Significance of Security Information and Event Management (SIEM) in modern Organizations

Meenu Chopra, Cosmena Mahapatra

Abstract: ***This paper addresses Security Information and Event Management in terms of modern-day scenario and how it has come about to be an evolved and better technology than earlier. Merging the basics of two different technologies, namely Security Information Managgement and Security Event Management, SIEM has been successful in not only identifying the potential and actual threat but also extends to manage and present remedial solutions. In the wake of advanced security invasions, it has replaced Intrusion Detection and Prevention System with remarkable efficiency. The working of SIEM, how it is related to the log management and what are the implications of deploying it in a modern enterprise is presented. Finally, what all criterias matter while selecting a suitable SIEM has been discussed in the paper.***

Index Terms— SIEM, SIM, SEM, log management

I. INTRODUCTION

SIEM, Security Information and Event Management, was introduced in early 21st century to assist organisations detect probable data breach or cyber attack as early as possible. However, the technology apparently became ineffectual in matching up to the changing security requirements of the modern business which deals with huge volumes of assorted data having high velocity. Moreover, the advanced security threats and malwares have also proved a challenge. Threats encountered in last decade were relatively predictable, unlike modern ones which are polymorphic and covert. Also, as SIEM is a costly affair, not many enterprises are equipped with resources required for dedicated maintenance of the infrastructure. In addition to that, implementation of SIEMs turns out to be difficult due to unsuccessful and stalled deployment. So just when it seemed that SIEM is a dead technology, it came back with much stronger presence than before [1]. Much like the Greek mythological bird Phoenix that regenerates from the ashes of its predecessor, Security Information and Event Management has become the emerging technology for detecting and responding to any threat. One may observe that it has effectively evolved and very much functional as a state-of-the-art practice in handling heterogeneous data in complex situations .

Moreover, it has been cast as the primary system for modern organisations who want to focus on their business affairs without looking over the shoulder for stealthy security breach [2].

Depending on the in-built organisational rules, SIEM not only detects an incident but resolves it for better compliance. The process becomes automatic creating alerts for potential intrusions.

Every organisation these days is working under certain regulatory requirements that govern its functioning on daily basis. Standard procedures like IT audits and other regulatory inspections have put a burden on the organisations to devote a major portion of their resources in assessing their defensive system, in regards to which system was accessed - when, how and by whom. Further, it needs to be definite whether the access was appropriate or not thereby identifying potential intrusive attempts. SIEM, thus, has a designated task with specific solutions to organisational problems. The market for security information and event management is governed by increasing demand from clients to fulfil not only compliance requirements but also the need to have a real-time alert in case of any threat, whether internal or external. The reason for SIEM popularity is that it empowers clients to analyse any security event in real-time for immediate threat management besides reporting on log data as well [3].

The present paper studies the solutions offered by SIEM and whether they are as effective as being theoretically considered. The upcoming sections, following this introduction will involve in-depth analysis of the evolution of SIEM, its working module, relation with log management and its utility. The analysis is in regards to SIEM functions in actual world. The conclusion will summarise the information imparted in this paper.

II. SECURITY INFORMATION AND EVENT MANAGEMENT

Merging of two domains

There are two separate areas that collaborate to make up SIEM, namely SIM (Security Information Management) and SEM (Security Event Management). SIM is concerned with accumulating, analysing and then reporting the recorded data. The data is aggregate information from host system, various applications, and all network and security devices (firewalls and antivirus).

Conversely, SEM is related to real time processing of information

Revised Manuscript Received on May 28, 2019.

Meenu Chopra,Vivekananda Institute of Professional Studies, GGSIPU, New Delhi, India.
Cosmena Mahapatra, Vivekananda Institute of Professional Studies, GGSIPU, New Delhi

from applications, host system, and all network and security devices. Every security event that gets generated across the entire infrastructure is scrutinized, compared and notified immediately. The two terms are not used separately anymore and only SIEM is used to describe the fusion of their functions. Thus, in a nutshell, SIEM collects and combines an organisation's log data that was generated across its entire infrastructure to identify, classify and examine the security threats, if any [3].

