Journal of Engineering and Applied Sciences 14 (Special Issue 9): 10497-10501, 2019
ISSN: 1816-949X

SIEM Implementation for Small and Mid-Sized Business Environments

Lubos Mercl and Josef Horalek
Faculty of Informatics and Management, University of Hradec Kralove,
Hradec Kralove, Czech Republic

Abstract: For companies it is also important to protect their assets and know-how. In today's world, this expertise channeled into information systems and resources that can be vulnerable to attackers who may wish to obtain such information or otherwise manipulated. It is necessary to use for protection technologies that enable the prevention, detection and monitoring of these threats. This study deals with the implementation of one of these technologies Security Information and Event Management (SIEM) system in two companies that must protect sensitive data. SIEM provides a comprehensive tool for ensuring the safety management in for cyber security and associates himself into several parts, thus log management, log analysis, reporting and event management. This study describes SIEM architecture, design and implementation of SIEM solutions for the small and mid-sized business environment and complemented by financial analysis solutions.

Key words: SIEM, security, information, monitoring, implementation, solutions

INTRODUCTION

Threats of information leakage can be for companies a big problem and in today's cyber world, it is important to protect information systems (Whitman *et al*., 2012). Security is a complex and extensive issues which range from technical and technological matters, to the procedural aspects of data security and information (Whitman *et al*., 2012).

The security of information systems is based on several standards that define basic rules for data security. For the security solution exist systems that help solve the area or cover at least a part of it. These systems are known as Information Security Management System (ISMS) and one such system is a tool Security Information and Event Management (SIEM) which deals with the management of security information and security events, above all their analysis and their reporting (Bejtlich, 2013; Lee *et al*., 2016).

Security of information systems and information is one of the most important factors management of companies and in many large organizations is dedicated to this problem very extensive attention (Barton *et al*., 2016; Bedwell, 2014).

As already mentioned, in larger organizations, it is dedicated to this problem much attention but in smaller environments safety is put into the background and is preferable smooth operation rather than the security of data and information (Bedwell, 2014).

This study deals with security and data protection in the small business environment and the actual deployment of security technology in two environments.

For safety, there are many standards that the company must or wants comply and it gives the company credibility of the statute. One of these standards is the group ISO/IEC 27000 which includes the most important standards that relate to the solution of information security.

These standards help companies to meet legislative requirements, provide an overview of the systems that are suitable for information security solutions and define the terms that are used in a number of other standards (Bedwell, 2014; Lee *et al*., 2016). International standard ISO/IEC 27000 is applicable to all kinds of companies and organizations, whether commercial or non-commercial sector.

As part of the ISO/IEC 27001, a standard of ISO/IEC 27000 family, defined the concept of Information Security Management System (ISMS) which is a system for managing information systems security and which are defined by the information assets, risk management and checked compliance with the safety standards.

Among the tools ISMS include:

- Identity management for identity management and authentication, access management for managing and control access to systems and to data
- Accessibility monitoring for monitoring system and data availability
- Security information and event management for monitoring of security and check security threats and events in information infrastructure
- Endpoint management for managing end-user devices

Corresponding Author: Lubos Mercl, Faculty of Informatics and Management, University of Hradec Kralove, Hradec Kralove, Czech Republic

Another important concept for ISMS is the concept of information security which is based on the fact that the information that is valuable should be adequately protected (Miller *et al*., 2010) and this protection can be anything that prevents the loss on the part of so-called CIA triad which is based on ISO/IEC 27002 and which includes the areas:

- Confidentiality
- Integrity
- Availability

Solving one of ISMS areas provides a tool from IBM Security Information and Event Management (SIEM) which deals with security information and events. As already stated, SIEM tools offer a solution to one of the areas that is defined by ISO/IEC 27000 (Miller *et al*., 2010).

SIEM arose as a response the growing risk of cyber threats within the environment. Issues addressed by the SIEM solution are linked with four related concepts which are Miller *et al*. (2010).

- Security which is a condition where the object is secured or protected from hazards and threads information which is the basic information and which are encoded data
- Event which is the state of the process or the process that takes place, took place or will take place
- Management which is the process of creating and maintaining an environment where individual actors working together

These SIEM processes include these parts (Miller *et al*., 2010).

