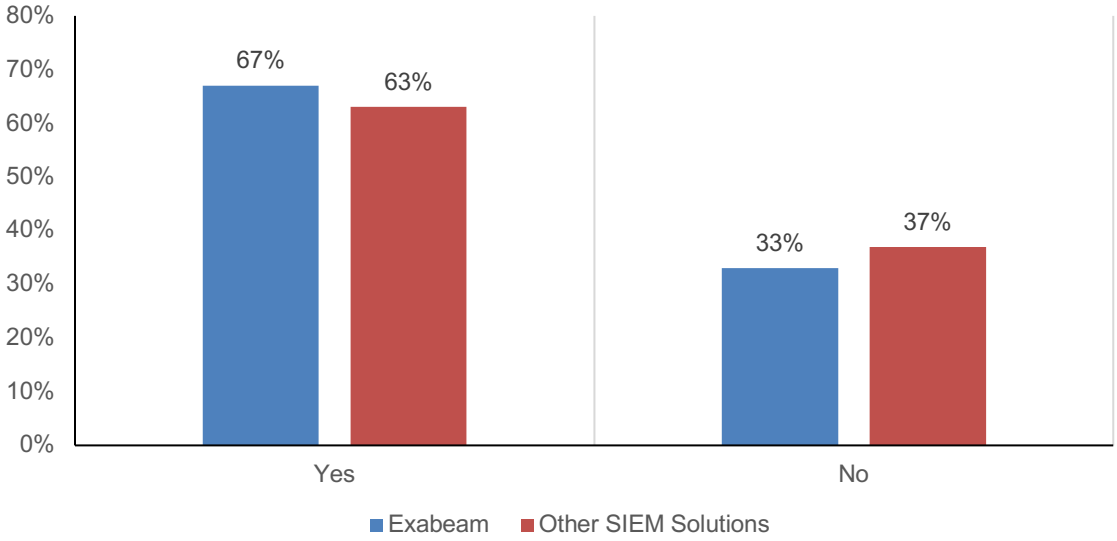
Exabeam users report they are able to reduce the cost of using a SIEM. Respondents were asked to rate the effectiveness in minimizing the costs associated with using their SIEM to detect and investigate cyberattacks on a scale from 1 = not effective to 10 = highly effective. Figure 9 shows the highly effective (7+) responses. High effectiveness is almost double among Exabeam users when compared to other SIEM solutions.

Figure 9. Effectiveness in minimizing the costs associated with using your SIEM to detect and investigate cyberattacks
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



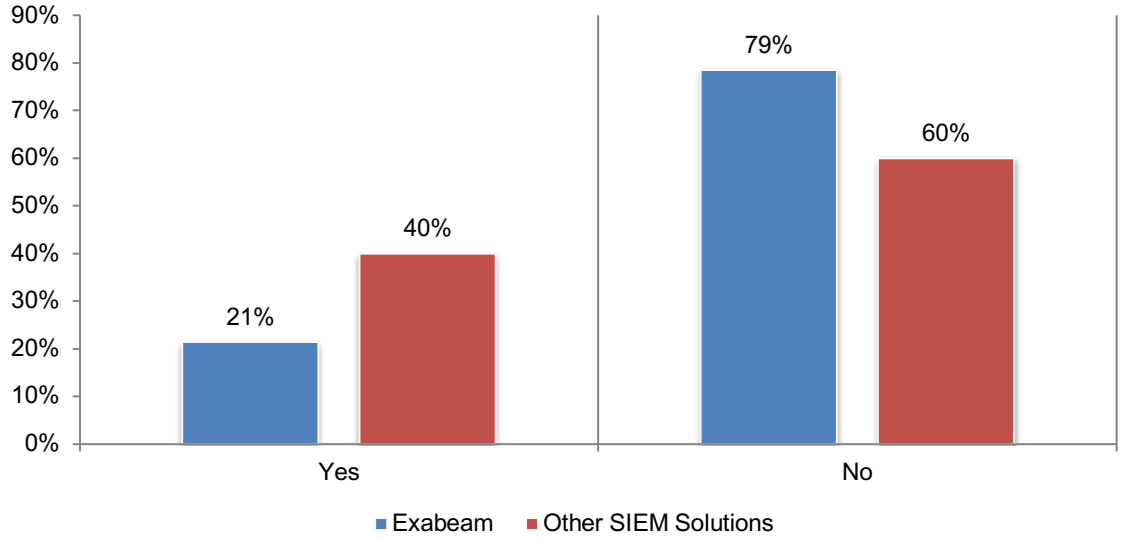
SIEM solutions enable organizations to replace point security solution products. According to Figure 10, most respondents say their organizations were able to replace point security solution products. Exabeam users say they replaced an average of 7 point security solutions and users of other SIEM solutions replaced an average of 5 point security solutions.

Figure 10. Was your organization able to replace any point security solution products?



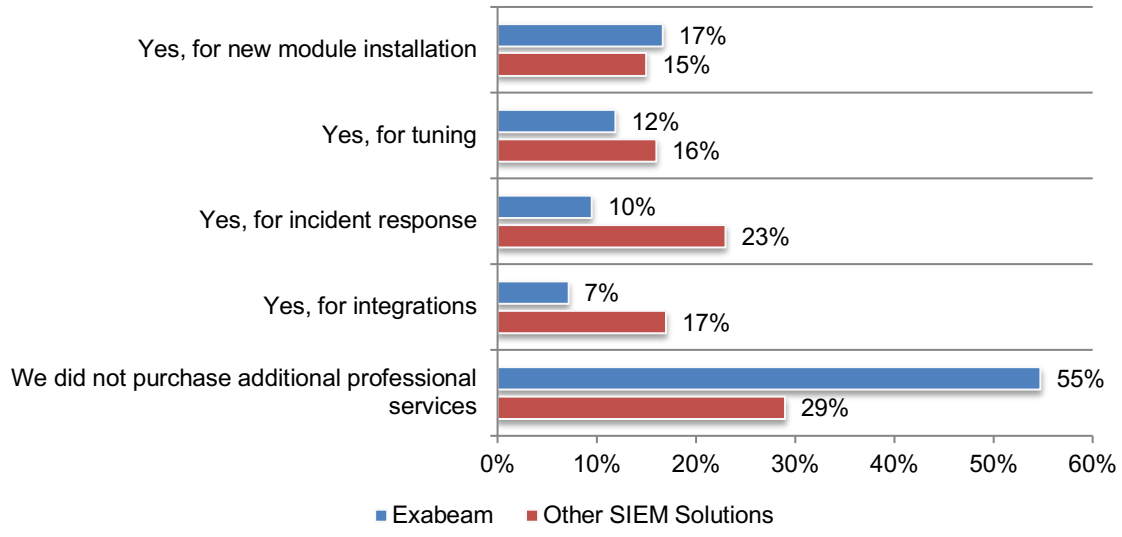
Exabeam requires fewer professional services to help with the SIEM deployment. According to Figure 11, only 21 percent of Exabeam users engaged professional services to help with its deployment. Respondents in organizations that use other SIEM solutions were more likely to hire a professional services firm to assist with deployment.

Figure 11. Did your organization purchase any professional services to help with the SIEM deployment?



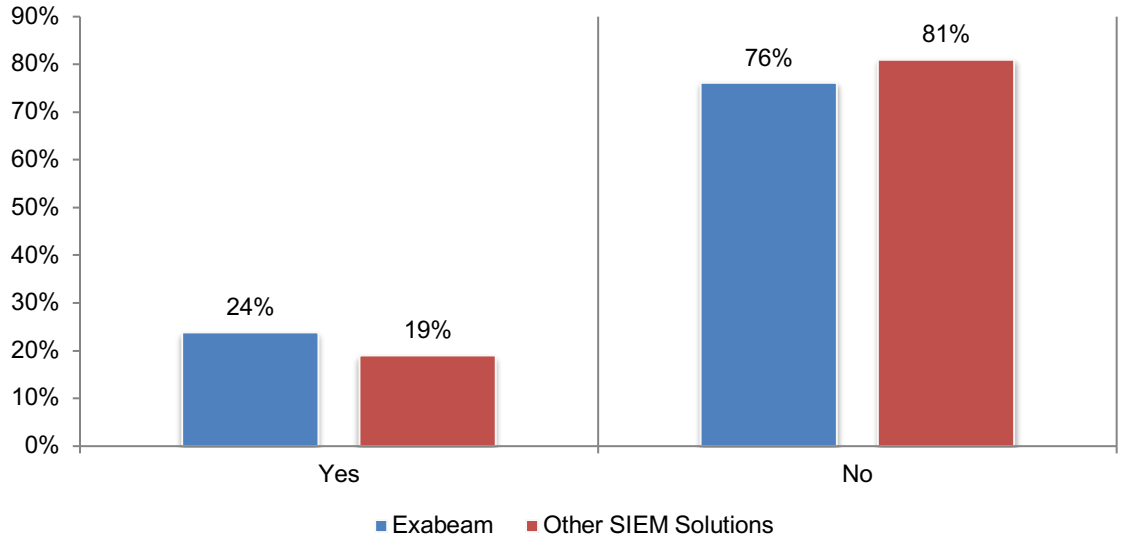
Further, Exabeam users are less likely to purchase additional professional services, as shown in Figure 12.

