Journal of Electrical Engineering 5 (2017) 196-203
doi: 10.17265/2328-2223/2017.04.004

The Impact of Human Factors in the Implementation of SIEM Systems

Bojana Vilendečić[1], Ratko Dejanović[2] and Predrag Ćurić[3]

1. M:tel a.d. Banja Luka, Direction for Technic, Banja Luka, Bosnia and Herzegovina

2. Faculty of Electrical Engineering, University of Banja Luka, Banja Luka, Bosnia and Herzegovina

3. NLB Banka a.d. Banja Luka, Branch Office Banja Luka, Banja Luka, Bosnia and Herzegovina

Abstract: This paper describes the process of the implementation of SIEM (security information and event management) systems in IT environment and the impact of human factors on that process. In the introductory part of the paper are listed security systems which are most often used in corporate environments, the key functionalities of SIEM systems and its importance in overall security of the IT environment. Then, the recommendations are listed for the successful implementation of SIEM systems, which goal is a higher level of corporate network environment security. It is further presented optimization of implementation of the SIEM systems through all stages. Further, the influence of the human factor is described in the implementation of these systems as well as the impact of human perceptions in correlations to the detection of attacks.

Key words: SIEM, security, correlation.

1. Introduction

In the IT environment, each administrator continuously monitors security information and events that are generated by system not only to detect error in operations, but also for detecting attacks. Administrators, except reviewing above described records, have regular daily tasks to perform and analyzing a large number of records can pose a painstaking job or be considered as a casual commitment. Both of these approaches have negative aftermath if we look at it from security point. Incidents are usually detected by analyzing logs of multiple different systems of corporate network that are often administered by different administrators, and real attack may be undetected and unnoticed regardless of the time that administrator spends by analyzing the logs of the systems. The same happens when administrators neglect analysis of logs and devote other maintenance activities of the system.

Corresponding author: Bojana Vilendečić, bachelor of electrical engineering, B.E.E., research field: information security.

Along with the trend of increasing number of the security threats and complexity of attacks, also increases the number of different types of security mechanisms to monitor and protect against attacks increases. Completely safe environment does not exist. Companies that care about the security of their corporate IT environment use a large number of systems of protection: Firewall, Intrusion Prevention System, Web Application Firewall, Database Firewall, Intrusion Detection System, Anomaly Detection System, Web and database vulnerability scanners, antivirus system and other. These are only the most commonly used systems of protection in corporate network environment which is shown in Fig. 1. Accordingly, every system generates a large amount of information that can be of the crucial importance for security of the entire corporate IT environment (servers, workstations, security systems and others). It comes to the conclusion that almost every company that aims to set security level to an acceptable level should implement one system that will centrally collect security information and events, normalize them

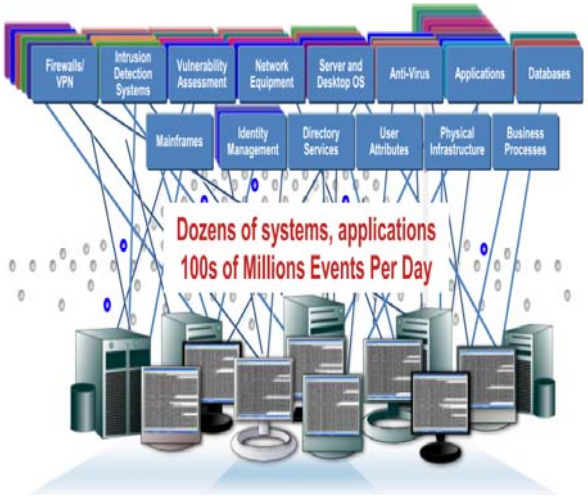

Fig. 1 A variety of systems and applications of corporate networks and hundreds of millions of daily events [1].

whereas every system generates specific format of log, analyze and correlate collected data in real-time in order to detect security attacks and automate all previously listed. Such systems are called SIEM (security information and event management) systems.

2. The Implementation of SIEM Systems

The implementation of SIEM systems [2] requires previous analysis and planning of implementation. In this context, analysis and planning of implementation implies:

- define the security goals of the company,
- implementation of the internal security policies which exactly prescribe what and which level of logging should exist on certain system, and which security and monitoring system reports should be imported in SIEM in order to achieve security objectives of the company,
- define the period of keeping data on SIEM system in accordance with the security objectives of company and/or legal regulations,
- determination average number of generated events per second—EPS (events per second) per system that generate data of interes for SIEM system (taking into account the planned expansion of the IT environment) and the total number of EPS,
- determination of the number of sources (taking into account the planned expansion of the IT environment).

