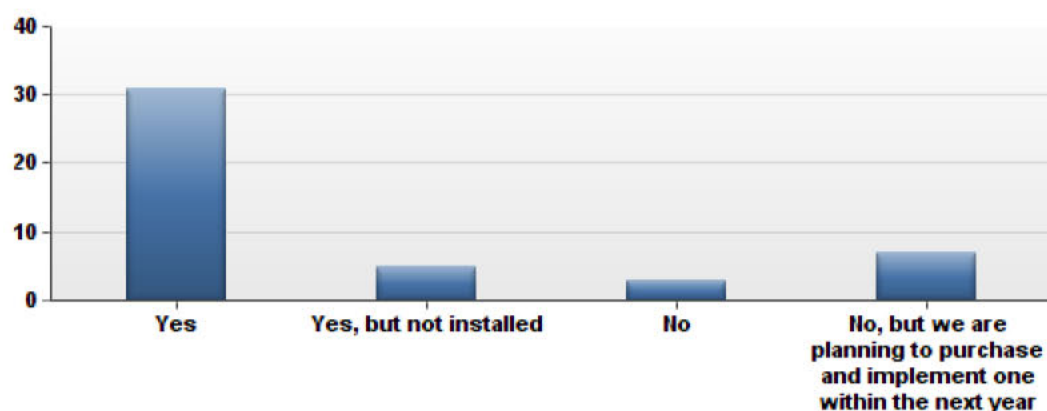


1. Does your institution have a SIEM?



#	Answer	Response	%
1	Yes	31	67%
2	Yes, but not installed	5	11%
3	No	3	7%
4	No, but we are planning to purchase and implement one within the next year	7	15%
	Total	46	100%

2. Which vendor did your institution select?

Answer	Response	%
Splunk	6	22
LogRhythm	4	14
AlienVault	3	11
Nitro	3	11
Arcsight	2	7
QRadar	2	7
EIQ	1	3.5
RSA	1	3.5
Intel Security	1	3.5
Panopticon	1	3.5
Blank	4	14
Total	28	

3. How long has your institution had its SIEM implemented (in years)?

#	Answer		Response	%
1	0-1 years		11	41%
3	2-5 years		11	41%
4	6-9 years		3	11%
6	10 or more years		2	7%
	Total		27	100%

4. How does your institution use its SIEM?

#	Answer		Response	%
2	Threat data		3	11%
3	Incident detection		13	48%
5	Other, please explain:		11	41%
	Total		27	100%

5. Please rate the usefulness of the SIEM-produced data to the incident response team.

#	Question	Very useful	Somewhat useful	Not very useful	Not at all useful	Not sure	Total Responses	Mean
1	Detecting compromised user accounts	7	15	1	1	3	27	3.33
2	Detecting suspicious network traffic	9	11	2	2	2	26	3.27
3	Detecting data breaches	3	5	9	2	8	27	4.63
4	Detecting suspicious workstation/server activity	8	10	3	1	5	27	3.67

6. How many full time equivalent (FTEs) staff members are dedicated to the SIEM and what are their roles?

Number of FTE	Roles
0.1	Network Specialist
2	
1	.5 Network Engineer + .5 Security Analyst
1	sysadmin
1	Network Security Engineer
1.5	Network Engineer and System administrator
1	Security Analyst
2	Manage infrastructure
1	Information Security Team Lead
1.0	IT Security Specialist - Advanced level
2	ITS
.5	
1/2	Security analyst
.5	Anylist
1	siem security analyst
2	Security Technician
1.2	.2 Sys admin/index admin; .5 index admin/security; .5 developer - not just one dedicated individual.
3	1 Information Security Engineer & 2 Information Security Analyst
2.0	monitoring, configuration, and maintenance (4 actual employees, each with other duties).
1	administrator
0.5	IT Security Specialist
1	
	IT Security Officer
	We absorbed the project with existing staff. One staff member increased workday for evaluation and implementation.
	Should have 2

7. Please provide additional comments or suggestions below:

Text Response

Strongly advise that the scope of the implementation is firm, otherwise you end up trying "SIEM" your entire network and never complete the implementation. We had ArcSight for six-years; it barely made it off the pallet in six-years. (INTEL SECURITY)

