INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 07 ISSUE: 03 | MARCH - 2023 IMPACT FACTOR: 7.185 ISSN: 2582-3930

Importance of SIEM in Organization

Amol Bhalerao
Keraleeya Samajam (Regd.) Dombivli's Model College, Thakurli (East), Maharashtra, India

Abstract*—In this paper we explore the modern-day scenario of Security Information and Event Management (SIEM) and how it has evolved into a more sophisticated technology. SIEM is a combination of two different technologies, Security Information Management and Security Event Management, that not only identifies potential and actual threats but also manages and presents remedial solutions. Due to its remarkable efficiency, SIEM has replaced the Intrusion Detection and Prevention System in the wake of advanced security invasions. The paper presents the workings of SIEM, its relation to log management, and the implications of deploying it in a modern enterprise. Lastly, the paper discusses the essential criteria that should be considered when selecting a suitable SIEM.

Keywords— Log Management, Security Information, Event Management.

I. INTRODUCTION

SIEM (Security Information and Event Management) was introduced in the early 2000s with the aim of helping organizations detect potential data breaches or cyberattacks as early as possible. However, as security threats continue to evolve, SIEM has struggled to keep pace with the changing security needs of modern companies that deal with massive amounts of high-speed data. Additionally, the increased prevalence of security threats and malware has made the task even more difficult. Modern-day threats are polymorphic and elusive, making them difficult to predict. Moreover, due to the high implementation cost, few companies have the necessary resources for dedicated maintenance infrastructure, and implementing SIEM has proven to be a challenge due to failed and stalled implementation. Despite these difficulties, SIEM is making a comeback with renewed vigor [6]. SIEM, like the mythical Phoenix bird, has emerged as a state-of-the-art technology for detecting and responding to threats. It has evolved significantly and is highly effective in handling diverse data in complex scenarios. Additionally, it has become the primary system for modern organizations that wish to concentrate on their business without worrying about concealed security breaches [7]. The purpose of this paper is to examine the effectiveness of SIEM solutions in practical applications, compared to theoretical considerations. In the following sections, we will provide a detailed analysis, including the evolution of SIEM, its operational mechanism, its correlation with log management, and its practical utility. The analysis will primarily focus on the real-world functionality of SIEM. Finally, we will summarize the information presented in this paper.

II. SECURITY INFORMATION AND EVENT MANAGEMENT

The merging of the two domains: -

SIEM is composed of two distinct components - SIM (Security Information Management) and SEM (Security Event Management) - that work in tandem. SIM's primary function is to collect, analyze, and report on recorded data from various sources, including host systems, applications, and network and security devices such as firewalls and antivirus software. In contrast, SEM is responsible for real-time processing of data from applications, host systems, and network and security devices. All security events generated throughout the infrastructure are immediately scrutinized, compared, and alerted on. The two terms SIM and SEM are no longer used separately, and only SIEM is used to describe the combined function. In essence, SIEM gathers and correlates an organization's log data generated throughout its entire infrastructure to identify, classify, and investigate potential security threats [1].

Current State of the SIEM

SIEM is widely used by security researchers as a tool for threat management in companies. However, there are some gaps in research regarding successful configuration. When analyzing significant security breaches of the 21st century, it is crucial to question whether sufficient considerations were taken to ensure correct deployment of SIEM. Although numerous open source platforms exist that detail how to implement the system, information regarding basic configuration, such as time zone adjustment, is lacking. Even minor mistakes in configuration can result in an inability to identify security threats in a timely manner. While there is significant literature supporting the effectiveness of SIEM for organizations, there is a noticeable lack of data for those organizations that have not employed SIEM for security. Generally speaking, SIEM is mostly used by public companies and large organizations that place a significant emphasis on compliance and regulations governing its use. The software is preferably run "on premises" due to the sensitivity of the data that goes through it. Some mid-size and small companies have also reported using SIEM, but as a software-as-a-service (SaaS) platform due to financial considerations and a lack of resources to maintain SIEM continuously. As discussed earlier, SIEM has a significant market share, and its demand is high because it delivers on two major objectives. First, it generates regular reports of failed logins, malware activities, and suspicious attempts. Second, it sends out alerts for any activity that deviates from the predetermined set of rules, highlighting potential security breaches.

