Effectiveness of Security Incident Event Management (SIEM) System for Cyber Security Situation Awareness

Bandr Siraj Fakiha

Assistant Professor, Department of Medical Health services, Faculty of Health Sciences, Umm Al-Qura University, K.S.A.

Abstract

Cyber-attacks have always targeted information communication technology systems of various organizations. Intruders and hackers have within their reach, very powerful tools through which they capable to bypass the existing network security so as to deliver a payload that might have a severe impact on the whole organization. Therefore, it has become essential for organizations to develop mechanisms through which they can detect a possible cyber threat and then respond accordingly. By establishing cybersecurity situation awareness, organizations will understand what is happening and then respond effectively. The present study evaluated the effectiveness of the Security Incident Event Management (SIEM) system for Cyber Security Situation Awareness. A Hierarchical Network Security Situation Assessment Model (referred to HNSSAM) which joins Security Incident Event Management (SIEM) system evidence theory fusion rules with classified quantitative risk assessment method was applied. Data processing was initially designed so as to collect security data from various sensors. Mechanisms for data verification were then adopted so as to establish whether SIEM was effective in successfully detecting any form of cyber-attack. Results show that SIEM tools may be applied by security analysts to gain visibility into the security threats attacking the IT systems of an organization and then respond appropriately.

Keywords*: SIEM, Security, Cybercrime, IT systems, HNSSAM, Cyber-attack, Network, Technology, Cyber threats, Information.*

Introduction

The development of Information Communication and Technology is argued to have gone hand in hand with the emergence of a number of cybersecurity threats and vulnerabilities. The problem of computer security involves a form of deliberate act that can affect the three essential properties of a given information system [1]. The properties outlined in this case include the confidentiality, for example, the ability of network or computer system to store relevant information which is considered as sensitive to the business in a secured manner and maintaining some aspects of exclusive access to only relevant users who have been designed for that purpose. The second property is integrity, the assurance that all the programs and data or the available information are properly designed and modified only within a given manner authorized or acceptable by the company authorities [4].

The problem of cybersecurity has the potential of impacting on the individual users, both big and small business organizations, resulting into a number of financial implications like direct cost such as theft of money, digital assets and sensitive information [2]. Cyber threats also have the possibility of causing indirect costs in the general form of interrupting the business services, lower productivity, as well as legal liability that takes place due to diverted resource like computing power, personnel, capital and bandwidth which can further lead into some given costs that are associated to the long-term impact of the security attack on the image of the

Corresponding Author:
Bandr Siraj Fakiha
Assistant Professor, Department of Medical Health services, Faculty of Health Sciences, Umm Al-Qura University, K.S.A.

organization, bad reputation, competitiveness as well as the financial markets [3].

Despite the challenges associated with cybersecurity, most business companies are constantly going through a radical transformation for the need for embracing the current age of information [10]. This has always ended up making them rely on information technology for the need of handling some important part of their main service deliveries and consequently, a proper asset that is very valuable for the information of the whole organization. Protection against the risk associated with cybersecurity is one of the most important things that the current business organizations are up to [13]. Very many organizations are moving forward towards creating E-service and making their information more digital, convenient, accessible, and secured. But this has greatly come with several risks, a serious cyber threat [5]. The information is likely to be stolen, hacked, wiped or even sabotaged. The literature identifies that cyber breaches are serious threat not only to business but also to the security of all the devices and people involved. As per some statistics, cybercrime actually costs several businesses all over the world more than $400 billion annually. What is even troubling from the perspective of information technology is the fact that cyber-criminals are trying to ostensibly breach secure systems with several layers of protection that are put in place [10]. The present article seeks to establish the effectiveness of Security Incident Event Management (SIEM) system for Cyber Security Situation Awareness among companies. By establishing cybersecurity situation awareness, organizations will understand what is happening and then respond effectively.

Material and Methods

This section proposed a Hierarchical Network Security Situation Assessment Model (referred to HNSSAM) (Figure 1). The model joins Security Incident Event Management (SIEM) system evidence theory fusion rules with classified quantitative risk assessment method and applies confidence level, host importance and service importance. The advantage of using this model is to solve the problem of processing mass data, to offer three different levels of intuitive security threat, and to subsequently establish the weaknesses within the system or rather the security situation.