For context, we looked at LogRhythm, Splunk, AlienVault, HP ArcSight, and IBM QRadar. Our main concern driving the purchase was PCI compliance. LogRhythm, AlienVault and Splunk were our three finalists for this reason. LogRhythm and AlienVault both have built-in PCI reporting for no additional cost, and Splunk has a PCI app that adds to the cost but is very easy to use. IBM never called us back. HP ArcSight has a very dated interface and everything is buried in a cumbersome menu structure, but it is an old standard in SIEM and works quite well. AlienVault shows a lot of promise, but has stability issues. I think they will have a very strong product in 3-5 years. Splunk is very good, but is much more expensive than many of the other options, and some apps, such as the PCI compliance app, exacerbate this. If you can afford it, you will probably find that Splunk is the easiest to get set up and run because they will send their professional services team out to do it for you. It is also extremely versatile. You are basically limited to your imagination when it comes to working with data in Splunk. I would recommend trying to get to a SplunkLive! conference to see some of the creative uses people have found for this product. LogRhythm has a very responsive team that went to great lengths to make sure their POC was successful. The software is currently in transition from a console you remote into to more of a web GUI and is in a somewhat awkward stage at the moment, but the underlying technology is strong. (LOGRHYTHM)

Great product. Great vendor to work with. I wrote unsure on breach as one has not been detected. Hopefully it will work well in that scenario. (EIQ)

We have worked closely with Extreme networks and they have a suite of tools that is integrated that would be an ultimate setup. They have a SEIM and incredible Analytics that draw off of their unsampled netflow. If I had funding I would go with the Extreme solution hands down. (NO RESPONSE)

Absorbent cost - may be considering alternative products soon. (IBM QRADAR)

We're in the middle of the rollout. Too early to tell (LOGRHYTHM)

This is a very difficult area to research. Providers have varied features that don't always make for head to head comparison. (NO RESPONSE)

Would not buy nitro security again - nor products McAfee purchases. (NO RESPONSE)

The SIEM was pressed into production before fully deployed. Even so, it has been invaluable in providing visibility into operations. Our ability to quickly write rules to aid in ongoing incident management and discovery and post incident data analysis has also been invaluable. And its not in full production configuration yet! Make sure you define scope ahead of design and procurement. Incident discovery and management and compliance can have very different requirements. Make sure your back end logging infrastructure is up to snuff. Make sure you're feeding it good intelligence (raw, untuned IDS data is not good, tuned IDS rules are much better). Make sure you have some idea what your data retention and deletion policy will be. The learning curve is a mixture of learning your suddenly more visible environment behavior, learning what the intelligence sources actually mean, learning how to tune the SIEM to provide you with the information you want, and determining what information you want and what you plan to do with it with a clearly defined monitoring and incident response policies and procedures. We actually brought in three systems for evaluation and used all three with all logs going to them for a period of 60 days. Though it meant long hours, I believe we came out of the process with a good understanding of capabilities and differences that we would not have attained any other way. McAfee was one third the price of some of the more popular products and I believe it is on par with them. They have made great strides in the past 18 months in product features. (MCAFEE)

We enjoy using USM and would highly recommend it. (ALIENVAULT)

We currently use Splunk for logging and monitoring which is why we purchased Splunk Enterprise Security as the SIEM solution. We are very hopeful that it will help with compromised accounts but are still installing. (SPLUNK)

There are tons of out of the box alerts, but most of them require some tweaking. Also it is easy to build your own, but the process is ongoing as you think of new ways to sense things that are going on. (LOGRHYTHM)

SIEMs require much more time than we have allotted for it. The information can be extremely valuable if we could dedicate the time to set it and the reports up correctly. (NITRO)

DB access is very quick. One of the deciding factors. We have also attached the ELM (log storage to the SIEM which aids in forensics by being able to pull complete logs of events. (NITRO)

Alienvault is far more baked and doesn't require a lot of "apps" that may be unsupported by a vendor. (SPLUNK)