Figure 12. Has your organization purchased any additional profession services to assist since your SIEM was implemented?



SIEM solutions do not help reduce headcount costs. According to Figure 13, few organizations represented in this research were able to reduce the staff needed to deal with daily security incidents.

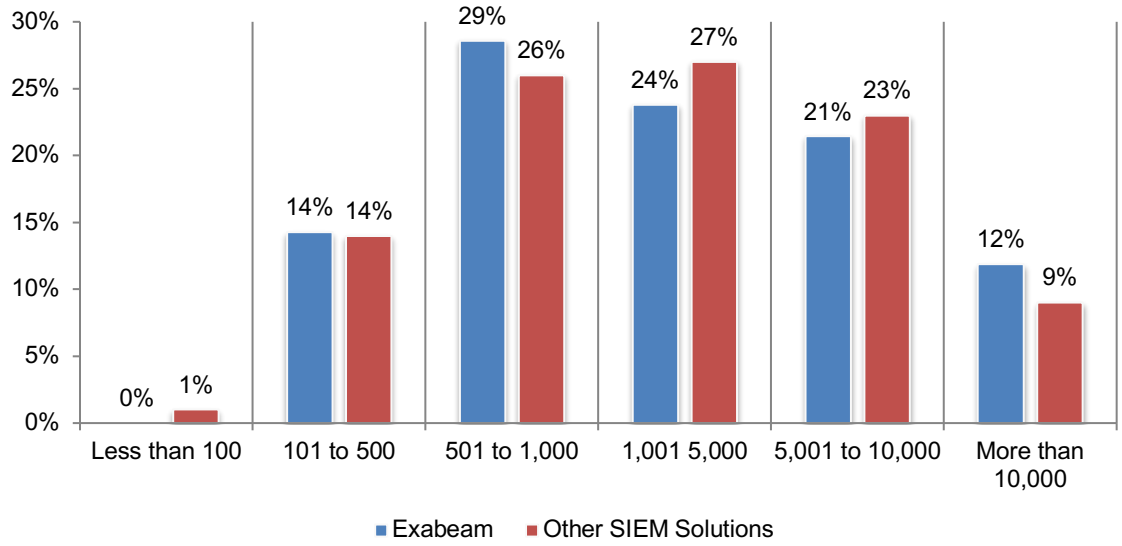
Figure 13. Did the use of SIEM help reduce headcount costs with daily security incident investigations?



Improving Security Effectiveness

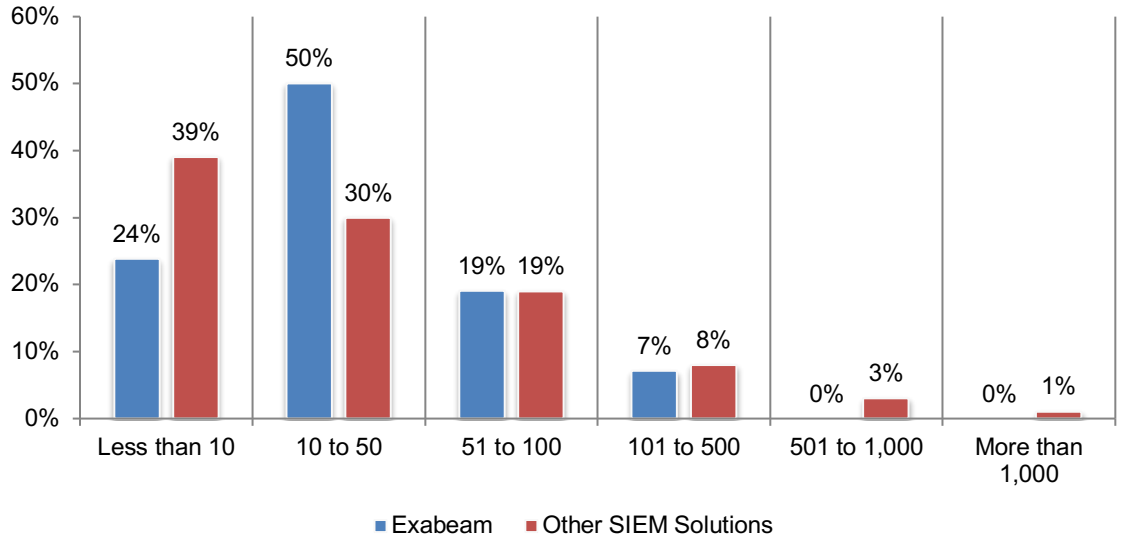
All organizations detect a similar amount of attacks each week. As shown in Figure 14, 57 percent of Exabeam respondents and 59 percent of respondents with other SIEM solutions say their organizations experienced more than 1,000 attacks each week.

Figure 14. How many actual attacks does your organization see any given week?
Extrapolated value: Exabeam 4,007 attacks
Extrapolated value: Other SIEM solutions 3,853



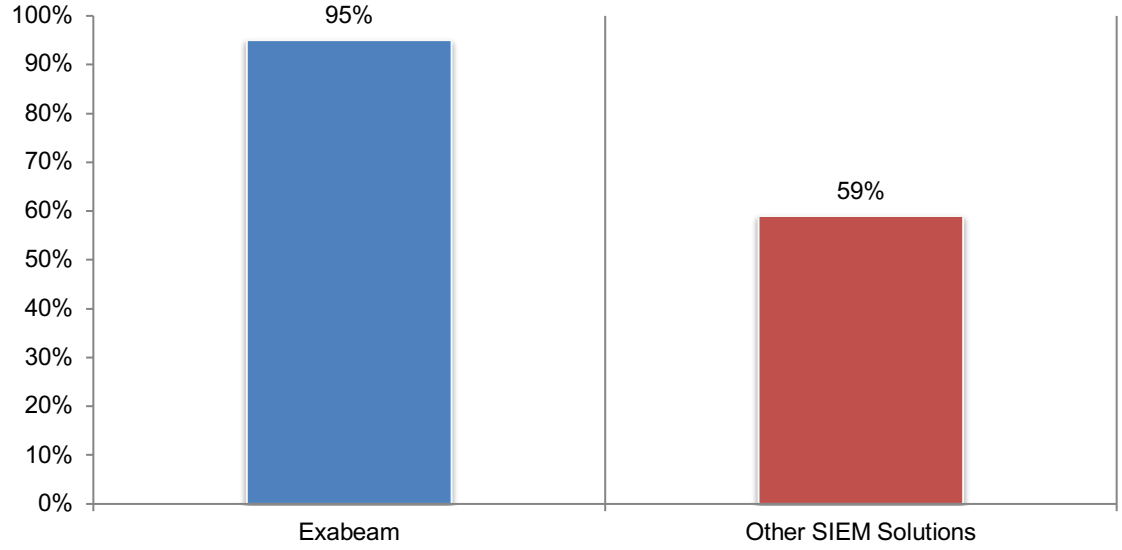
In the past 12 months, 74 percent of Exabeam respondents report having less than 10 to 50 security breaches in the past 12 months. Similarly, 69 percent of respondents with other SIEM solutions had the same range of data breaches, as shown in Figure 15.

Figure 15. How many known security breaches did your organization have in the past 12 months?



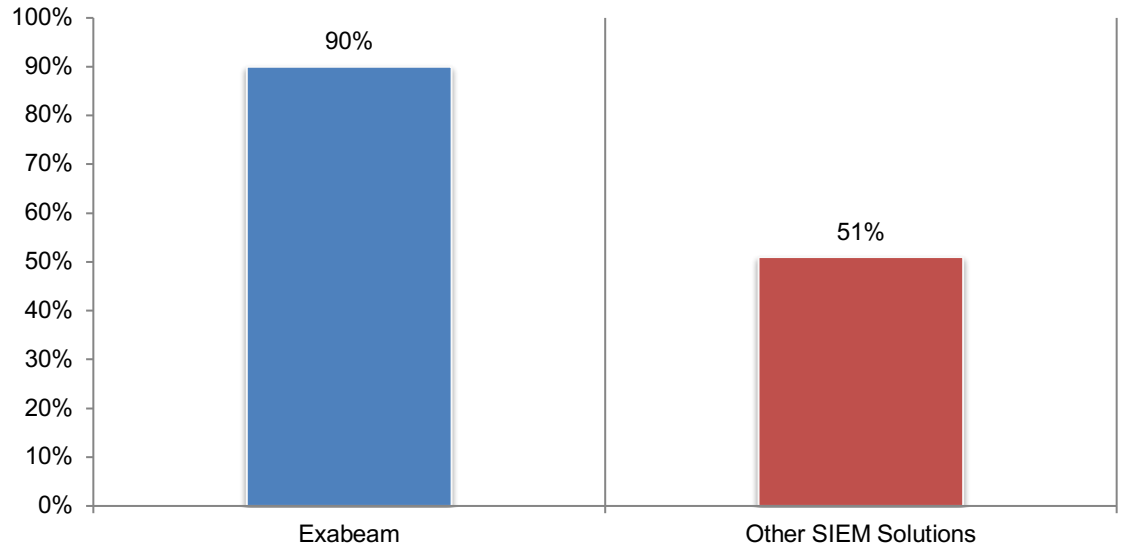
Exabeam is more effective in detecting and investigating cyberattacks. Respondents were asked to rate the effectiveness of their SIEM in detecting and investigating cyberattacks on a scale of 1 = not effective to 10 = highly effective. Figure 16 presents the highly effective responses and the effectiveness in detecting and investigating cyberattacks for the Exabeam solution is much higher (95 percent of Exabeam respondents versus 59 percent of other SIEM solutions).