- Log management which is defined as the process of receiving information from sources logs into the database
- Log analysis which includes analysis of the received logs and their evaluation and distribution of any subsequent preservation
- Reporting which includes selected logs reporting which were evaluated as information that should be transmitted to human interaction
- Event management which includes the processes related to the handling of data from received events and their fair analysis. To define the size of a SIEM solution is also important to define the basic concepts that are important for the proper deployment of the solution (Miller *et al*., 2010)

The first term is the notion Events Per Second (EPS) which represents the number of events per second processed by system and the second one is Flows Per Minute (FPM) which represents the number processed network flows and network traffic (Miller *et al*., 2010).

SIEM architecture: SIEM technology is a very comprehensive tool that has several parts that work independently of each other but their mutual cooperation is important. Among these components SIEM systems include (Howell, 2015):

- Source devices which are devices that generate the log records and send logs to the system for processing and evaluation. These sources can include operating systems, applications, network devices and other devices
- Log collection which are processes for extracting data from the logs which are admitted to the system from the device
- Parsing and normalization of the logs is the most important part of the system that takes care of the processing and preparation of logs for analysis During this process the logs are processed into a normalized state
- Rule engine that is used to create rules which then identifies suspicious events that enter the system and the most common rule format is a condition of "what-if"
- Correlation engine that compares data from the source device and looking at them events which could mean a potential security incident. It is therefore an autonomous system that looks at incoming data correlation
- Log storage is part of a system that takes care of storing large volumes of data processed logs. Storing such data is important for the analyzing and auditing systems
- Event monitoring is a very important component which cares about the event monitoring and reporting. It also is used for date viewing, analyzing, structuring and rules for further analysis and data logs

To define the principles of SIEM is necessary to choose the appropriate product with this technology considering the primary aspects of society including politics, budget, company size, size information infrastructure and technological capabilities (Miller *et al*., 2010).

IBM Security QRadar SIEM: IBM Security QRadar SIEM is fully commercial solution of SIEM currently under distribution by IBM. Security architecture IBM QRadar has several tens of possible variations depending on the type of the component its performance but also the ability to cooperate smoothly with the rest of the infrastructure. Within the distribution is a choice of buying options of product QRadar:

- The first option is to distribute the specific infrastructure using tools built for the model solution which is more demanding to install and configure but this option guarantees scalability
- The second option is to purchase all-in-one solution which include needed components
- The last option is to purchase licenses to use their own hardware or virtual appliance

IBM Security QRadar SIEM runs on the operating system Red Hat Enterprise Linux 6.7 and uses a 64 bit system version and the current version bears the IBM QRadar Security 7.2.6. It is also necessary to define the difference between logical components which are necessary for running this SIEM system and witch are optional.

Necessary logical components are:

- Console for managing of environment and user interface components in the environment
- Event processor for processing events from one or more collectors
- Event collector for collecting events from local and distant sources
- Flow collector for collecting event stream data traffic on ports
- Flow Processor for processing event flows

And there are some optional logical components which can be used and they are:

- Incident forensics for reverse mapping of attacker actions
- Packet rupture which is optional part of incident Forensics for data flow capturing and collection
- Vulnerability manager for definitions of vulnerabilities
- Risk manager which can be used for threats asset management and vulnerabilities
- Anomaly detection for detecting of anomalies in environment
- Data node for storage and data management

Small business implementation: The first company for which it was designed solution of implementation SIEM technology is a small business company which is from the health sector. The company has 48 employees.

The organization has entire IT infrastructure located in one geographic location and therefore does not need to invent complex SIEM solutions. In the analysis, it is necessary to define as precisely as possible the number of devices sent their events to QRadar. These facilities in this company include:

Table 1: Small business solution and components

Component/locality 1)	Appliance
Console	QRadar 3105 (All-in-One)
Flow processor	
Flow collector	
Event processor	
Event collector	

- 1 UNIX and 12 Windows servers
- 2 databases
- 3 network devices
- 4 applications
- 45 workstations

Furthermore, one device generates flow records which is a flow probe positioned on the perimeter which analyzes network traffic and stations outside the corporate network.

Based on these data we were dimensioned necessary data for designing SIEM solutions that have been identified by calculations for individual parameters of a future solution.