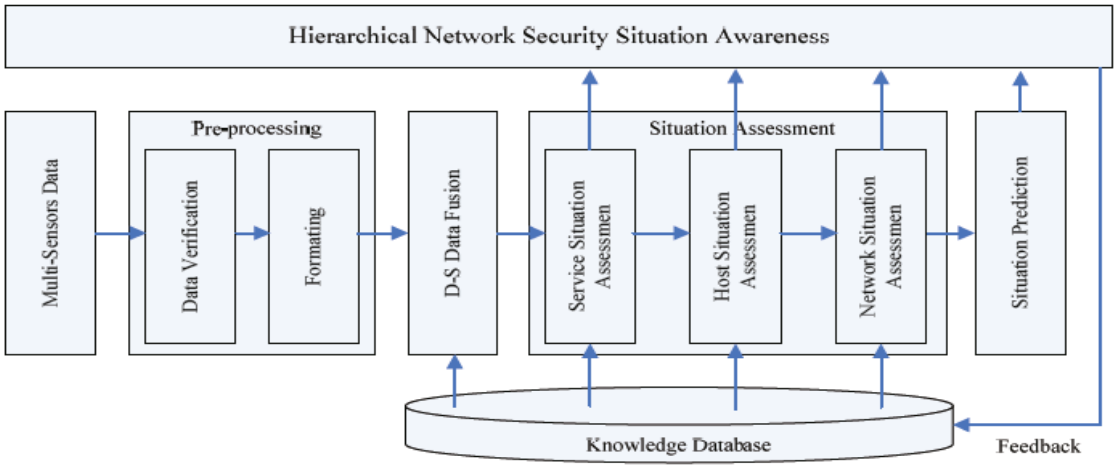

Figure 1: Hierarchical framework for network security situation awareness

Data pre-processing was initially designed so as to collect security data from various sensors. Mechanisms for data verification were adopted to determine whether SIEM was effective in successfully detecting any form of cyber-attack. Through a comparison of relevant conditions as well as configuring information that were considered essential for any form of successful cyber-attack, the researcher would simply remove the non-impact attack alert. For example, IDS did successfully detect a great number of serv-u directory traversal attacks which actually aimed at serve-u software running on Windows system. However, the target host was run on the Linux system, so that attack could not be succeeded. The security data was then converted into some sorts of

uniform format to realize the HNSSAM architecture.

As per the basic description of SIEM, the researcher did set the target framework as either True positive or False Positive. Considering the fact that the alerts that are generated by the security equipment had two possibilities; true positive and false positive, the researcher defined confidence values of an alert as True Positive Rate (TPR): m (correct alerts) = TPR. The researcher did get TPR through the supervised training of the relevant security devices in numerous forms of attacks. The confidence values were subsequently stored within knowledge Base for an additional usage. The fusion process is demonstrated in the figure below.

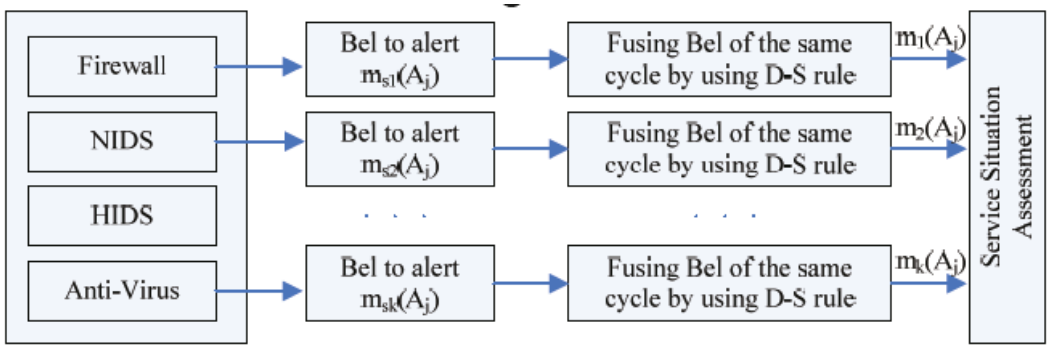

Figure 2: Illustrating the fusion model that is D-S rule-based alert

In order to test the effectiveness of SIEM, the researcher subsequently simulated a multi-sensor network environment as shown in figure 2. In such simulated network environment, the researcher did deploy four distinctive sensors, the firewall at the internet entry, network intrusion detection system, the detection system of host intrusion as well as the specific anti-virus software that are installed within the hosts.

