netwrix

2016
SIEM Efficiency
Survey

Contents

Introduction

Companies deploy SIEM (Security information and event management) solutions to get a comprehensive understanding of what is happening across their entire IT network. Companies use SIEM products to collect, correlate and analyze high volumes of diverse machine data from all over the IT environment because they want to get real-time indicators of potential security violations.

Data collection is the first among SIEM's core functions, which SIEM solutions handle without any issues. However, when it comes to data analysis, reporting and alerting to security violations, the limitations become even more obvious. SIEM solutions often lack granular details about any events hiding behind a load of raw logs. When SIEM analysts get an alert, they have to spend hours looking through event logs to find an answer to what exactly is happening. This often results in delays in detection of security threats and low-speed reactions to an incident.

The need to increase the visibility of what is going on across the entire IT infrastructure pushes SIEM users to search for a solution. Some companies opt to add an IT auditing solution to enhance SIEM. Designed to bring more context into what is going on, IT auditing solutions provide necessary details about user activity and help to better understand which changes are business critical and require special attention.

Netwrix Corporation decided to find out how efficient IT auditing solutions are in increasing visibility into SIEM. For this report, 234 large companies that are involved in more than 20 industries were interviewed. The respondents were asked to describe their experience of using SIEM as an all-sufficient solution and SIEM enforced by IT auditing solution. The results are partially compared to the 2014 SIEM Efficiency Survey to provide more detailed insight into the state of technology perception.

Highlights

- The majority of companies deploy SIEM solutions to get better security threat awareness (67%) and be more efficient in root-cause analysis and incident investigation (61%).

- Almost 81% (75% in 2014) of respondents have stated that SIEM reports contain too much noise data. About 65% of companies face difficulties searching across the log data generated by SIEM to find answers to auditors' questions. Also, 57% of IT pros have to adapt the reports generated by SIEM for non-tech employees.

- Around 69% of respondents are looking for ways to slash SIEM bills. An average of 85% of SIEM users have stated that the total cost of the solution has risen significantly as the organization continues to use it. This includes expenses on staff augmentation, support services, product maintenance and hardware upgrades.

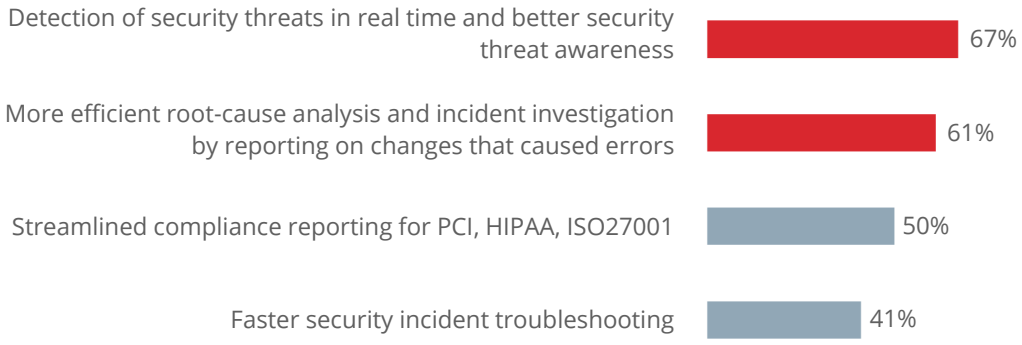
- In order to leverage their existing SIEM solution, about 55% of SIEM users stated that they are ready to hire additional personnel; 41% opt for strengthening SIEM with additional solutions.

- About 90% of companies using both SIEM and IT auditing solutions agree that IT auditing helps to overcome SIEM drawbacks. IT auditing advances report quality and simplifies searching through audit data.

SIEM Deployment Reasons

Each company deploys SIEM solutions for its own purposes. We asked the respondents about all applicable drivers for deploying a solution. The chart below shows that better security threat awareness takes the top of the rating as the most popular driver (67%). Other use cases include more efficient root-cause analysis and incident investigation (61%), streamlined compliance reporting (50%) and faster incident troubleshooting (41%).