Based on the above steps of analysis and planning the implementation, should be performed the dimensioning of the system to meet the requirements for memory space required to store data desired time period and the system should be dimensioned to support the processing of a certain total number of EPS and the desired number of sources of data [3].

When the system is properly dimensioned, a minor problem is the choice of the system. The Gartner's Magic Quadrant helps many companies regarding the choice of the system. The following figure (Fig. 2) shows the Gartner's Magic Quadrant for SIEM 2015. After analyzing and planning the implementation and electing the system, it follows the phase of the implementation of the system. At first, if it is not already, it should be configured the logging/auditing on the systems that are planned to be log sources according to defined level of logging. Log sources also need to be configured in SIEM system and this step is the final step of configuring automated centrally collecting data. SIEM performs normalization of the collected data of different formats into the unified format so searching, analysing and filtering of data become very easy.

Fig. 2 Gartner's Magic Quadrant for SIEM systems for 2015 [4].

Key functionality of SIEM systems is the possibility of automated correlations of the collected data. This functionality is the main (but not the only) difference with Log Management systems, which makes SIEM systems more superior from the security aspect. Correlations of the data are performed automatically and in accordance with configured rules. When correlation rules are created it is very important to take into account results of the correalation rules which need to be led by advance defined security goals regarding implementation of the SIEM system. This is the most difficult step of the implementation, because correlation rules request continiously improvment in order to minimise the number of false positive results of correlations. So, setting up the correlation rules never stops. A team of security experts, trained for working on SIEM system, continiously monitor the new security threats and the signatures of the attacks and continiously create, analyse and improve new correlation rules. It is desirable to document the procedures of creating, analysing and setting correlation rules in order to define a method of tuning up the correlation rules. It is also good to keep the results of the correlation rules (number of false positive warning) because these results are good indicator for the correlation rules improvment (for example decreasing the number of false positive results after tuning up the correlation rule) [5].

Each SIEM system has a set of predefined correlation rules used for the detection of known attacks. In most implementations, these predefined correlation rules are used after implementation but team of security experts continiously analyze results of them in order to exclude those who are not in interest of specific IT environment safety, because those correlation rules unnecessarily burden the SIEM system. Those ones, that are in interest of the specific IT environment will continue to be used but these are going to be tuned up on the same method as previously described especially created correlation rules. There is briefly described the process of the correlation rules creation, analyzing of the predefined correlation rules and fine-tuning of the correlation rules which is the most challenging step of the implementation of SIEM systems.

The second demanding step is establishing the process of the responding to the alerts. With the predefined algorithms for determining the relevance and the criticality of the correlation results, SIEM also offers the possibility of adjusting them. The practice shows that it is the most effective to reduce the number of the responding processes to the alerts on the lowest possible number. It should be created a new process of response on some alert only if it does not yet exist one applicable. Therefore, it would be ideal to reduce the number of different responses to the alerts, all the way to the limit of the process existence to every alert, so that there is a response for every alert. These processes define what is acceptable “good” behavior and show whether some changes are needed in corporate network. It is necessary to continiously analyze each offense/alert, the correlation rules that generate it, group of events/activities that fulfill conditions of correlation rule and trigger an offense, consider possibility that it is a false positive alert and discover what should be changed in correlation rule to stop generating false positive offenses/alerts. In this case, the following gold rule applies: More time spent on analyzing only one alert means less time spent on analyzing the other alerts. Less time spent on analyzing one alert means more undiscovered malicious activities (Fig. 3). When an appropriate process of response on alert is established, it should be documented on the repeatable way and available to all members of security team.

Text that follows, describes a simple example of the data collection for the SIEM system, creation of the correlation rules, analysis of the alert and defining response to a possible incident. It is shown the process of stablishing a dinamic list of users of oracle database and monitoring new legitimate and suspicious users. It

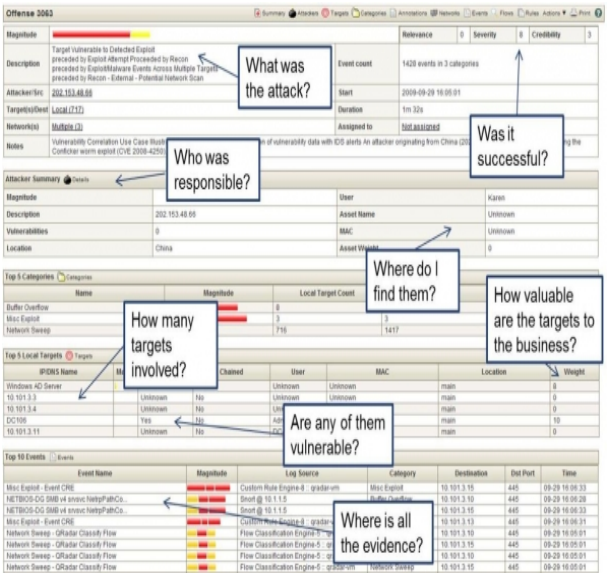

Fig. 3 Analysis of an alert [6].