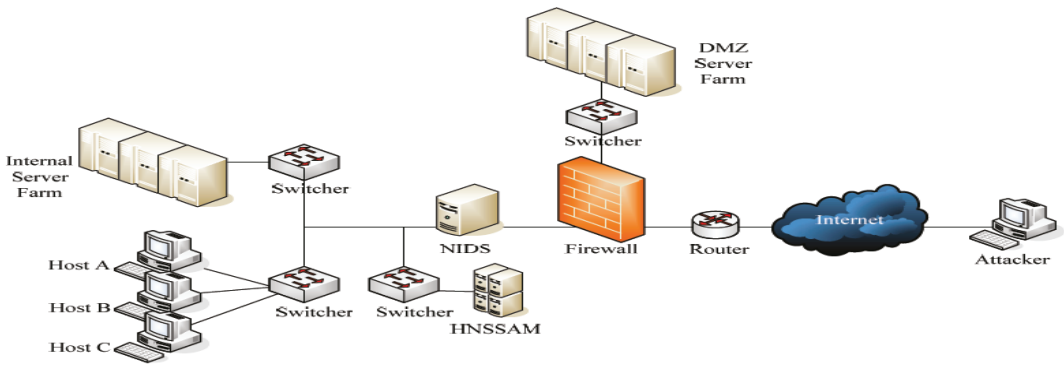

Figure 3: Illustrating the investigational network topology

A day was divided into three different periods: t1 = 0 ~ 8, t2 = 8 ~ 18, t3 = 18 ~24. Each period was subsequently assigned with varied significant level. The observed time T1 and T6 did fall under period t3, T2 ~ T3 felt in the period t1, T4 ~ T5 felt in the period t2. As from T1 to T6, information was collected for SIEM detection of an attack on the host A, B, C.

Based on the collected security data, the researcher looked up the level of confidence that correspond to the security data within the knowledge base. By the fusion rule of DA, the researcher fused the confidence value. The results were then multiplied by the brutality value of attacks within the knowledge base. The results were subsequently drawn as shown in the figure below. It could clearly be demonstrated from the results, as shown in figure 4, that the services of RPC on the Host A suffer a very high level of threats which need to be given first priority. The researcher generated the host security as illustrated in figure 4b. It seen that attacks were more active during the period of T1 to T4.