Figure 16. Effectiveness in detecting and investigating cyberattacks
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



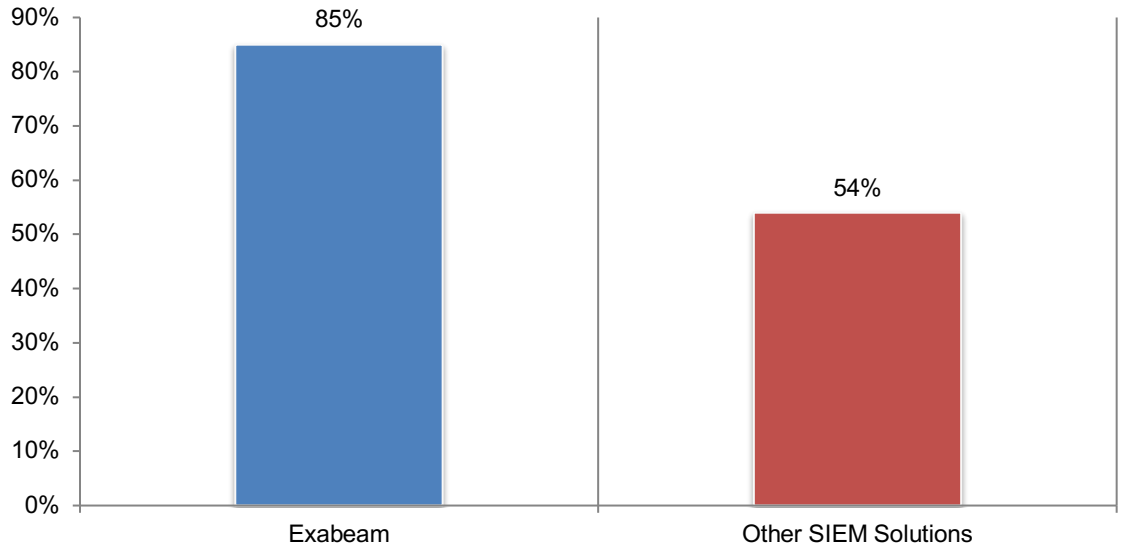
A benefit of Exabeam is the ability to prioritize alerts. Respondents were asked to rate the effectiveness of their SIEM solution in prioritizing alerts on a scale from 1 = not effective to 10 = highly effective. Figure 17 shows the highly effective responses (7+ responses). Almost all Exabeam users (90 percent) say they are highly effective in prioritizing alerts that pose a significant cyber risk.

Figure 17. Effectiveness in prioritizing alerts that pose significant cyber risk
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



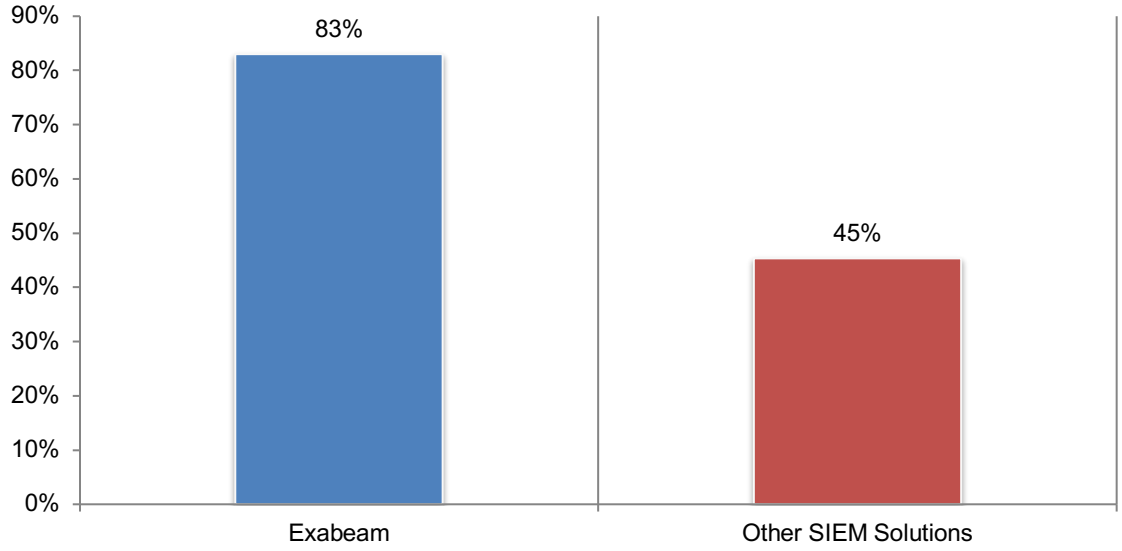
Similarly, 85 percent of Exabeam users rate their organizations as highly effective in minimizing false positives, as shown in Figure 18.

Figure 18. Effectiveness in minimizing false positives when using SIEM to detect and investigate cyberattacks
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



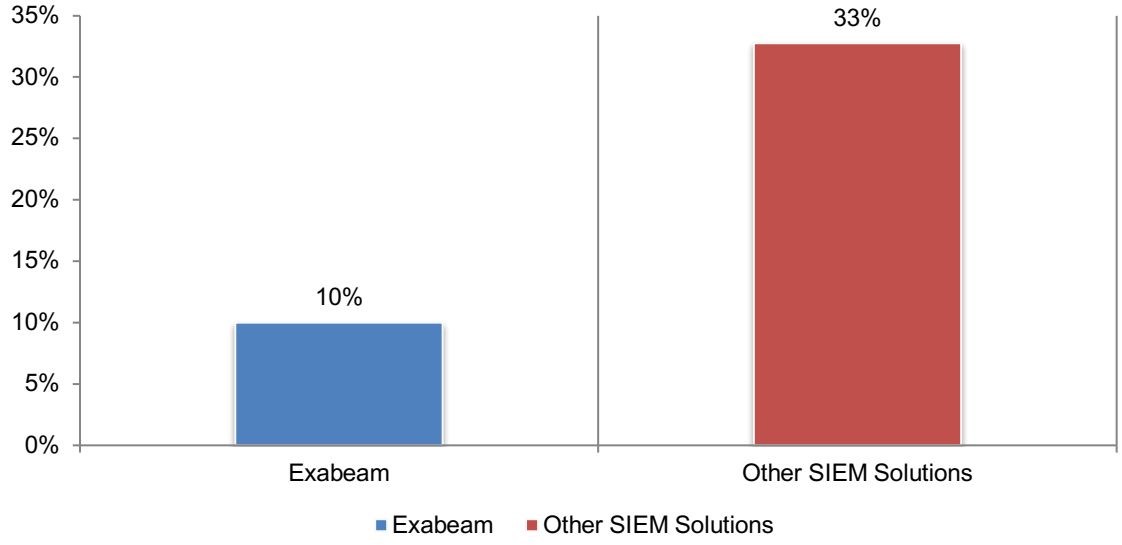
Exabeam users have a higher average of daily alerts to investigate than users of other SIEM solutions. According to Figure 19, Exabeam users have an average of 83 percent of alerts to investigate. Users of other SIEM solutions report an average of 45 percent of alerts to investigate.

Figure 19. Percentage of daily alerts in your SIEM you are able to investigate
Extrapolated values



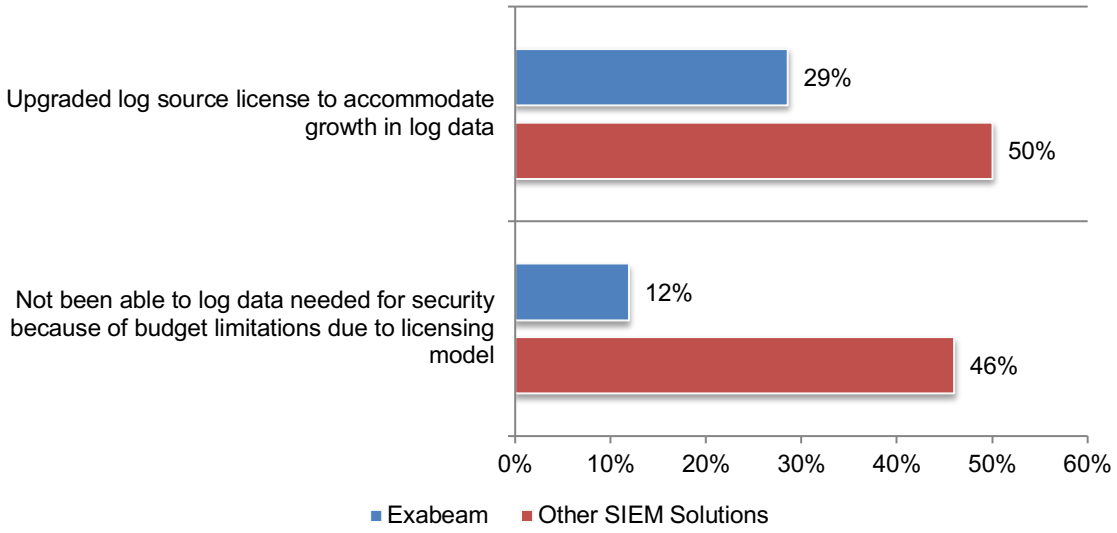
Exabeam users also have fewer false positives. According to Figure 20, only 10 percent of all alerts are false positive versus 33 percent in other SIEM solutions.