was assumed that the database auditing is enabled (for example, parameter audit_trail = "DB"—enable audit and keep data in database table sys.aud$) and auditing of all logins to Oracle database is enabled (statement AUDIT SESSION). On the SIEM side of the system, according to the manufacturer's procedure, a new log source is configured—oracle database and collecting audit data (it depends on the supported protocols—the most often is necessary to create database account which SIEM uses for accessing dba_audit_trail by JDBC protocol). After that SIEM is supplied by data needed for establishing list of database users in real-time. The reference list can be updated by administrators and by correlation rules. Correlation rules check the following conditions: the destination IP address should be the same as IP address of database server, log source should be that database on that server, name of event should be name which corresponds to sucessful logon event (LOGON SUCCESSFUL) and attribute. Username of that event is not in the reference list of database users. If they are all conditions fulfilled, simultaneously is triggered alert regards the new user and started updating of the user list with the new user username. Applying this correlation rule, the reference list of database users is updated each time when a new user successfully logs and alert about new users is triggered. Every alert should have an appropriate response to that alert. Security team analyzes all alerts and should check a new user. In almost all of companies, it is common to apply for the request for creating a new user database account and to comply with the prescribed convention rules for database accounts, but also, the creating database accounts are approved through telephone official lines for the purpose of emergency interventions on the database. The lack of an approved requirement for creating database account or ignoring the naming convention are the most common indicators of suspicious accounts. The response on this alert depends on the results of the analysis and could result in disabling suspicious account and deleting username of that account from the list of database users, or only renaming account or disabling compromised account by which is created suspicious account and all accounts which are created by this compromised account. It analyzes how and why that account is created (misuse of administrator privileges, compromising of privileged account and creating a new account, ignoring prescribed procedure for account creation process omitting approved request etc.), which privileges are assigned to suspicious account, which activities are successfully performed by that account etc.

For automated checking existance of approved requests for creating a new database accounts for every first-time login, it needs to be created a correlation rule and a reference list of approved requests. In this case, the reference list is filled by administrators who fill the username of account in reference list after receiving approved request and before creating account. Correlation rule has the same conditions like previously described rule and one additional condition—the reference list of approved database users that does not contain this username. An offense/alert is triggered if all conditions of correlation rule are met. The response on this alert should be blocking that account as in preceding

example. So, this correlation rule triggers alert if a new user whose username is not in reference list of approved database users successfully logins, and if there doesn't exist approval for creating that user account. The application of this correlation rule requires regular updating of the reference list of approved requests for creating new users in the database. Otherwise, a number of alerts would be false positive. The application of the response on the alert disables the accounts of legitimate users if database administrators do not update the reference list regularly. The application of this correlation rules is desirable in every ISO27001 environments. Both, previously described, examples are applicable in almost all of environments.

3. The Optimization of the Implementation of SIEM

Many of the implementations that were not preceded by analysis and planing, did not give a positive security result nor contributed to a higher level of IT security environment and the possibilities of optimizing the implementation of the SIEM system are visible already in this phase of the implementation. The analysis and planning process not only facilitate the implementation, but they are necessary for optimal system dimensioning. Unless a good environmental assessment is made related to the total number of EPS or memory space, it happens that the system cannot process a sufficient number of EPS which are generated on systems in corporate network or can not meet the requirements of the law or internal security policies regarding the time period of data storage.

It is possible a cost saving related to the licence of SIEM system for a smaller number than real number of log sources which send data to SIEM system. SIEM systems are usually licensed, beside by the numbers of EPS, by the number of log sources which send data to SIEM system. IT environments even before SIEM implementation usually already have implemented Log Management system or some syslog server to whom are sent logs from network devices by the syslog protocol. Let assume that one such a syslog server collects logs from 300 network devices. If syslog server is considered like one log source, than SIEM collects data from 300 network devices per one log source, but if each from all 300 network devices is considered like one log source than SIEM have comletely the same data but an appropriate licence for SIEM is more expensive. All this depends on the SIEM system vendor licence metric, because it is possible by this way to make a huge cost saving by some SIEM systems vendors while the other vendors licences SIEM systems by the number of ending devices.