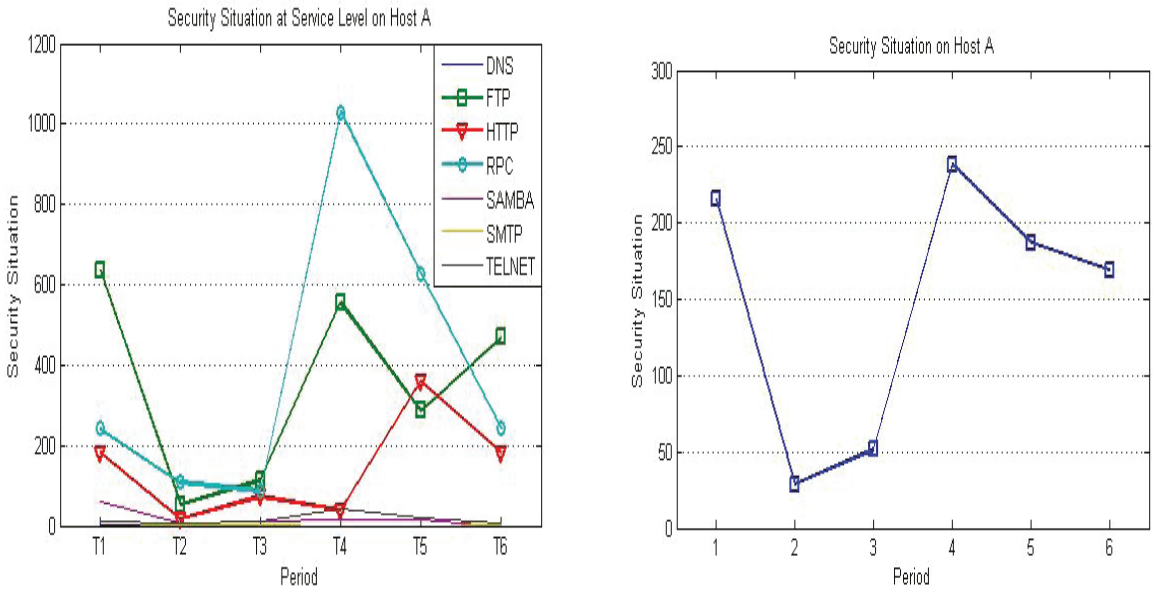

Figure 4. (a) Situation of security in all the services within host A; (b) Host A security situation

As per the analysis of the results that had already been generated, it was possible to draw the security situation of all the hosts as shown in Figure 5a. From the figure, it was possible for the administrators to establish the level of threat on every host.

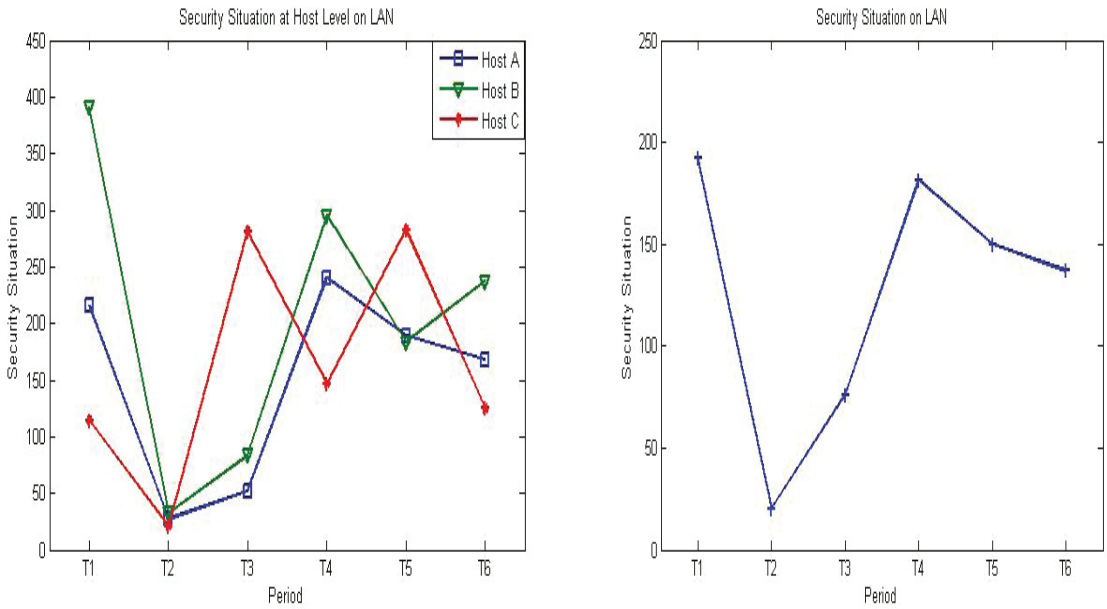

Figure 5. (a) The security situation of all the hosts on LAN; (b) The security condition of LAN

Findings

As per the methodology above, it can be observed that the SIEM framework offer three different levels of cybersecurity situation. The method in this may significantly overcome the shortcomings of the present hierarchical situation awareness systems. It might subsequently help the relevant decision-makers to adjust their policy so as to enhance company security.

These findings show that SIEM tools help security analysts gain visibility into the security threats attacking the IT systems of a given business organization. This is done by examining the logs generated by network devices and searching for signs of an on-going attack. The biggest challenge faced by SIEM systems is the

affectivity of filtering the data being displayed to the security analysts. The SIEM system is able to correlate a large amount of logs multiple sources of logs and identify an attack with a high detection rate and low false-positive rate. This is done while prioritizing alerts so that security analysts can focus on attending to the high threat alerts generated by the system.