Key drivers for using SIEM solutions



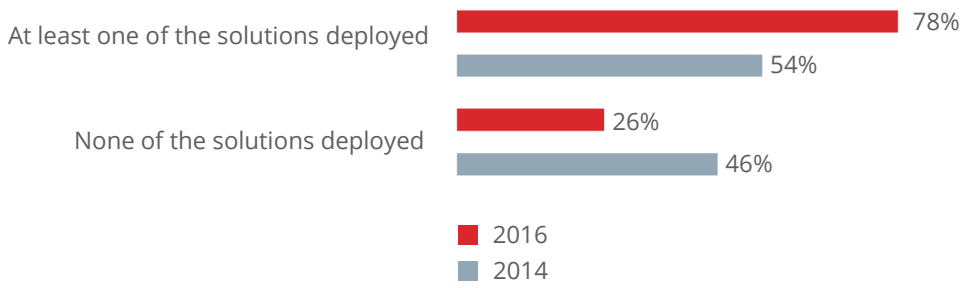
USE SIEM SOLUTION TO MONITOR WHAT IS HAPPENING ACROSS THE NETWORK

SIEM in Use

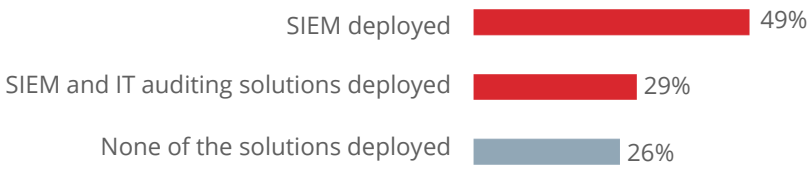
Compared to the results of 2014, the number of companies that deployed SIEM or integrated it with an IT auditing solution has increased from 54% to 78%. In this chapter, we analyze the answers of this group to get a detailed picture of their experience from using an IT auditing solution.

About 29% of survey respondents are using both SIEM and IT auditing solution to monitor what is happening across the IT infrastructure. Companies that have only SIEM deployed use it for auditing and reporting purposes in almost 75% of cases (against 68% in 2014).

Companies monitor their IT infrastructures in 2014 and in 2016



Companies using solutions in 2016

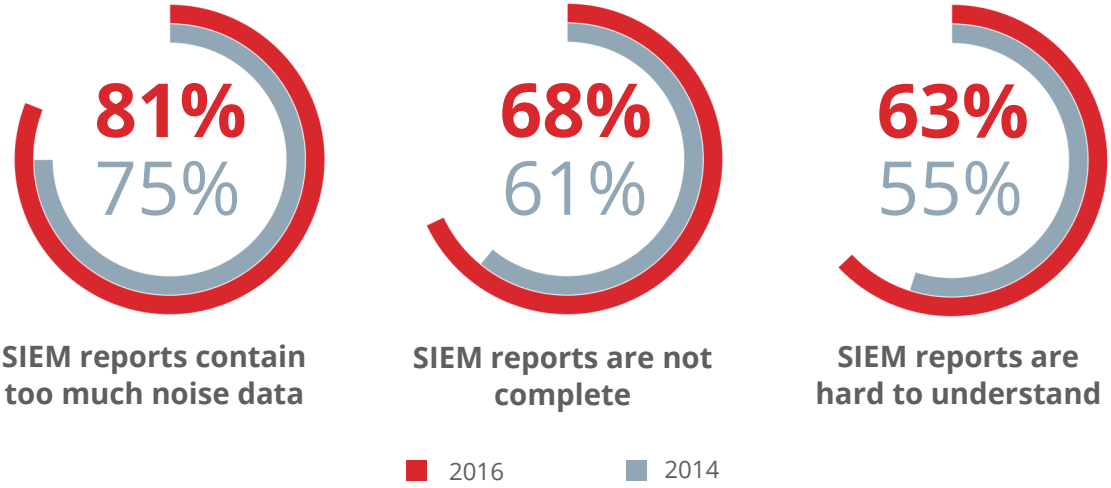


SIEM Limitations

SIEM has a reputation as a helpful and must-have solution to improve security for any enterprise. However, Forrester experts* say that SIEM has certain limitations, which makes it inefficient without additional investments in technology and personnel. We decided to find out whether companies achieve their goals with the help of SIEM, which limitations companies see in SIEM solutions and how they deal with them.