Current stance

SIEM is considered as a useful tool by security researchers for threat management of a company. However, certain gaps in research can be observed when it comes to successful configuration. While analysing the notable security breaches of the 21st century, the important question that comes up is whether enough considerations were taken to ensure correct deployment of SIEM. A lot of open source platforms are present that enlist how to implement the system but information pertaining to basics of configuration like time zone adjustment is lacking. A minor mistake in configuration can result in major disability to identify security threat on time. Though literature supports the effectiveness of SIEM for organisations, there is notable scarceness of data for organisations that have not employed SIEM for security.

Generally speaking, SIEM is mostly favoured by public companies and large organisations that place a huge importance on the compliance and regulations governing the use of SIEM. The software is preferably run "on premises" due to sensitivity of the data that goes through it. Mid size and few small companies have also reported using SIEM but as software-as-a-service (SaaS) platform due to monetary considerations and further lack of resources to maintain SIEM on a continuous basis.

As discussed earlier SIEM has a huge market share and its demand is high because it delivers on two major objectives. First, it regularly generates reports of failed logins, malware activities and suspicious attempts. Second, it sends out alerts for any activity that is in aberration to the predetermined set of rules, and thus highlights potential security breaches.

Technology firm Gartner [4] has reported that the current security market is huge with SIEM alone standing at $1.6 Billion. It is the demand created by various enterprises that has driven the SIEM products which have undergone innovations to lend newer capabilities to customers. For instance, new security potential that observes both network and user behaviour will be more intelligent to identify probable threat. Similarly, innovation like creation of threat intelligence feeds besides the customary log data, and introduction of technologies like Machine Learning, Artificial Intelligence, and using advanced statistical analysis makes SIEM, as Gartner puts it, "better threat detection tool" [4]. Deep learning capability in SIEM tools render better inference capacity due to "pattern-based monitoring and alerting" [5] along with threat management. Thus from simple monitoring, the technology has transformed into remedial-suggestive tool. With such newer potential, vendors have marketed the SIEM products as a detection tool that promises accurate results within a small time frame. Nevertheless, it is yet to be quantified how much enterprises have actually benefited from the innovations employed in SIEM software and whether there are any tangible advantages to them.

III. HOW SIEM EVOLVED

Initially companies invested a major chunk of their resources on intrusion detection and prevention system that were useful in identifying external security threats. However, as these systems relied on engines that are signature-based, there were high chances of false-positives. This gave rise to first generation SIEM that aimed at reducing signal-to-noise ratio, thus helped in capturing the most significant security threat. Any event that was in violation of security policy was detected using rule-based correlation method. By tradition, SIEM has exacted quite a lot of monetary and time investment but it has also done away with the issue of false alerts thereby efficiently carrying out the security task. The system was running all well till new and complex threats emerged. Keeping them in view, newer regulations like "Sarbanes-Oxley Act" and "Payment Card Industry Data Security Standard" were rolled out that imposed much stringent IT controls and data security norms [6]. To comply with these norms, organisations were required to go deep with their log events. The data needed to be collected, analysed, reported and archived for thorough monitoring of activities occurring in the entire IT infrastructure. This was directed at not only external protection but to generate regular reports about user activity and create forensic reports for any particular incident. Although collection of log events is an integral part of SIEM, they process only a small set of data that is related to security breach. The large amount of data generated throughout the IT thread, like various applications, routers, switches, OS, firewalls, IDS or IPS is a little too much for SIEM to handle. Hence, with the objective of monitoring the activities of user instead of managing external threat, a separate log management system came about. The log management architecture helped handle excessive volumes of data that flowed through large enterprises. SIEM and log management complement each other to gain the common objective of achieving organisational requirements. While log management have tools that can gather a large set of data to report and archive, SIEM tools run correlation on a sub-set of data to identify the most significant security incident. An organisation's effective IT weaponry includes both log management and SIEM solution. SIEM run correlation on log data that has been sorted and then forwarded by the log management tools that take on the part of a large data warehouse. Thus business enterprises get a good return on their investment through an effectual and efficient security management [7].