Cost savings can also be achieved by using already existing Log Management system and implement only upgrade of this system that has all key functionality of SIEM system. One of these systems is ArcSight Express. If the upgrade of Log Management system is possible, then it is possible not only the cost savings, but much simpler implementation. Planning the Log Management system implementation is very similar as planning SIEM system implementation and it is considered that in such environments already have been defined log sources and the most important logs. Experiences with Log Management system and environment needs for an upgrade of the existing system indicate that environment is "ripe" for the implementation of SIEM system and it is known in advance what is the goal of that implementation. Security experts even recommend this kind of implementation of SIEM system, step by step, from the Log Management system to SIEM system.

It is necessary to supply SIEM system with as much as possible data of interest in order to achieve good analysis. The rule applies here is "data analysis is better with more available data on SIEM system".

It requires a lot of time in order to achieve defined security goals with the SIEM system implementation. As much as the implementation of the SIEM system seems to be simple at first, it is necessary to know that

it is only inicial implementation which involves locating network devices, configuring basic network parameters and collecting logs from network systems. Implementation of SIEM system that has a goal to achieve higher level of security in the entire network never stops. Correlation rules adjustment is an iterative process and by analyzing the results of the created correlations the methods for decreasing the number of false positive/negative results are constantly revealed. When the correlation rule is created, the results of these correlations are analyzed for a while, then the correlation rules are fine-tuned in order to reduce the number of false-positive results and set appropriate thresholds of correlation rules. The thresholds can be set too high resulting in unnoticed actual attacks, while on the other side, too low thresholds can give a large number of false positive alerts. The security team has the task of following the latest threats, and with new threats and new attack models, it is necessary to create new correlation rules or adjust those which are already created to detect new types of attacks or suspicious activities.

4. The Impact of Human Factors in Implementation of SIEM Systems

The previously described implementation requires continuous engagement of the security team and the influence of the human factor is evident. Despite the fact that SIEM is a system that performs automated correlations and desired detections, this system can detect attacks only on the basis of data analysis collected from the IT system. However, today's hackers perform attacks by combining various vulnerabilities, including social engineering and physical access to IT systems. SIEM system cannot detect such attacks because it only analyzes data collected from an IT system not including human intelligence or perception. SIEM system cannot notice the information that people can e.g. that some official laptop or mobile phone with confidential data and credentials has been stolen or lost, that someone has tried to find out the password of admin account during a conversation with the administrator etc.

Standard ISO/IEC 27001 covers human resources, records management, business continuity and risk management (A.13.1—Information Security Incident Management; A.13.1.1—Reporting information security events and weaknesses; A13.1.2—Reporting security weaknesses etc.). Implementation of the SIEM system meets the standard requirements and contributes to its implementation. It can be concluded that the SIEM system, although it has a built-in high intelligence, would give the best safety results in combination with human perceptions. The question is how to provide the system with information that human can conclude or observe. It is not impossible to develop interface which provides supplying SIEM system with security informations which are the result of human perception or thoughts. For example, a seemingly harmless phone call of an unknown person who urgently asks for a password to access an IT system could be a good input to the SIEM system for further security analysis of that system. Additionally, if firewalls and IDS (intrusion detection system) show more malicious activities targeted at this system, the level of criticality of this alert is raised. This is just a simple example of malicious activity detection where the input data are human perception.

There are numerous abuses initially suspicious only to humans, and later analysis can confirm that they are

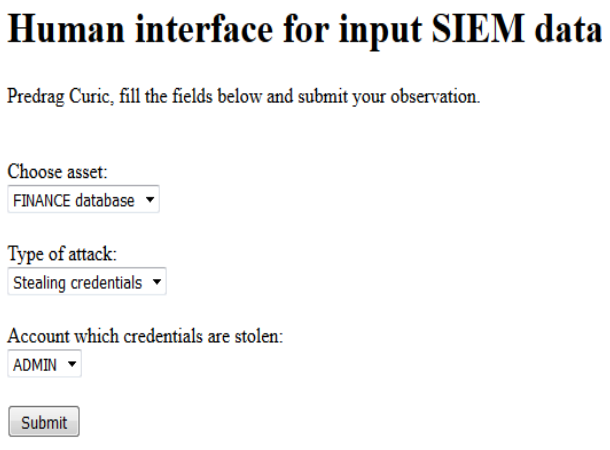

Fig. 4 User interface for data entry.