Back in 2014, we asked companies whether they noticed any gaps in audited data, suffered from too much noise in change auditing reports or found those reports hard to understand. The vast majority of respondents (75%, 61% and 55%, respectively) stated that they encountered the following problems.

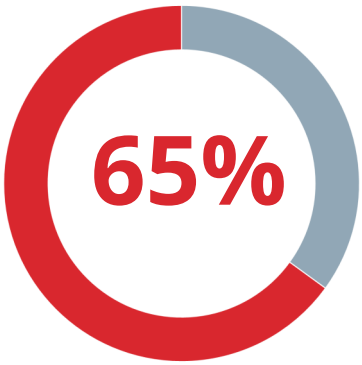
In 2016, the survey revealed that above-mentioned issues continue to bother SIEM users. Almost 81% of respondents claimed that SIEM reports contain too much noise data. The survey also showed that in general, the degree of concern around SIEM limitations is higher when compared to the results of 2014.



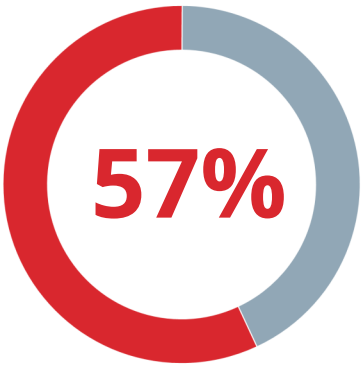
* Source: "Security Analytics Is The Cornerstone Of Modern Detection And Response. Organizations Must Evolve Beyond SIEM To Address The Rapidly Changing Threat Landscape," Forrester Research, Inc., December, 2015.

About 68% of companies found that SIEM reports often lacked necessary information, and 63% claimed that the reports are difficult to understand, especially for non-technical people.

Having raised the question about the key limitations of SIEM when it comes to auditing and reporting, we also were interested in whether this somehow influences the process of passing IT audits or validating internal security policies. The majority of companies (65%) stated they have issues with finding necessary audit data upon request. Also, 57% experienced situations in which they needed to adapt SIEM reports to make them more understandable for non-tech employees.



FACED ISSUES WITH FINDING NECESSARY AUDIT DATA ON REQUEST

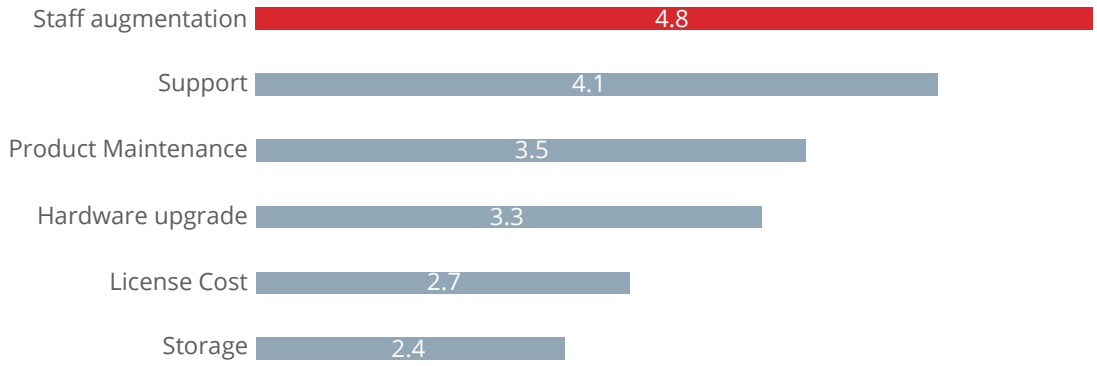


NEEDED TO ADAPT SIEM REPORTS

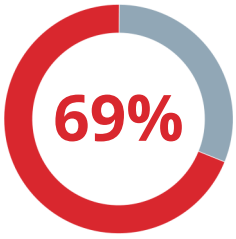
Cost of Ownership

Despite being a must-have solution, SIEM is known to require a considerable investment. The respondents were asked to rate the main expenses that influence the total cost of SIEM ownership using a scale of 1 to 5, where 1 is “free of charge” and 5 is “very expensive.”