Moreover, security analysts are able to classify the different components from the various departments so they can priorities threats and respond to the most critical threats first. As the amount of cybercrime increases worldwide, having a clear legal framework for dealing with it is critical [12]. SIEM system structures the accumulation, analysis and correlation of events that occur from diverse sources. Management of threats, response to incidences and management of log comprise of the key capabilities of the current SIEM solutions.

Even though it has widely been reported that SIEM has matured within the recent years, the system still depends on the previous complex rules in detecting security threats [11]. However, it is important to note that correlation which is rule-based can never be sufficient in protecting information from security threats that are continuously evolving and become dynamic. There is a high need for complementing correlation which is rule-based with techniques which are more advanced like detection of an anomaly for quite a good number of reasons. First, it is a fact that the rule-based system only has the ability to detect incidents that had been defined and observed earlier. In most of the circumstances, a zero-day threat which is not known might fail being detected by the current appliances and hence results into great damage due to leakage of data or downtimes of the network [6].

Discussion

SIEM is a security tool that can be utilized in strengthening the security of communication and information systems just the same way it is always witnessed with firewalls, antivirus software and schemes for access control. It is a kind of device or application of the software that screens system or network activities that are related to violation of the policy or malicious activities and release a report to the station of management [8]. Even though this technology of detecting the intrusion is somehow immature and hence need not to be considered as a reliable defence, literatures argue that it plays some important role within the information security architecture [18].

Since any form of deployment is likely to incur some costs for maintenance and operation, each individual organization utilizing this kind of device need to consider the full life cycle of SIEM before coming up with a valid choice [9]. In the event that SIEM is installed appropriately, it would be providing some warnings that indicate that the system is being attacked from elsewhere even in the circumstances when there is no specific attack that the system is vulnerable to [15]. Such warnings can assist the users in altering the defensive posture of the installation so as to increase the resistance of the system to the attack. Additionally, SIEM might also serve to confirm operation and configuration which is secure of other mechanisms of security like firewalls. With regards to the disadvantages it is possessing, it can be applied for defensive posture; though need to be fully relied upon as the only means of system protection [16]. The situation of information system security is likely to worsen as the issues of e-commerce continue to become more attractive to the targets.

A network-based SIEM system, on the other hand, is a kind of system that is designed to detect malicious activity for instance service attacks denial, port scans or even any form of attempts of cracking into the computer by network traffic monitoring [17]. This kind of system is able to read all the packets that are incoming with the aim of getting any form of suspicious patterns described as rules or signatures. If for instance, a big amount of TCP connection requests to numerous numbers of dissimilar ports is observed, then it is possible for one to assume that there is an individual who is doing a port scan to all the computers found within that network [19]. The third classification of SIEM, which is anomaly-based, revolve around first determining the behaviour profiles of the users, programs or other resources that have an interest to the given system and then making an observation to the actual activities as generated within the audit data so as to detect any deviation considered significant from the existing profiles [14]. Detection of an anomaly, in this case, is statistical in their nature. In order for the system to detect security threats at its early stages, all individual's system log files need to be analyzed and correlated [7].

Conclusion

Cyber-attacks have been, in many instances, targeted on information communication and technology systems of different organizations. Hackers and intruders currently have within their reach; very lethal tools through which they can safely bypass the existing network security to deliver payload that have a great negative impact on the entire system. Cyber threats have always continued to exploit the connectivity and complexity within the important infrastructure to make a plan and launch attacks on the existing computer systems. This has been a great challenge experienced by different business organizations. In order for any business organization to be safe from cyber threats, they require a complex security system that can protect the existing computer networks from dangerous threats. The security system can comprise of firewalls, a system that detects and prevent intrusion and solutions for path management, together with some strong anti-virus.

Ethical Clearance: Nil.

Source of Funding: Nil.

Conflict of Interest: Nil.

References

[1] Garfinkel S, Spafford G. Web security, privacy & commerce. " O'Reilly Media, Inc."; 2002.