Figure 20. Percentage of alerts in your SIEM that are false positive
Extrapolated values presented



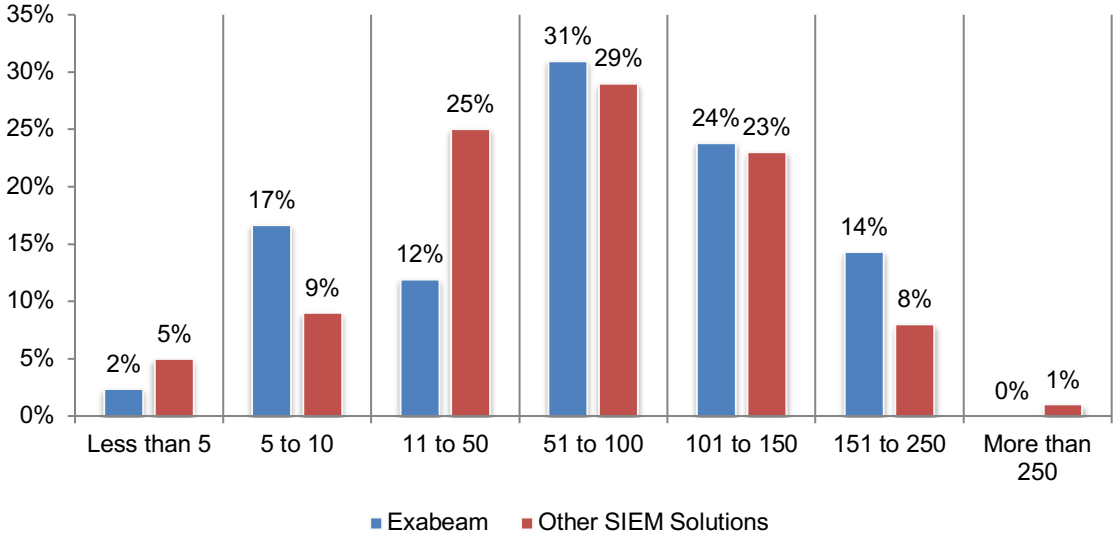
The licensing model for Exabeam is more efficient. Fewer Exabeam users need to upgrade their log source license to deal with growth in log data and deal with budget limitations. According to Figure 21, 50 percent of respondents with other SIEM solutions have had to upgrade their log source license because of growth in log data and 46 percent of these respondents have not been able to log data needed for security because of budget limitations due to the licensing model.

Figure 21. Did you upgrade your log source license to accommodate growth in log data and were you not able to log data you needed for security because of the licensing model?
Yes responses presented



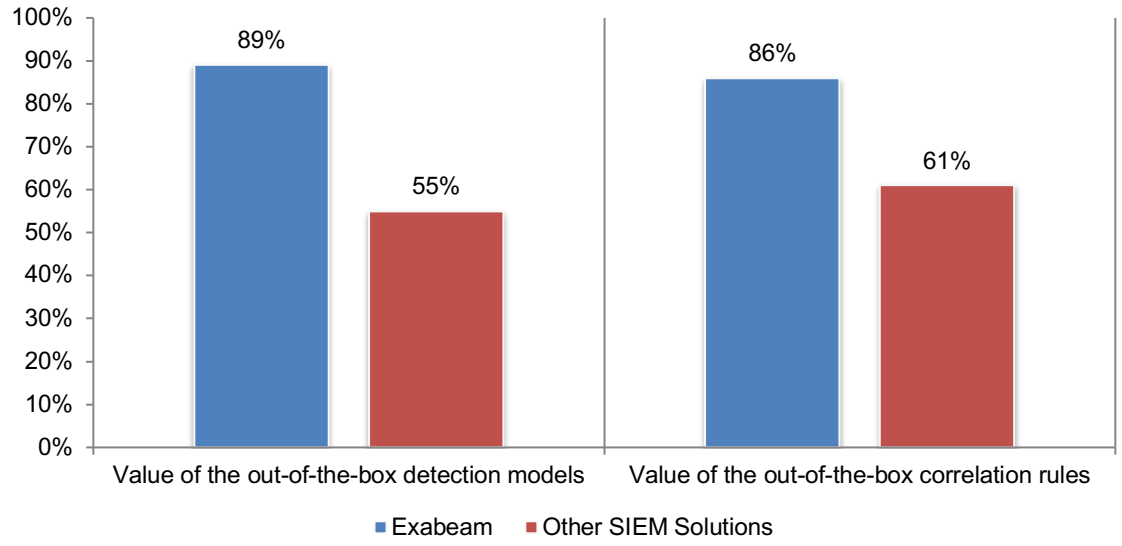
Exabeam organizations use more data sources to detect attacks. Respondents were asked how many data sources are used to detect attacks. On average, Exabeam organizations use an average of 86 data sources and users of other SIEM solutions use an average of 78, as shown in Figure 22.

Figure 22. How many data sources does your organization use to detect attacks?
Extrapolated average value for Exabeam = 86
Extrapolated average value for Other SIEM solutions = 78



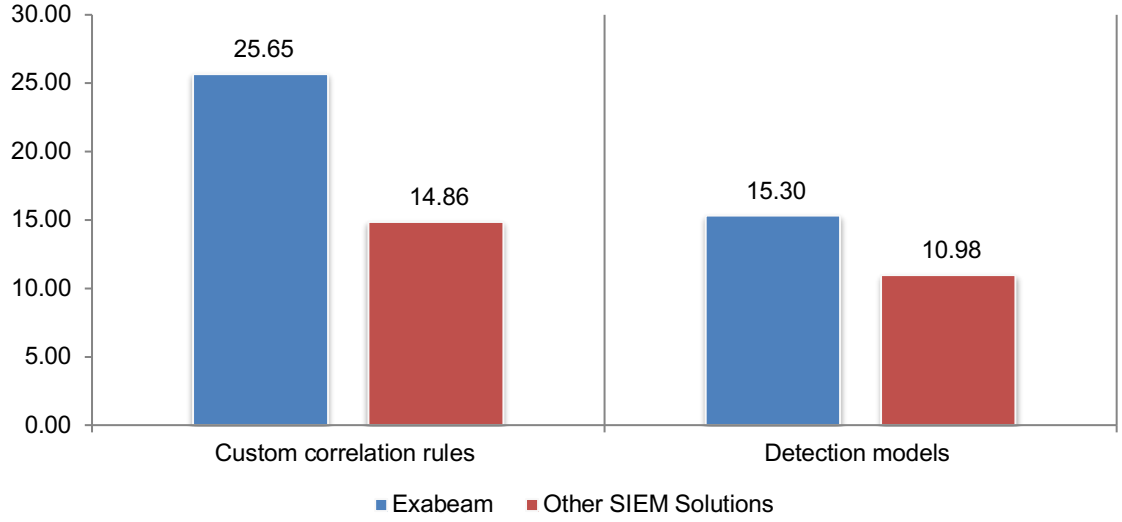
Exabeam users find out-of-the-box correlation rules and detection models more valuable than other SIEM solutions. Respondents were asked to rate the value of out-of-the-box correlation rules and detection models on a scale of 1 = not valuable to 10 = very valuable. As shown in Figure 23, 86 percent and 89 percent of Exabeam respondents find out-of-the-box correlation rules and detection models very valuable.

Figure 23. How valuable are out-of-box correlation rules and detection models?
On a scale from 1 = not valuable at all to 10 = very valuable, 7+ responses



Exabeam respondents create more custom correlation rules and detection models than users of other SIEM solutions. As shown in Figure 24, the average custom correlation values created by Exabeam users is approximately 26 versus approximately 15 for other SIEM solution users. Similarly, Exabeam users created an average of 15 detection models versus 11 created by other SIEM solution users.

Figure 24. How many custom correlation rules and detection models have you developed?
Extrapolated values presented



Part 3. Methods

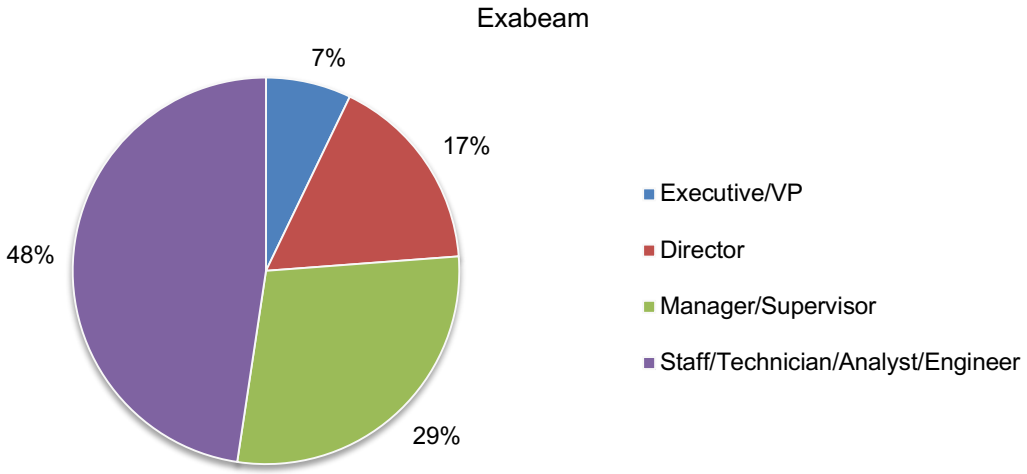
A sampling frame of 16,446 experienced IT and IT security practitioners located in the United States were selected as participants to this survey. Table 2 shows 647 total returns. Screening and reliability checks required the removal of 51 surveys. Our final sample consisted of 596 surveys (3.6 percent response rate). The final sample included a subsample of 42 Exabeam customers.