Expenses, increasing the cost of SIEM ownership



The first result that became obvious is that SIEM users admit to high costs of ownership, as the majority of expenses are rated as expensive or very expensive. SIEM users see staff augmentation, like personnel training or hiring more security analysts, as the most critical factor inflating the price of SIEM. Also, SIEM users are concerned about expenses related to support (4.1), product maintenance (3.5), hardware upgrades necessary to deploy the solution or ensure its efficient performance (3.3), additional license costs (2.7) and storage solutions (2.4).



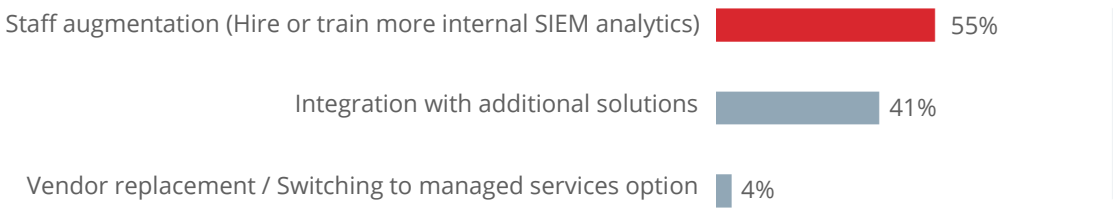
LOOKING FOR SOLUTIONS TO SLASH SIEM COSTS

While SIEM deployment entails significant investments by default, 69% of companies are not ready to put up with high costs and consider options that could help reduce SIEM expenses.

Dealing with SIEM Limitations

The majority of respondents (55%) said that the most preferable way to deal with SIEM drawbacks would be to hire additional personnel, while 41% opted for strengthening SIEM with additional solutions that are capable of overcoming the limitations.

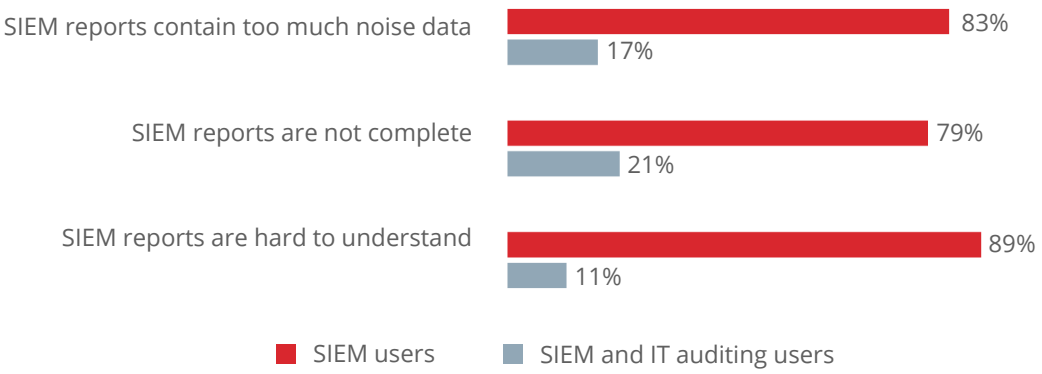
SIEM users on dealing with products' limitations



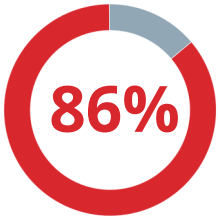
Unfortunately, these options still present their own challenges. Integration requires painstaking selection of reliable vendors, that should provide products with suitable features and seamless integration with various SIEM solutions. On the other hand, development of human resources requires time and additional investments in hiring well-qualified employees and implementing trainings, which makes integration with other solutions more advantageous in the long run.

Most of those who have successfully integrated SIEM with IT auditing solutions (86%) have agreed that it helped them to overcome SIEM drawbacks. Also, they became more satisfied with reporting capabilities, as reports contained less noise, included before and after values and were easier to understand, even for non-technical staff. Integration also enabled quick searches across the audit trail to meet specific requests, and in some cases, it reduced SIEM licensing, as it allowed people to process fewer event logs and therefore decreased data volume.