We will be working on this for a couple of more years to get everything going to the SIEM. As we add more, our license needs to increase which takes time....we are working on trimming off the 'fat' in some data collection. (SPLUNK)

We had selected QRadar before they were acquired by IBM, we were relieved when IBM placed Qradars top executives over their security program. We have had very good support and are adding new logs to expand our dashboards and reports. (QRADAR)

We are happy to discuss our implementation if desired. (ALIENVAULT)

Would like to see your survey results in order to provide insight to our upcoming SIEM implementation. (NO RESPONSE)

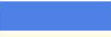
Our SIEM is not yet production, so I can't say how useful the graphs and reports are yet. It will be production inside two weeks, we are just receiving training. The IT Security team has two specialists, and the SIEM product is one part of their job. (ARCSIGHT)

We are looking at QRadar, LogRhythm and Alienvault (NO RESPONSE)

We used to run a Nitro Security SIEM but outgrew it and would not go back now that it is owned by McAfee (price and support). We are looking at LogRhythm and QRadar mostly. (NO RESPONSE)

Currently using OSSEC an Open Source Host-based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. (NO RESPONSE)

8. Which team maintains the tool?

#	Answer		Response	%
1	Information Security Office		14	54%
2	Network Operations Center		6	23%
3	Incident Response Team		0	0%
4	IT Department		6	23%
5	Outsourced		0	0%
6	Other		0	0%
	Total		26	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	1.92
Variance	1.51
Standard Deviation	1.23
Total Responses	26

9. How many are on the team?

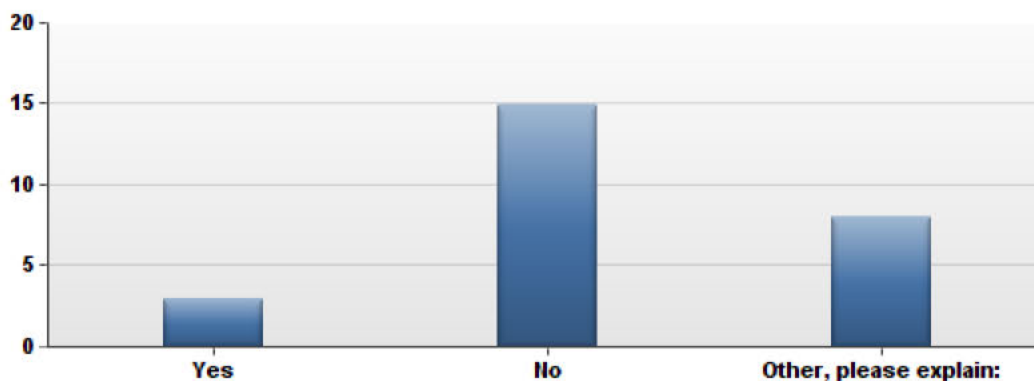
#	Answer		Response	%
1	1		4	15%
2	2-3		12	46%
3	4-5		5	19%
4	6 or greater		5	19%
	Total		26	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	2.42
Variance	0.97
Standard Deviation	0.99
Total Responses	26

10. How much time did this team spend creating SIEM alerts and reports before the alerts or reports became useful and valuable?

#	Answer		Response	%
1	None, they were immediately valuable and useful		3	12%
2	0-3 months		4	15%
3	3-6 months		5	19%
4	6-12 months		6	23%
5	The reports are still not helpful, and require additional tweaking		8	31%
	Total		26	100%

11. Would your institution have selected a different vendor if your institution could repurchase the product?



#	Answer		Response	%
1	Yes		3	12%
2	No		15	58%
3	Other, please explain:		8	31%
	Total		26	100%

Other, please explain:

We've been running OSSIM (free alienvault) for some time now, but have only recently purchased the full product, and it's not implemented yet.

major needs other than security

Not sure. Existing solution needs much tuning to give a fair consideration.

Not sure as we are still implementing the product

uncertain, they're all difficult to use/establish

There is debate - the cost is getting very expensive for sending more logs. We are still not having everything go to the SIEM.

not sure - still fully implementing

Potentially, given how Splunk have released a SIEM package for their log too.