Overall demand for storage events are TB 0.92 a month or 2.8 TB for the entire interval auditing. SIEM solutions based on IBM Security QRadar for such an organization requires the following elements:

- Console
- Event processor
- Event collector
- Flow collector
- Flow processor

So, there are implemented only necessary logical components for IBM security QRadar SIEM proposed solutions and distribution of various components including proposed this appliance for mid-sized company is shown in Table 1.

For processing and collection of events and data segments were selected physical appliance QRadar 3105 (All-in-One) that is part of its functionality is able to meet all the performance and capacity demands now placed. This appliance is capable in the basic version with 1000 EPS 25000 FPM and for purposes of storage capacity 9 TB space which is usable 6.2 TB.

These performance and capacity aspects far exceeds the requirements for a solution for this organization but it is important to realize that while maintaining the use of appliances and components only from IBM this is the best choice in price/performance ratio. Pricing and costing for all devices for this solution is shown in Table 2.

Mid-sized business implementation: This chapter deals with SIEM implementations for mid-size business in the banking sector which employs 235 workers.

Table 2: Cost calculation for small business proposed solution

License	Price (€)
IBM Security QRadar Core Appliance XX05 G2 Appliance Install Appliance+Subscription and Support (12 Months)	31 748 €
IBM Security QRadar SIEM All-in-One 31XX Install License+Subs and Sup. (12 Months)	79 226 €
Total (€)	110 974 €

Table 3: Locality 1 equipment for mid-sized business

Component/locality 1)	Appliance
Console	QRadar 3128 (All-in-One)
Flow processor	
Flow collector	
Event processor	
Event collector	
Capacity license	Up to 2,5 k EPS

Table 4: Locality 2 equipment for mid-sized business

Component/locality 2	Appliance
Event collector	QRadar event collector 1501

Table 5: Cost calculation for mid-sized business proposed solution

License	Price (€)
IBM Security QRadar Core Appliance XX28 G2 Appliance Install Appliance+Subs. and Sup. (12 Months)	84 534 €
IBM Security QRadar SIEM All-in-One 31XX Install License+Subs. and Sup. (12 Months)	79 226 €
IBM Security QRadar SIEM Event Capacity Increase from 1K to 2,5K EPS Install License+Subs. and Sup. (12 Months)	62 049 €
IBM Security QRadar Event Collector 1501 G2 Appliance Install Appliance + Subs. and Sup. (12 Months)	16 019 €
Total (€)	241 828 €

Table 6: Compared solutions for both companies

Attribute	Small company	Little company
Employees	48	235
Number of locations	1 location	2 locations
Number of devices	43	220
Audit requirements	3 month	6 month
Number of EPS	468	1110
Number of FPM	2412	23664
Capacity requirements	3,36 TB	17 TB
Kind of SIEM solution	QRadar 3105 (All-in-One)	QRadar 3128 (All-in-One), QRadar Event Collector 1501, Event
Capacity Increase from 1-2,5 K EPS Install License		
Price (€)	110 974 €	241 828 €

Very important information is that the information infrastructure of this company is divided into two geographical locations, hence, it is required to collect events from those two places. For implementation QRadar can use both physical and virtual solutions, in this case used a distributed physical solution because it was one of the requirements of the organization. Among the devices that generate records include:

- 20 UNIX and 150 Windows servers
- 20 databases
- 10 network devices
- 4 applications
- 220 workstations
- 2 equipment which generates flow records

Based on these figures it is then possible to dimension the implemented solution. Another necessary attribute is the size of the data store. For medium-sized companies, the value appropriate for the storage of events set at 2.18 TB per month. With respect to storage requirements which are 6 months, the total value of 13.08 TB. Monthly demand for storage capacity for a flow of 0.16 TB. For the period of six months is equal to the value of 1.12 TB. Overall, 14.2 TB, about 20% margin is 17 TB. SIEM solutions for such organization needs the same logical elements that were introduced in section 3.2 when designing a solution for a small company and so only necessary elements will be installed.

Proposed solution and distribution of various components including proposed this appliance for mid-sized company is shown in Table 3 for the first locality which is main location of company and where are located main infrastructure and in Table 4 for the second.