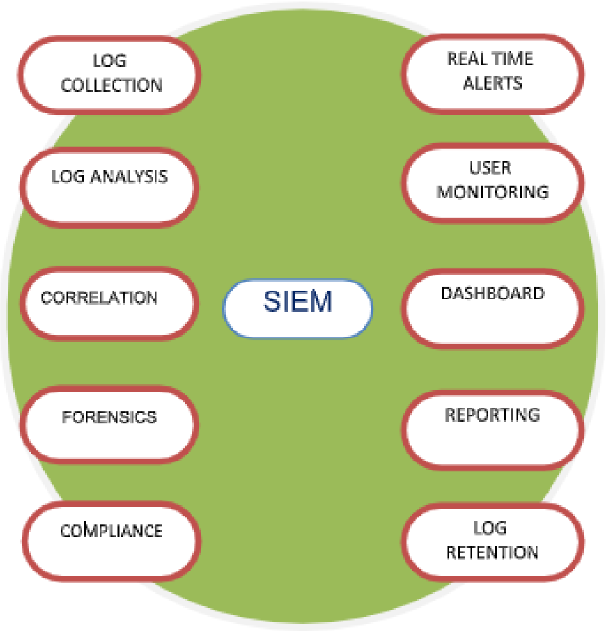

Fig. 1 Security information and event management

IV. HOW SIEM WORKS

Though there are specific differences in different SIEMs provided by vendors, the general framework is same. The basic functions of SIEM are collection followed by analysis, often called aggregation, and then retention. It is abbreviated as CAR. As SIEM gather log data from multiple devices, the transportation from source to destination needs to be secure and reliable to decrease chances of any false logs. There are many standard protocols for data collection viz. "Syslog, SNMP, SFTP, IDXP and OPEC". In case of absence of these protocols, software (known as agent) is installed that normalise the collected data into a format that is understandable to SIEM. In other words, log data, of varying format, is accumulated from multiple sources that further undergo normalisation to get converted into a "proprietary format". The process is called as consolidation. The consolidated data from all devices is correlated, thus bringing individual parts of the threat together to generate a complete picture. This stage demands contextual knowledge regarding the network environment and general kind of attacks. The results of analysis are generated through alerts and reports. For few hours, the log data is stored online on the SIEM before being moved on to an archive. The archived data is useful in case of forensics, and may be otherwise required too as per the regulations. There are two methods of data collection. In first scenario, called as Pull, SIEM makes an effort to retrieve data from the source device or agent. The second instance is called Push where the source device or agent will transfer the log from time to time [8]. Pull approach gives control to SIEM to gain access to each device and hence more significant. As high processing power is needed, if real-time data is not a priority, data can be transferred whenever there is less network traffic.

The correlation process involves putting together varying log events to create a picture of an attack or security incident. This is quite complex and intensive process as careful identification of threat is needed. The knowledge can be gained through information available from online databases and implementing contextual data to better grasp the network environment. This data is concerned with directories, physical location and device information etc. Additionally, information can be gathered from security events to update contextual information, although this may mean extra computational cost. So, in ideal conditions contextual information should be incorporated in the SIEM, to be updated on regular basis [9].

Detection of an attack can be done through two approaches, commonly employed in Intrusion Detection System, namely, anomaly based and misuse based. In anomaly based approach, anything that has not been specified as "good" will be considered as an attack; while in misuse based approach, all that has been categorised as "bad" will be reacted upon. In former approach, there is a need to write a lot, mentioning all the "good" behaviour. Still, there remains a high probability of acting on safe activities that were missed in policy. Nevertheless, anomaly approach has been quite effective in identifying abuse of license, internal attacks and uncharacteristic user activities. As soon as detection is done, information is communicated to administrator in one of the three ways. Either the threat is intimated as soon as it happens or it can be conveyed in its periodic reports. In the third option administrator actively scrutinizes SIEM in real time to be informed about any threat immediately. Reporting can be done in pre determined templates to generate quick reports which usually contain login activity of a definite time period. Real time monitoring usually entails a lot of investment on resources required for it and thus does not find much support in literature. During analysis, the data is stored online and later archived if not needed at the moment. For legal purposes, data in its raw or original form is needed while at other times, normalised and aggregated data can be retrieved to make things quick. SIEM devices have huge storage capacity extending in Terabytes and thus are able to store millions of events. Data can be compressed or encrypted for more safeguarding [10].