not only suspicious but malicious. All on-site visits, as well as maintenance of a company's IT system by non-employees with the maintenance contract, may be suspicious. When credentials of employees are written on paper on the desks, even the cleaners staff, secretaries and any other person who enter in the offices can be suspicious. But all of above listed is not possible to detect by any IT system including SIEM unless there is an additional interface developed for data entry of that type. People are sometimes the best detectors of unusual activities and possible abuses. In a large number of cases, employees do not have anyone to report or they are hesitant to do so. Reasons for employees scruple to report suspicious activities are numerous: they consider that their suspicion is irrelevant, they are afraid of ridicule by security team or the other employees, they are afraid of negative consequences or punishments, they feel embarrassed because of thought that they were reported or suspected the wrong person etc. If the interface for data entry of this type would be developed and adequately defined the ways in which these data would be entered/reported, along with the employees education about the importance of their involvement in raising the level of IT security environment, employees would be encouraged to report such cases and intelligent SIEM systems would be enriched with human intelligence, which would certainly result in a higher level of IT security environments.

The development of such interface for SIEM system was one of the themes published in RSA Conference 2014 which took place in San Francisco [7] and in this paper is used only as an idea for optimizing the implementation of the SIEM system and maximizing the usability of these intelligent systems. The development of that interface requires detailed analysis and planning. In order to make the interface model of functioning, it is necessary to explore the ways in which a person can influence the security of the information system and to consider which group of employees is the most critical regarding to manipulations related to access to information systems and to define vectors of combined attacks that need to be monitored. Designing a web application that generates the desired logs comes at the end. The simplest application would offer to the users a choice of predefined systems (e.g. database with personal data), then choice of type of combined attack that can be reported and the ability of the risk level assessment and optional description addition. An application would need to generate a log record as an output that sent them to an SIEM system, in which all logs keep stored on a centralized location and correlate them with other logs and security informations for attack detection.

5. Conclusions

Numerous functionalities of SIEM system significantly facilitate the job of every administrator individually because, by the implementation of the SIEM system, all events and security information are collected, analyzed and correlated on centrallized location. It is evident that a human factor has a big impact on a successful implementation of the SIEM system—the expertise and competence of the security team, training of employees, dedication of security team to the correlation rules adjustment and establishing a mechanism for responding to incidents and human observations regarding IT safety. Correlation of human observations and data available to SIEM systems could be possible. Developing an application as an SIEM interface for entering logs that carry human-perception information means a lot in the security of the entire IT environment and covers part of the detection of non-technical threats and weaknesses of each environment. Non-technical attacks are very difficult for detection and processing, particularly to the systems, and possibility of automated correlations human observations and security informations and events generated by all IT systems, contribute to the overall security of the IT environment.

References

[1] Radosavljević, A., and Milojević, S. 2011. "Arcsight Solution for Log Management—Case Study of Information System by Telekom Srbija, S&T Serbia, 2011." Accessed April 29, 2017. http://idcrussia.com/ru/events/39016-idc-it-security-and-datacenters-transformation-roadshow-2011/10-agenda, http://idcrussia.com/dwn/PRES_37977/aleksandar_radosavljevic_s_t_srdjan_milojevic_telekom_srbija.pdf.

[2] Miller, D. R., Harris, S., Harper, A. A., VanDyke, S., and Blask, C. 2011. *Security Information and Event Management (SIEM) Implementation.* New York: McGraw-Hill.

[3] Butler, J. M. 2009. "Benchmarking Security Information and Event Management (SIEM)." SANS Whitepaper.

[4] http://www.splunk.com/goto/SIEM_MQ (accessed April 29, 2017).

[5] http://blogs.gartner.com/anton-chuvakin/2015/11/25/siem-use-case-implementation-and-tuning-process/ (accessed April 29, 2017).

[6] van Zadelhoff, M., and Mulligan, B. 2013. "IBM Security Systems—Disrupt the Advanced Attack Chain with Intelligent, Integrated Security, Security Inteligence: Think Integrated, November 2013." [Online], accessed April 29, 2017. http://www.slideshare.net/ibmsecurity/disrupt-the-advanced-attack-chain-with-intelligent-integrated-security.

[7] Wesselmann, B., and Wiele, J. 2014. "A Human Factor Interface for SIEM." RSA Conference, San Francisco. [Online], accessed April 29, 2017. http://www.rsaconference.com/events/us14/agenda/sessions/935/a-human-factor-interface-for-siem.