Since we collected from two separate samples we calculate a margin of error for the larger sample of SIEM users at 4.69 percent at the 95 percent level of confidence. The margin error for the much smaller subsample of Exabeam users is 6.12 percent.

Table 2. Sample response	FY2018
Total sampling frame	16,446
Total returns	647
Rejected or screened surveys	51
Final sample	596
Exabeam subsample	42
Response rate	3.6%

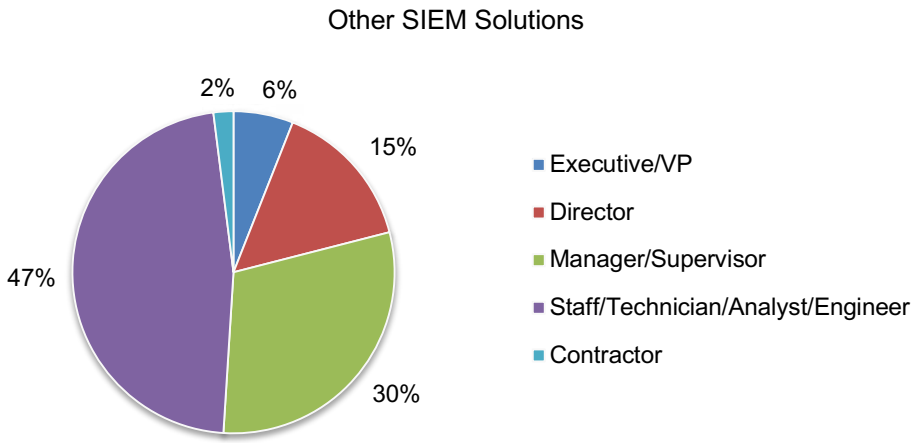
Pie Chart 1 reports the Exabeam respondents' position in participating organizations. By design, more than half of respondents (52 percent) are at or above the supervisory levels and 48 percent of respondents reported their position as staff/technician/analyst/engineer.

Pie Chart 1. Current position of Exabeam respondent within the organization



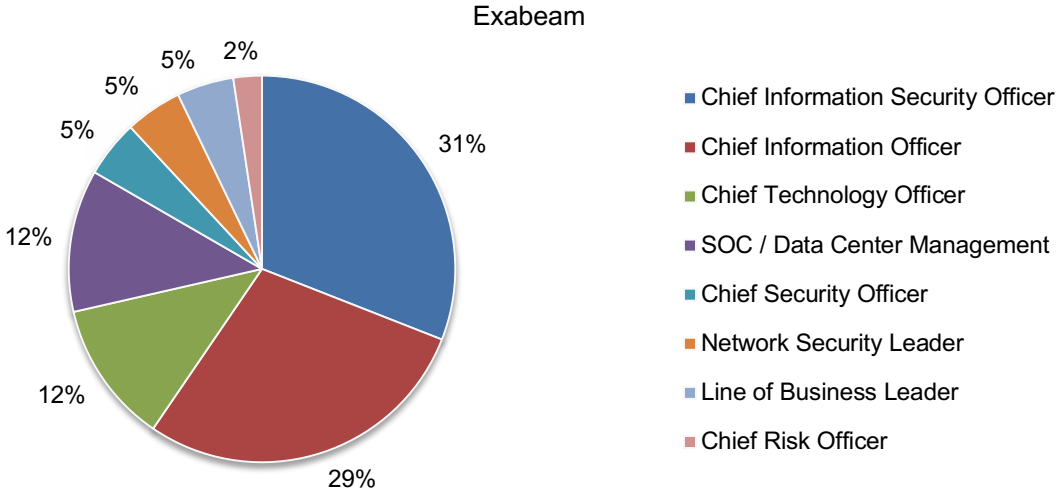
Pie Chart 2 reports the other SIEM solution respondents' position in participating organizations. By design, more than half of respondents (51 percent) are at or above the supervisory levels and 47 percent of respondents reported their position as staff/technician/analyst/engineer.

Pie Chart 2. Current position of other SIEM solution respondent within the organization



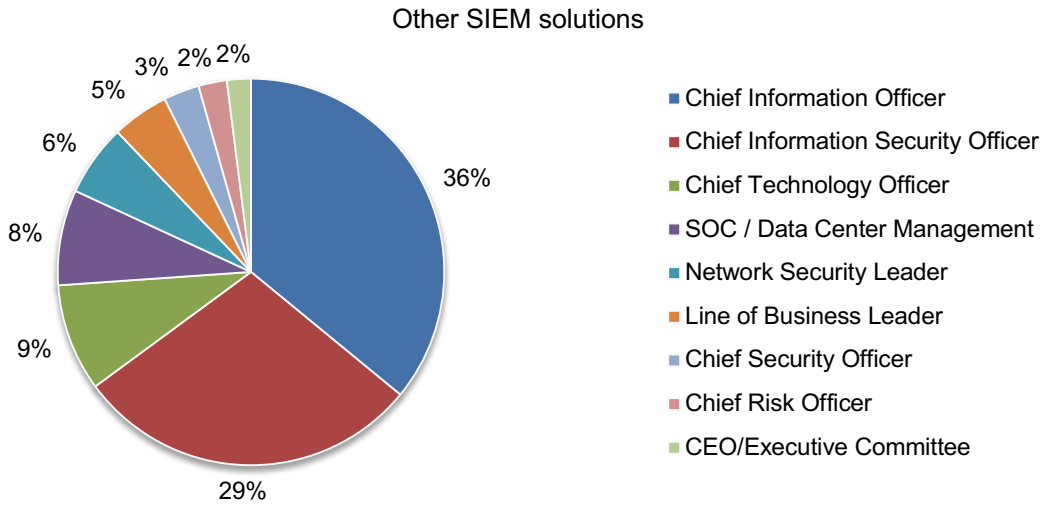
As shown in Pie Chart 3, 31 percent of Exabeam respondents report to the chief information security officer, 29 percent of respondents report to the chief information officer, 12 percent of respondents report to the chief technology officer and another 12 percent report to the SOC/data center management.

Pie Chart 3. Primary person Exabeam respondent or IT security leader reports to



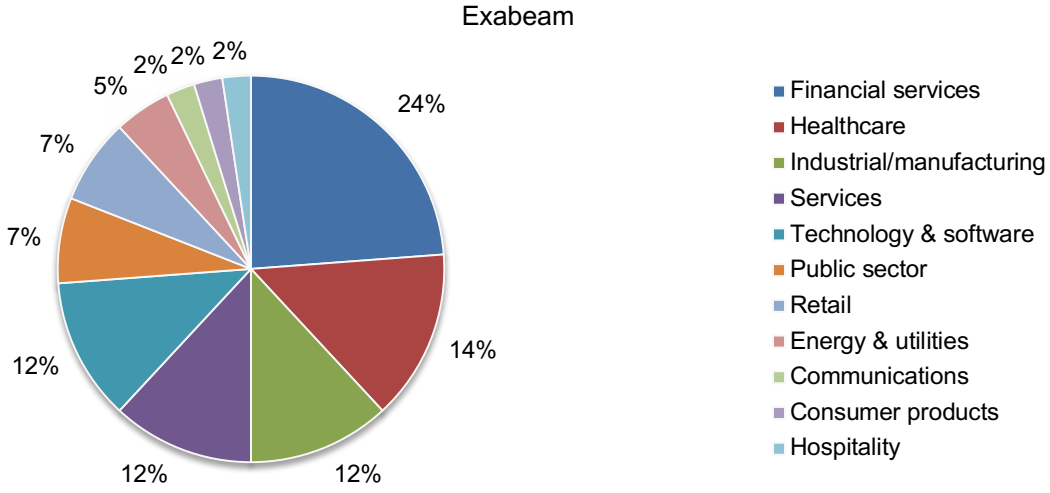
As shown in Pie Chart 4, 36 percent of other SIEM solution respondents report to the chief information officer, 29 percent of respondents report to the chief information security officer and 9 percent of respondents report to the chief technology officer.