V. UTILITY OF SIEM

The very obvious reason of employing SIEM from operational vantage point is to lessen the number as well as impact of security threats by automatic analysis of potential events, and reducing them to a controllable list. Multiple devices like Firewall, VPN, user activities etc can generate thousands of events on daily basis. Many small-medium enterprises have reported more than one hundred-thousand events per day. With comprehensive monitoring and correlation by SIEM among devices, there will be an alert from the attacked device raising alarm and calling for additional defences to be put up. The detection rate of SIEM is over 99.9% as it automates the process of going through individual event log for any intrusion. It has basically replaced the traditional human intervention that involved multiple skilled security engineers going through each event to detect abnormal activity [11].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

VI. SIEM Selection Criteria

While selecting an SIEM, the point of consideration is what is being expected from the SIEM. If the requirement is only limited to log management, vendor can import data from each of the log sources. It is significant to determine the purpose for using logs, whether it is for identifying threats, reporting compliance or investigative reasons [12]. Also, it is important to determine if data will be recorded in real time or not. In case of threat identification, more than 99% correlation or consolidation or aggregation can be attained. When appropriately tuned, even 99.99% efficiency has been reported. Generally, an organization is regulated under different compliance requirements in accordance to type of sector they are catering to [13]. For instance, General Electrics, a Fortune 500 company, is subjected to not only SOX but HIPPA, FISMA and more. Each of its corporate division is under obligation to produce compliance reports for every regulation.

VII. CONCLUSION

Integrating two different technologies, SIEM is a complex tool yet indispensable for any organization. Still, there is fluctuation in terms of market segment because it requires immense technical skills. Further, there is extensive training needs and certification vendors' part. When log-based activity data and correlation inspired from any security event is applied to different business issues, SIEM demonstrates quite productiveness. As a matter of fact, SIEM is much beyond the regulatory compliance, activity monitoring or business intelligence. Many informed customers are extending the utility of tools to security of Web 2.0 applications, mobile devices and cloud services. The point is establishing a centralized record of activity pertaining to user and the system. With open architecture, different business users can access the data for solving many of their organizational problems. Thus, SIEM can be an effective solution making the process of intrusion detection and response better.

REFERENCES

1. N. Zhang and H. Bao, "Research on Information Security in Modern Network," *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, Wuhan, Hubei, 2009, pp. 386-389.
2. A.Williams "Security Information and Event Management Technologies" Siliconindia Vol. 10 No. 1 2006 pp. 34-35.
3. D.F. Carr "Security Information and Event Management". Baseline No. 47 2005 pp. 60-83.
4. M. Nicolett K.M. Kavanagh "Magic Quadrant for Security Information and Event Management" Gartner RAS Core Research Note G00212454 12 May 2011.
5. "What is SIEM Software? How it works and how to choose the right tool," *csoonline.com,* 28-Nov-2017 [Online] Available: https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html. [Accessed: 19-Feb-2019]
6. S. Bhatt P. K. Manadhata L. Zomlot "The operational role of security information and event management systems" IEEE Security Privacy vol. 12 no. 5 pp. 35-41 2014.
7. G. Shipley, "Are SIEM and log management the same thing?," *Network World*, 30-Jun-2008. [Online]. Available: http://www.networkworld.com/reviews/2008/063008-test-siem-log-integration.html. [Accessed: 20-Feb-2019].
8. Wang-Cheol Song, Lee-Hyun Baek and Chang-Eon Kang, "Design and implementation of a security management system," *Proceedings of IEEE Singapore International Conference on Networks and International Conference on Information Engineering '95*, Singapore, 1995, pp. 261-264.
9. R. Gabriel, T. Hoppe, A. Pastwa and S. Sowa, "Analyzing Malware Log Data to Support Security Information and Event Management: Some Research Results," *2009 First International Confernce on Advances in Databases, Knowledge, and Data Applications*, Gosier, 2009, pp. 108-113.
10. Aguirre and S. Alonso, "Improving the Automation of Security Information Management: A Collaborative Approach," in *IEEE Security & Privacy*, vol. 10, no. 1, pp. 55-59, Jan.-Feb. 2012.
11. M. Cinque, D. Cotroneo and A. Pecchia, "Challenges and Directions in Security Information and Event Management (SIEM)," *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Memphis, TN, 2018, pp. 95-99.
12. "6 point SIEM solution evaluation checklist," *ComputerWeekly.com.* [Online]. Available: https://www.computerweekly.com/tip/6-point-SIEM-solution-evaluation-checklist. [Accessed: 19-Feb-2019].
13. "SIEM Product Selection Criteria in 2018," *Huntsman*, 28-Nov-2018. [Online]. Available: https://www.huntsmansecurity.com/blog/siem-product-selection-criteria-2018/. [Accessed: 19-Feb-2019].