[2] Cuppens N, Cuppens F, Lanet JL, Legay A, Garcia-Alfaro J, editors. Risks and Security of Internet and Systems. Springer International Publishing; 2018.

[3] Kung A, Kargl F, Suppan S, Cuellar J, Pöhls HC, Kapovits A, McDonnell NN, Martin YS. A privacy engineering framework for the internet of things. InData Protection and Privacy:(In) visibilities and Infrastructures 2017 (pp. 163-202). Springer, Cham.

[4] Wang P, Chaudhry S, Li L, Li S, Tryfonas T, Li H. The Internet of Things: a security point of view. Internet Research. 2016 Apr 4.

[5] Lopez J, Rios R, Bao F, Wang G. Evolving privacy: From sensors to the Internet of Things. Future Generation Computer Systems. 2017 Oct 1;75:46-57.

[6] Yousuf T, Mahmoud R, Aloul F, Zualkernan I. Internet of Things (IoT) Security: Current status, challenges and countermeasures. International Journal for Information Security Research (IJISR). 2015 Dec;5(4):608-16.

[7] Bhatt S, Manadhata PK, Zomlot L. The operational role of security information and event management systems. IEEE security & Privacy. 2014 Oct 15;12(5):35-41.

[8] Leszczyna R, Małkowski R, Wróbel MR. Testing situation awareness network for the electrical power infrastructure. Acta Energetica. 2016.

[9] Onwubiko C, editor. Situational Awareness in Computer Network Defense: Principles, Methods and Applications: Principles, Methods and Applications. IGI Global; 2012 Jan 31.

[10] Huynen JL, Lenzini G. From situation awareness to action: an information security management toolkit for socio-technical security retrospective and prospective analysis. InProceedings of the 3rd International Conference on Information Systems Security and Privacy 2017.

[11] Albanese M, Cooke N, Coty G, Hall D, Healey C, Jajodia S, Liu P, McNeese MD, Ning P, Reeves D, Subrahmanian VS. Computer-aided human centric cyber situation awareness. InTheory and Models for Cyber Situation Awareness 2017 (pp. 3-25). Springer, Cham.

[12] Albanese M, Cooke N, Coty G, Hall D, Healey C, Jajodia S, Liu P, McNeese MD, Ning P, Reeves D, Subrahmanian VS. Computer-aided human centric cyber situation awareness. InTheory and Models for Cyber Situation Awareness 2017 (pp. 3-25). Springer, Cham.

[13] AlSabbagh B, Kowalski S. A Framework and Prototype for A Socio-Technical Security Information and Event Management System (ST-SIEM). In2016 European Intelligence and Security Informatics Conference (EISIC) 2016 Aug 17 (pp. 192-195). IEEE.

[14] Radanliev P, De Roure DC, Nurse JR, Montalvo RM, Burnap P, De Roure DC, Nurse JR, Montalvo RM, Cannady S. Design principles for cyber risk impact assessment from Internet of Things (IoT). University of Oxford. 2019.

[15] Borgolte, Kevin, Tobias Fiebig, Shuang Hao, Christopher Kruegel, and Giovanni Vigna. "Cloud

strife: mitigating the security risks of domain-validated certificates." (2018).

[16] Goldstein M, Asanger S, Reif M, Hutchison A. Enhancing Security Event Management Systems with Unsupervised Anomaly Detection. InICPRAM 2013 (pp. 530-538).

[17] Kotenko IV, Polubelova O, Saenko I. Data Repository for Security Information and Event Management in Service Infrastructures. SECRYPT. 2012 Jul;24:308.

[18] Menges, Florian, Fabian Böhm, Manfred Vielberth, Alexander Puchta, Benjamin Taubmann, Noëlle Rakotondravony, and Tobias Latzo. "Introducing DINGfest: An architecture for next generation SIEM systems." 2018 (257-260).

[19] Chuvakin A. The complete guide to log and event management. Dosegljivo: https://www. microfocus. com/media/whitepaper/the_complete_guide_to_ log_and_event_management_wp. pdf.[Dostopano: 7. 9. 2019.]. 2010 Mar.