Pie Chart 4. Primary person other SIEM solution respondent or IT security leader reports to



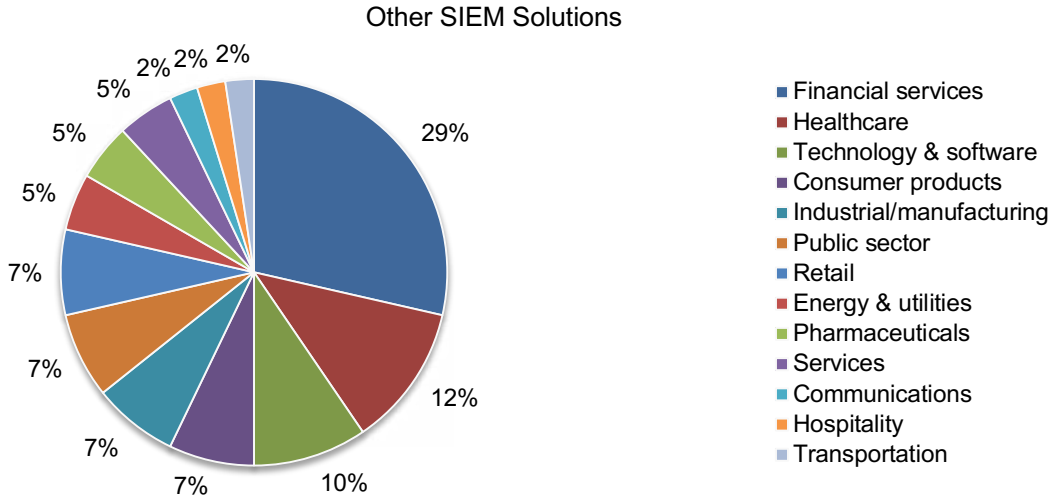
According to Pie Chart 5, financial services (24 percent of respondents), healthcare (14 percent of respondents) and industrial/manufacturing (12 percent of respondents) are the industries most represented in the Exabeam respondent sample.

Pie Chart 5. Industry focus of Exabeam respondents' organizations



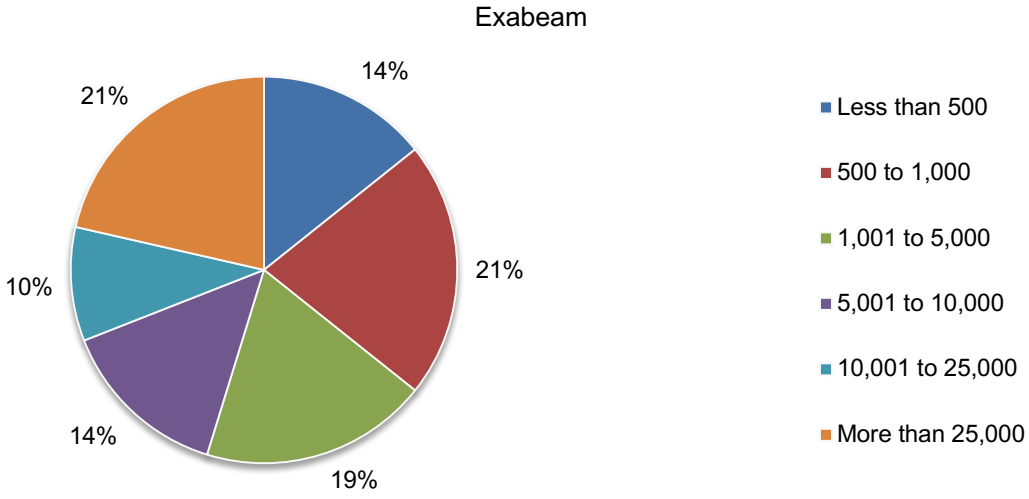
According to Pie Chart 6, financial services (29 percent of respondents), healthcare (12 percent of respondents) and technology and software (10 percent of respondents) are the industries most represented in the other SIEM solution respondent sample.

Pie Chart 6. Industry focus of other SIEM solution respondents' organizations



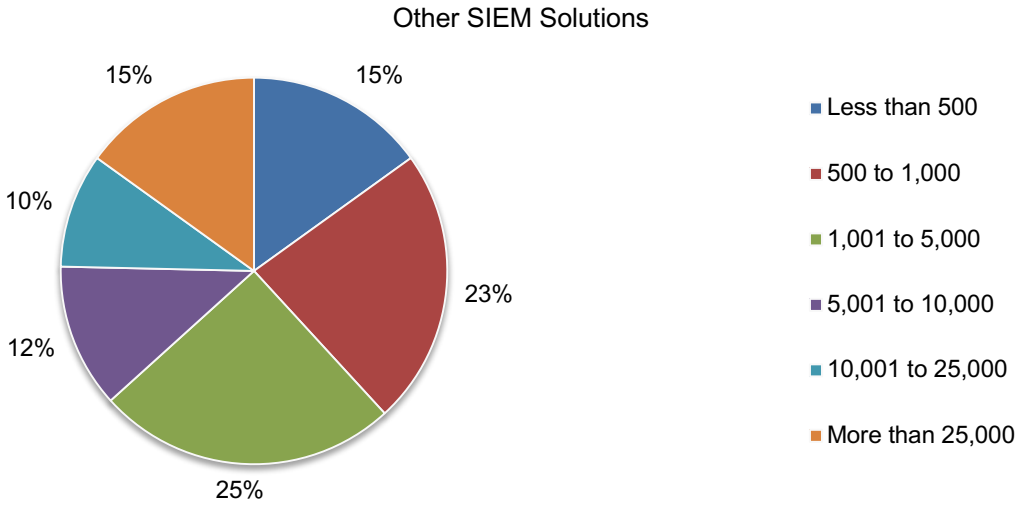
According to Pie Chart 7, 65 percent of Exabeam respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 7. Worldwide headcount of the organization for the Exabeam sample



According to Pie Chart 8, 62 percent of other SIEM solution respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 8. Worldwide headcount of the organization for the other SIEM solutions sample



Part 4. Caveats to this study

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

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners, 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 that are IT or IT security practitioners. Because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, the possibility remains that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from May 8, 2019 to May 22, 2019.

Survey response	Freq	Pct%
Total sampling frame	16446	100.0%
Total returns	647	3.9%
Rejected surveys	51	0.3%
Final sample	596	3.6%
Exabeam subsample	42	

Part 1. Screening Questions

S1. Does your organization use Exabeam as its primary SIEM provider?	Exabeam	Other SIEM Solutions
Yes	100%	0%
No	0%	100%
Total	100%	100%

S2. How familiar are you with your organization's SIEM deployment?	Exabeam	Other SIEM Solutions
Very familiar	48%	45%
Familiar	38%	40%
Somewhat familiar	14%	15%
No knowledge (stop)	0%	0%
Total	100%	100%

S3. Do you have any responsibility in the detection, investigation and/or remediation of security threats inside your organization's network?	Exabeam	Other SIEM Solutions
Yes, full responsibility	48%	46%
Yes, some responsibility	40%	41%
Yes, minimum responsibility	12%	13%
No responsibility (stop)	0%	0%
Total	100%	100%

Part 2. Background

Q1. Using the following 10-point scale, please rate your organization's effectiveness in using its SIEM to detect and investigate cyberattacks.	Exabeam	Other SIEM Solutions
1 or 2	0%	4%
3 or 4	0%	13%
5 or 6	5%	24%
7 or 8	19%	23%
9 or 10	76%	36%
Total	100%	100%
Extrapolated value	8.93	6.98

Q2. Using the following 10-point scale, please rate your organization's effectiveness in minimizing false positives when using its SIEM to detect and investigate cyberattacks.	Exabeam	Other SIEM Solutions
1 or 2	5%	3%
3 or 4	7%	8%
5 or 6	2%	35%
7 or 8	14%	30%
9 or 10	71%	24%
Total	100%	100%
Extrapolated value	8.31	6.78

Q3. Using the following 10-point scale, please rate your organization's effectiveness in minimizing the costs associated with using your SIEM to detect and investigate cyberattacks.	Exabeam	Other SIEM Solutions
1 or 2	0%	6%
3 or 4	2%	11%
5 or 6	7%	34%
7 or 8	20%	23%
9 or 10	70%	26%
Total	100%	100%
Extrapolated value	8.69	6.54

Q4. Using the following 10-point scale, please rate your organization's effectiveness in prioritizing alerts that pose significant cyber risk.	Exabeam	Other SIEM Solutions
1 or 2	0%	6%
3 or 4	2%	16%
5 or 6	7%	27%
7 or 8	21%	23%
9 or 10	69%	28%
Total	100%	100%
Extrapolated value	8.83	6.52

Q5. What Exabeam product features does your organization currently use?	Exabeam	Other SIEM Solutions
Data lake	79%	
Cloud connectors	50%	
Advanced analytics	67%	
Threat hunter	79%	
Incident responder	40%	
Case manager	48%	
Total	362%	

Q6. What metrics does your SIEM provide for pricing/licensing the product?	Exabeam	Other SIEM Solutions
Number of end users	74%	23%
Organizational size	19%	15%
Volume of transactions	5%	57%
Other (please specify)	2%	5%
Total	100%	100%

Q7. Approximately, how many data sources does your organization use to detect attacks?	Exabeam	Other SIEM Solutions
Less than 5	2%	5%
5 to 10	17%	9%
11 to 50	12%	25%
51 to 100	31%	29%
101 to 150	24%	23%
151 to 250	14%	8%
More than 250	0%	1%
Total	100%	100%
Extrapolated value	86	78

Q8. Have you ever had to upgrade your log source license to accommodate growth in log data?	Exabeam	Other SIEM Solutions
Yes	29%	50%
No	64%	44%
Unsure	7%	6%
Total	100%	100%