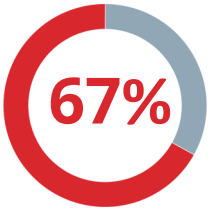
Problems with SIEM reports quality



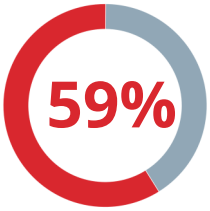
IT auditing users:



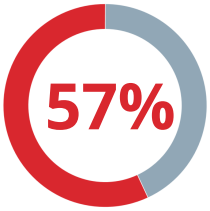
AGREED THAT IT AUDITING HELPS TO OVERCOME SIEM DRAWBACKS



HAD NO ISSUES FINDING NECESSARY AUDIT DATA ON REQUEST



STATED THAT REPORTS ARE UNDERSTANDABLE FOR NON-TECH EMPLOYEES



AGREED THAT IT AUDITING SLASHED COSTS BY REDUCING THE DATA VOLUME INDEXED BY SIEM

Conclusions

As companies strive to enhance protection against security threats, SIEM solutions can bring enormous benefits to these processes, helping with aggregation and analysis of diverse log data coming from all over the IT environment. The majority of companies agree that SIEM is useful for faster detection of security threats and simplifying root-cause analysis and incident investigation. Nevertheless, these solutions have limitations that companies need to consider.

- Almost 81% of companies said that SIEM reports deliver excessive amounts of data that have to be excluded to better understand what is going on and simplify the reports for non-technical stakeholders. Besides, SIEM analysts must search through audit data to find out what has happened to meet specific requests or conduct root-cause analysis. This influences time-sensitive tasks, such as incident troubleshooting, security investigations or passing compliance audits.

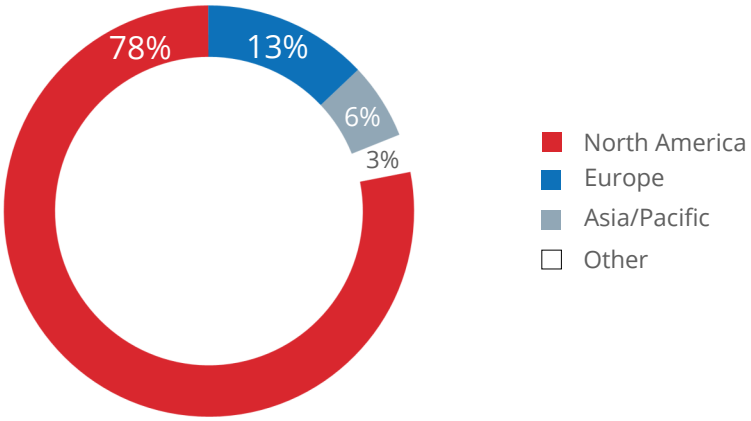
- The total cost of ownership is another main concern related to SIEM solutions, which is the result of its overall complexity. Additional employees, staff trainings, vendor-consulting services and other factors are unlikely to go unnoticed in companies' budgets. Therefore, many organizations (69%) have started to consider methods of cost reduction. About 29% of companies have chosen IT auditing solutions integrated with existing SIEM as a way to overcome limitations and slash costs.

- About 86% of those who integrated their SIEM with an IT auditing solution claim that it helped them overcome SIEM drawbacks. The majority of enterprises have fewer complaints about report quality, can search through audit data more quickly and don't need to adapt the reports for non-tech employees.

Respondent Demographics

Netwrix has surveyed 234 large enterprises to gather data for this research. According to Gartner's definition of organizational size, large enterprises have more than 1000 employees.

Geography



Top 8 industries represented in the survey

21% Technology

15% Education

11% Banking

10% Manufacturing

8% Health Care

7% Retail & Wholesale

6% Consulting

5% Service

About Netwrix Corporation

Netwrix Corporation provides IT auditing software that delivers complete visibility into IT infrastructure changes and data access, including who changed what, when and where each change was made and who has access to what. Over 150,000 IT departments worldwide rely on Netwrix to audit IT infrastructure changes and data access, prepare reports required for passing compliance audits and increase the efficiency of IT operations. Founded in 2006, Netwrix has earned more than 70 industry awards and was named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S. For more information, visit www.netwrix.com.

Netwrix Corporation

300 Spectrum Drive, Suite 1100,

Irvine, CA 92618, US

Toll-free: 888-638-9749

Int'l: 1-949-407-5125

EMEA: +44 (0) 203 318

netwrix.com/social