For the assembly and processed physical appliance was selected QRadar 3128 (All-in-One) which is in functionality defines everything what is needed for this infrastructure Table 5 and 6.

This appliance is capable of in a basic version with 1000 EPS, 25,000 FPM and for the purpose of storage there are 48 TB (of which 40 TB usable). As regards the aspects of performance to flow and storage requirements

for storage, said apparatus is ideal and with a reserve meets these requirements. However, it was found that the performance for the collection and Processed events is not sufficient. For this reason, you need to purchase a license which will upgrade this appliance to a level where it is able to exercise instead of the previous 2500, 1000 EPS.

For the second location where it is necessary to collect events from servers to be used collector event collector 1501 that his performance guarantee timely collection and delivery of the event to the all-in-one appliance at first location where events will be processed. Pricing and costs for all devices for this solution is shown in Table 5.

CONCLUSION

The implementation was carried out analysis of options and approaches on the issue of security of information and security events using the Security Information and Event Management (SIEM) from IBM. These problems include many technical and legal aspects and requirements that must be respected.

Part of the solution can be implemented in both companies is engaged and how to implement the IBM Security QRadar SIEM and is supplemented by a summary of the costs of this solution. Generally speaking, it describes the design and implementation can be applied to any organization while respecting aspects of company size and legal aspects and socially responsible.

During deployment several times showed the need for professional guidance and assistance because that issue is very complex and implementation without the necessary knowledge may sow the seeds of new problems. Coverage of the entire portfolio of threat is a process that is necessary to constantly perform and innovate and keep a list of current threats.

The solution was completed the acquisition of large practical skills and experience in analyzing environment described not only the environment but also other environmental or security solutions based on IBM Security QRadar SIEM.

In a practical solution described for both companies it was found that the proposed solution are important attributes that affect the resulting robustness SIEM solutions between these attributes belong:

- The number of company employees
- Geological division of IT infrastructure
- Fiscal aspects and limitations of the company
- The number and type of devices that are managed by the system
- The audit reporting requirements

Table 6 summarizes both solutions and attributes for comparison, use SIEM solution and price the cost of implementation of the proposed solutions. As can be seen from the accompanying table above the number of employees and those accessing the system, it is almost 5 times more for medium-sized companies. It also makes a difference whether the infrastructure is shared between multiple geographic locations. This requires additional appliance at the place where the rest of the infrastructure is placed.

Size claims FPM is based primarily on the number of workstations that are connected to the network as well as the number of servers that the organization wishes to be monitored by flow sensors.

Capacitive storage requirements are five times more for a medium enterprise which is only logical, if taken into account the number of events and flows which are stored.

This difference is also due to the fact that the audit interval, respectively, for data storage is for a medium enterprise 6 months. Interval for a medium enterprise is twice as long as for small businesses.

From a purely comparative purposes, it can be assumed that the interval was the same for both organizations. In this case, the difference between demands on both sites diminished. Capacity requirements for small organizations would have increased twice, thus, to 6.72 terabytes. After the change interval lengths auditing the resulting figures were only 2.5 times more in favor of mid-sized company. All the above factors have caused the final price solutions for SME is more than two times greater than in the case of a small business.

ACKNOWLEDGEMENTS

The research has been partially supported by the Czech Scientific Foundation project No. 15-11724S DEPIES-Decision Processes in Intelligent Environments.

REFERENCES

Barton, K.A., G. Tejay, M. Lane and S. Terrell, 2016. Information system security commitment: A study of external influences on senior management. Comput. Security, 59: 9-25.

Bedwell, P., 2014. Finding a new approach to SIEM to suit the SME environment. Network Secur., 2014: 12-16.

Bejtlich, R., 2013. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, San Francisco, California,.

Howell, D., 2015. Building better data protection with SIEM. Comput. Fraud Secur., 2015: 19-20.

Lee, C., C.C. Lee and S. Kim, 2016. Understanding information security stress: Focusing on the type of information security compliance activity. Comput. Secur., 59: 60-70.

Miller, D., H. Shon, A.A. Harris, S. VanDyke and C. Blask, 2010. Security Information and Event Management (SIEM) Implementation. McGraw-Hill, New York, USA., ISBN:978-0-07-170108-2, Pages: 429.