Q9. Have you not been able to log data you needed for security because of budget limitations due to licensing model?	Exabeam	Other SIEM Solutions
Yes	12%	46%
No	83%	49%
Unsure	5%	5%
Total	100%	100%

Q10. How do you manage your Exabeam or other SIEM solution today? Please select one top choice.	Exabeam	Other SIEM Solutions
Dedicated in-house team maintains solution, tunes rules and manages threats	52%	40%
Service provider maintains solution, manages threats, tunes rules and complete remediation activities	21%	29%
Split responsibility; service provider maintains solution, tunes rules and complete potential threats to an in-house team for investigation and response	26%	31%
Total	100%	100%

Part 3. Deployment Experience

Q11a. Did you purchase any professional services to help you with the initial SIEM deployment?	Exabeam	Other SIEM Solutions
Yes	21%	40%
No	79%	60%
Total	100%	100%

Q11b. If yes, how many weeks of professional services were used during the initial deployment?	Exabeam	Other SIEM Solutions
Less than 1 week	22%	14%
1 to 2 weeks	67%	36%
3 to 4 weeks	11%	21%
5 to 6 weeks	0%	16%
7 to 8 weeks	0%	10%
9 to 10 weeks	0%	3%
11 to 20 weeks	0%	0%
More than 20 weeks	0%	0%
Total	100%	100%
Extrapolated value	1.50	3.26

Q12. How long did it take your organization to realize **value** from Exabeam deployment?	Exabeam	Other SIEM Solutions
Within days	52%	28%
Within a week	40%	25%
Within a month	7%	26%
Within three months	0%	12%
More than three months	0%	5%
Value has not been realized as yet	0%	4%
Total	100%	100%

Part 4. Detection and analytics

Please rate the following statement using the 10-point scale from 1 = not valuable at all to 10 = very valuable.		
Q13. How valuable are the out-of-the box correlation rules?	Exabeam	Other SIEM Solutions
1 or 2	0%	5%
3 or 4	0%	6%
5 or 6	14%	28%
7 or 8	12%	29%
9 or 10	74%	32%
Total	100%	100%
Extrapolated value	8.69	7.04

Q14. How many custom correlation rules have you developed?	Exabeam	Other SIEM Solutions
None	0%	9%
1 to 10	29%	45%
11 to 25	36%	31%
26 to 50	24%	11%
51 to 100	6%	4%
More than 100	0%	0%
Total	100%	100%
Extrapolated value	25.65	14.86

Q15a. Does your SIEM have detection models?	Exabeam	Other SIEM Solutions
Yes	90%	90%
No	10%	10%
Total	100%	100%

Q15b. If yes, how valuable are the out-of-the-box detection models?	Exabeam	Other SIEM Solutions
1 or 2	0%	5%
3 or 4	3%	12%
5 or 6	8%	28%
7 or 8	21%	26%
9 or 10	68%	29%
Total	100%	100%
Extrapolated value	8.61	6.74

Q15c. If yes, how many detection models have you developed?	Exabeam	Other SIEM Solutions
None	5%	5%
1 to 10	45%	55%
11 to 25	29%	34%
26 to 50	21%	6%
51 to 100	0%	0%
More than 100	0%	0%
Total	100%	100%
Extrapolated value	15.30	10.98

Q16. On average, how many alerts do you see on a daily basis?	Exabeam	Other SIEM Solutions
Less than 50	5%	3%
51 to 100	21%	18%
101 to 250	26%	23%
251 to 500	21%	26%
501 to 1,000	19%	21%
1,001 to 5,000	7%	9%
5,001 to 10,000	0%	0%
More than 10,000	0%	0%
Total	100%	100%
Extrapolated value	500.60	579.50

Q17. What percentage of daily alerts in your SIEM are you able to investigate?	Exabeam	Other SIEM Solutions
Less than 10%	0%	5%
10% to 25%	2%	23%
26% to 50%	5%	35%
51% to 75%	10%	19%
76% to 90%	36%	10%
91% to 100%	48%	8%
Total	100%	100%
Extrapolated value	83%	45%

Q18. On average, what percentage of alerts in your SIEM are false positives?	Exabeam	Other SIEM Solutions
Less than 10%	74%	19%
10% to 25%	19%	36%
26% to 50%	7%	20%
51% to 75%	0%	15%
76% to 90%	0%	8%
91% to 100%	0%	2%
Total	100%	100%
Extrapolated value	10%	33%

Part 5. Post-deployment operational benefits

Q19. How many full or partial headcount are allocated to operating your organization's SIEM?	Exabeam	Other SIEM Solutions
None	12%	4%
Half FTE	33%	25%
1FTE	36%	36%
2 FTEs	17%	29%
2+ FTEs	2%	6%
Total	100%	100%
Extrapolated value	0.93	1.25

Q20. How many security operations employees are dedicated to managing, hunting, investigating and responding to threats?	Exabeam	Other SIEM Solutions
1 to 4	31%	26%
5 to 10	33%	40%
11 to 25	19%	14%
26 to 50	12%	12%
More than 50	5%	7%
Total	100%	100%
Extrapolated value	14.08	15.07

Q21a. Did the use of your SIEM provider help your organization **reduce headcount** costs associated with daily security incident investigations?	Exabeam	Other SIEM Solutions
Yes	24%	19%
No	76%	81%
Total	100%	100%

Q21b. If yes, how much headcount was reduced?	Exabeam	Other SIEM Solutions
None	0%	0%
Half FTE	40%	73%
1FTE	50%	23%
2 FTEs	10%	4%
2+ FTEs	0%	0%
Total	100%	100%
Extrapolated value	1.13	0.68

Q21c. If yes, how has staffing of your organization's security analyst team changed? Please select one top choice.	Exabeam	Other SIEM Solutions
We were able to replace more senior staff with more junior staff	50%	46%
Staff was transferred to more senior security analyst roles	30%	33%
Staff was transferred to a different part of the security team	20%	21%
No changes in structure of staffing	0%	0%
Total	100%	100%

Q22a. Has your organization purchased any additional professional services to assist with your SIEM provider since it was implemented?	Exabeam	Other SIEM Solutions
Yes, for tuning	12%	16%
Yes, for new module installation	17%	15%
Yes, for incident response	10%	23%
Yes, for integrations	7%	17%
We did not purchase additional professional services	55%	29%
Total	100%	100%

Q22b. If yes, how many days of professional services were purchased?	Exabeam	Other SIEM Solutions
Less than 1 week	74%	40%
1 to 2 weeks	16%	20%
3 to 4 weeks	11%	18%
5 to 6 weeks	0%	12%
7 to 8 weeks	0%	6%
9 to 10 weeks	0%	3%
11 to 20 weeks	0%	1%
More than 20 weeks	0%	0%
Total	100%	100%
Extrapolated value	1.54	2.68

Q23a. Was your organization able to replace any point security solution products as a result of the successful implementation and deployment of Exabeam?	Exabeam	Other SIEM Solutions
Yes	67%	63%
No	33%	37%
Total	100%	100%

Q23b. If yes, how many point solutions were replaced?	Exabeam	Other SIEM Solutions
1 to 2	21%	32%
3 to 5	32%	38%
6 to 10	29%	25%
11 to 20	14%	5%
More than 20	4%	0%
Total	100%	100%
Extrapolated value	7.00	4.78

Q24. What percentage of your cybersecurity staff is engaged in threat hunting activities?	Exabeam	Other SIEM Solutions
Less than 10%	10%	7%
10% to 25%	7%	8%
26% to 50%	38%	34%
51% to 75%	24%	29%
76% to 100%	21%	22%
Total	100%	100%
Extrapolated value	50%	52%

Q25. On average, how many actual attacks does your organization see in any given week?	Exabeam	Other SIEM Solutions
Less than 100	0%	1%
101 to 500	14%	14%
501 to 1,000	29%	26%
1,001 5,000	24%	27%
5,001 to 10,000	21%	23%
More than 10,000	12%	9%
Total	100%	100%
Extrapolated value	4,007	3,853

Q26. How many known security breaches did your organization have in the past 12 months?	Exabeam	Other SIEM Solutions
Less than 10	24%	39%
10 to 50	50%	30%
51 to 100	19%	19%
101 to 500	7%	8%
501 to 1,000	0%	3%
More than 1,000	0%	1%
Total	100%	100%
Extrapolated value	52	84

Part 6. Estimated Time

Instruction: Please provide your best time estimate spent by organizations before and after the deployment of Exabeam. All time estimates should be framed in hours during the typical week.

Q27. Approximately, how many hours each week is spent organizing and planning the organization's approach to detecting and evaluating suspicious and/or anomalous events? Please estimate the aggregate hours of IT security personnel.

Q27a. Before Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	7%	5%
5 to 10	10%	6%
11 to 25	10%	18%
26 to 50	14%	15%
51 to 100	12%	10%
101 to 250	17%	15%
251 to 500	17%	18%
More than 500	14%	13%
Total	100%	100%
Extrapolated value	194	189

Q27b. After Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	12%	12%
5 to 10	19%	19%
11 to 25	10%	2%
26 to 50	21%	21%
51 to 100	14%	12%
101 to 250	12%	12%
251 to 500	12%	19%
More than 500	0%	2%
Total	100%	100%
Extrapolated value	88	126

Q28. Approximately, how many hours each week is spent gathering actionable intelligence about cyber threats and vulnerabilities? Please estimate the aggregate hours of IT security personnel.		
Q28a. Before Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	12%	10%
5 to 10	17%	13%
11 to 25	2%	7%
26 to 50	7%	8%
51 to 100	14%	14%
101 to 250	21%	20%
251 to 500	17%	15%
More than 500	10%	13%
Total	100%	100%
Extrapolated value	173	185

Q28b. After Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	19%	15%
5 to 10	21%	16%
11 to 25	7%	12%
26 to 50	21%	12%
51 to 100	10%	9%
101 to 250	7%	12%
251 to 500	10%	15%
More than 500	5%	9%
Total	100%	100%
Extrapolated value	95	146

Q29. Approximately, how many hours each week are spent evaluating actionable intelligence? Please estimate the aggregate hours of IT security personnel.		
Q29a. Before Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	12%	8%
5 to 10	17%	11%
11 to 25	2%	11%
26 to 50	7%	9%
51 to 100	14%	14%
101 to 250	21%	21%
251 to 500	17%	18%
More than 500	10%	8%
Total	100%	100%
Extrapolated value	173	169

Q29b. After Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	19%	17%
5 to 10	21%	17%
11 to 25	2%	2%
26 to 50	21%	21%
51 to 100	12%	12%
101 to 250	12%	12%
251 to 500	12%	12%
More than 500	0%	7%
Total	100%	100%
Extrapolated value	85	127

Q30. Approximately, how many hours each week are spent investigating actionable intelligence and building incident timelines? Please estimate the aggregate hours of IT security personnel.		
Q30a. Before Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	2%	2%
5 to 10	7%	6%
11 to 25	5%	7%
26 to 50	7%	8%
51 to 100	12%	12%
101 to 250	26%	24%
251 to 500	19%	23%
More than 500	21%	18%
Total	100%	100%
Extrapolated value	259	250

Q30b. After Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	12%	5%
5 to 10	5%	12%
11 to 25	12%	12%
26 to 50	14%	10%
51 to 100	21%	21%
101 to 250	19%	19%
251 to 500	14%	14%
More than 500	2%	7%
Total	100%	100%
Extrapolated value	125	153

Q31. Approximately, how many hours each week are spent cleaning, fixing and/or patching networks, applications and devices as a result of an incident? Please estimate the aggregate hours of IT security personnel.		
Q31a. Before Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	2%	2%
5 to 10	0%	3%
11 to 25	5%	9%
26 to 50	10%	8%
51 to 100	14%	11%
101 to 250	19%	19%
251 to 500	24%	21%
More than 500	26%	27%
Total	100%	100%
Extrapolated value	295	287

Q31b. After Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	2%	2%
5 to 10	0%	7%
11 to 25	12%	12%
26 to 50	26%	10%
51 to 100	24%	24%
101 to 250	14%	14%
251 to 500	12%	12%
More than 500	10%	19%
Total	100%	100%
Extrapolated value	157	208

Q32. Approximately, how many hours each week are spent documenting security incidents (in conformance with policies or compliance mandates)? Please estimate the aggregate hours of IT security personnel.		
Q32a. Before Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	10%	11%
5 to 10	12%	13%
11 to 25	17%	14%
26 to 50	14%	12%
51 to 100	21%	18%
101 to 250	10%	16%
251 to 500	7%	7%
More than 500	10%	9%
Total	100%	100%
Extrapolated value	126	130

Q32b. After Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	0%	0%
5 to 10	19%	19%
11 to 25	21%	21%
26 to 50	24%	24%
51 to 100	19%	14%
101 to 250	14%	14%
251 to 500	2%	5%
More than 500	0%	2%
Total	100%	100%
Extrapolated value	62	82

Q33. Approximately, how much time spent by security personnel are wasted because the alerts or IOCs they chase are erroneous (i.e., false positives)? Please estimate the aggregate hours of IT security personnel.		
Q33a. Before Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	0%	0%
5 to 10	0%	0%
11 to 25	0%	0%
26 to 50	5%	4%
51 to 100	2%	7%
101 to 250	12%	10%
251 to 500	31%	33%
More than 500	50%	46%
Total	100%	100%
Extrapolated value	441	424

Q33b. After Exabeam/Current SIEM solution	Exabeam	Other SIEM Solutions
Less than 5	0%	0%
5 to 10	5%	5%
11 to 25	7%	7%
26 to 50	12%	6%
51 to 100	21%	10%
101 to 250	26%	26%
251 to 500	17%	21%
More than 500	12%	25%
Total	100%	100%
Extrapolated value	202	286

Part 6. Recap

Q27. Approximately, how many hours each week is spent organizing and planning the organization's approach to detecting and evaluating suspicious and/or anomalous events? Please estimate the aggregate hours of IT security personnel.	Exabeam	Other SIEM Solutions
Q27a. Before Exabeam/Current SIEM solution	194	189
Q27b. After Exabeam/Current SIEM solution	88	126
Hours saved	106	63
Q28.Approximately, how many hours each week is spent gathering actionable intelligence about cyber threats and vulnerabilities? Please estimate the aggregate hours of IT security personnel.	Exabeam	Other SIEM Solutions
Q28a. Before Exabeam/Current SIEM solution	173	185
Q28b. After Exabeam/Current SIEM solution	95	146
Hours saved	78	39

Q29. Approximately, how many hours each week are spent evaluating actionable intelligence? Please estimate the aggregate hours of IT security personnel.	Exabeam	Other SIEM Solutions
Q29a. Before Exabeam/Current SIEM solution	173	169
Q29b. After Exabeam/Current SIEM solution	85	127
Hours saved	88	42

Q30. Approximately, how many hours each week are spent investigating actionable intelligence and building incident timelines? Please estimate the aggregate hours of IT security personnel.	Exabeam	Other SIEM Solutions
Q30a. Before Exabeam/Current SIEM solution	259	250
Q30b. After Exabeam/Current SIEM solution	125	153
Hours saved	134	97

Q31. Approximately, how many hours each week are spent cleaning, fixing and/or patching networks, applications and devices as a result of an incident? Please estimate the aggregate hours of IT security personnel.	Exabeam	Other SIEM Solutions
Q31a. Before Exabeam/Current SIEM solution	295	287
Q31b. After Exabeam/Current SIEM solution	157	208
Hours saved	138	79

Q32. Approximately, how many hours each week are spent documenting security incidents (in conformance with policies or compliance mandates)? Please estimate the aggregate hours of IT security personnel.	Exabeam	Other SIEM Solutions
Q32a. Before Exabeam/Current SIEM solution	126	118
Q32b. After Exabeam/Current SIEM solution	62	82
Hours saved	64	36

Q33. Approximately, how much time spent by security personnel are wasted because the alerts or IOCs they chase are erroneous (i.e., false positives)? Please estimate the aggregate hours of IT security personnel.	Exabeam	Other SIEM Solutions
Q33a. Before Exabeam/Current SIEM solution	441	424
Q33b. After Exabeam/Current SIEM solution	202	286
Hours saved	239	138

Recap Q27 to Q33	Exabeam	Other SIEM Solutions
Before Exabeam/Current SIEM solution	1,661	1,622
After Exabeam/Current SIEM solution	814	1,128
Hours saved	847	494

Part 7. Demographics

D1. What best describes your position level within the organization?	Exabeam	Other SIEM Solutions
Executive/VP	7%	6%
Director	17%	15%
Manager/Supervisor	29%	30%
Staff/Technician/Analyst/Engineer	48%	47%
Contractor	0%	2%
Other (please specify)	0%	0%
Total	100%	100%

D2. Check the **Primary Executive** you or your IT security leader reports to within the organization.	Exabeam	Other SIEM Solutions
CEO/Executive Committee	0%	2%
Chief Information Officer (CIO)	29%	36%
Chief Information Security Officer (CISO)	31%	29%
Chief Operating Officer (COO)	0%	0%
Chief Risk Officer (CRO)	2%	2%
Chief Security Officer (CSO)	5%	3%
Chief Technology Officer (CTO)	12%	9%
Compliance Officer	0%	0%
General Counsel (OGC)	0%	0%
Network Security Leader	5%	6%
Line of Business (LoB) Leader	5%	5%
SOC / Data Center Management	12%	8%
Total	100%	100%

D3. What best describes your organization's primary industry classification?	Exabeam	Other SIEM Solutions
Agriculture & food services	0%	0%
Communications	2%	2%
Consumer products	2%	7%
Defense & aerospace	0%	0%
Education & research	0%	0%
Energy & utilities	5%	5%
Financial services	24%	29%
Healthcare	14%	12%
Hospitality	2%	2%
Industrial/manufacturing	12%	7%
Pharmaceuticals	0%	5%
Public sector	7%	7%
Retail	7%	7%
Services	12%	5%
Technology & software	12%	10%
Transportation	0%	2%
Total	100%	100%

D4. What is the total employee headcount that best describes your organization?	Exabeam	Other SIEM Solutions
Less than 500	14%	15%
500 to 1,000	21%	23%
1,001 to 5,000	19%	25%
5,001 to 10,000	14%	12%
10,001 to 25,000	10%	10%
More than 25,000	21%	15%
Total	100%	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

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.