III. HOW THE SIEM HAS EVOLVED

Initially, organizations invested a significant portion of their resources in detecting and preventing intruders was helpful in identifying external security threats. However, because these systems relied on signature-based engines, there was a high probability of false positives. he gavebecame the first-generation SIEM, which aimed to reduce the signal-to-noise ratio, making it possible to capture what matters most security risk. Any event that represents a security breach rules were discovered using the rule-based correlation method. Out of cost SIEM a lot of time and money investment, but also eliminated the problem of lying alerts that effectively accomplish the security task. Although collecting log events are an integral part of the SIEM and only handle a small number data related to a security breach. A large number of data generated throughout the computer cable, such as are various applications, routers, switches, operating system, firewall, IDS or IPS is a bit much for a SIEM. Therefore, to monitor user activity rather than manage it external threat appeared a separate log management systemo Log management architecture has helped manage the excessive amount of data flowing through large organizations. SIEM and log management

complement each other for achieving the common goal of meeting organizational needs. Although log management has tools that can collect large amounts of data for reporting and archiving, SIEM tools correlates with a subset of the data to identify the most significant security incident. Efficient organizational computing Armamentincludes both log management and SIEM solution. SIEM correlates with sorted log data and then examined the log management tools they were using from a large data warehouse. In this way, trading companies receive a good return on investment through effective and efficient security management.

IV. HOW DOES THE SIEM WORKS

Although there are specific differences in different SIEMs provided by vendors, the overall picture is the same. THESIEM core functions are collected and then analyzed.is often referred to as aggregation followed by retention. It will be shortenedas a car. Because SIEM collects log data from multiple devices, Transportation from source to destination must be safe and reliable to reduce the risk of false logs. There are many standard data collection protocols, viz."system logs, SNMP, SFTP, IDXP and OPEC". If not present Software (called an agent) is installed for these protocols, standardizes the collected data in a format SIEM understands. In other words, log data are of different formats collected from several crossing sources normalization to convert to a "proprietary format". This process is called as consolidation. Consolidated Data of all devices are related to each other and thus bring the individual pieces together threats together to create a complete picture. The Step requires context knowledge of the network The environment and the general nature of attacks. Results analyzes are generated via alerts and reports. For few hours of log data is stored online in SIEM before being archived. Archived data is useful, e.g. forensic case and can also be otherwise accof the regulation. There are two methods of the data collection. In the first scenario called Pull, SIEM retrieves data from a source or agent. The instance is called a push, with the source device or agent being sufficient sends a log from time to time [3].

The correlation process involves merging various log events to create a picture of a security incident or attack. This is quite a complex and intensive process as it requires careful identification of the threat. Knowledge can be gained through the information available in online databases and the implementation of contextual data to better understand the network environment. This data relates to directories, physical location and device information, etc. Information from security events can also be collectedto update contextual information, although this may incur additional computational costs.Therefore, ideally, contextual information should flow into the SIEM so that it is regularly updated [4].

Detection of an attack can be done through two approaches commonly used in intrusion detection systems,, namely anomaly-based and abuse-based. Based on anomalies Focus , everything that is not called "good".counts as an attack; whereas the abuse-based approach responds to anything deemed "bad".approximately. The above approach requires you to write a lot and mention all the "good" behavior. Despite this, there is still a highProbability of trading in safe activities strayed into Policy. However, the anomaly approach was very effective in identifying license abuse, insider attacks, anduncharacteristic user activities.Once the detection is complete, Theinformation is communicated to the administrator in one of thein three ways. Either the threat will be notified as soon as it occurs or it can be shared in your periodic reports. In the thirdOption Manager actively examines SIEM in real timeto be immediately informed of any threat. reporting cancan be run on standard templates to create quick reports, typically containing login activity from a defined point in time Period. Real-time monitoring generally implies a large investment in the resources required for it and therefore does not take placemuch support in the literature.During analysis, the datastored online and then archived when not needed.For legal purposes, data is required in its original or raw form, while at other times the data may be normalized and aggregatedrecovered to get things done quickly. SIEM devices have enormousstorage capacity that ranges in terabytes and are therefore ablestores millions of events. Data can be compressed or encrypted for additional protection [5].

V. WHAT THE CRITERIA FOR THE SELECTION OF SIEM

While opting an SIEM, the point of consideration is what's being anticipated from theSIEM.However, seller can import data from each of the log sources, If the demand is only limited to log operation. It's significant to determine the purpose for using logs, whether it's for relating pitfalls, reporting compliance or investigative reasons [8]. Also, it's important to determine if data will be recorded in real time or not. In case of trouble identification, further than 99 correlation or connection or aggregation can be attained. When meetly tuned, indeed99.99 effectiveness has been reported. Generally, an association is regulated under different compliance conditions in agreement to type of sector they're feeding to [9]. For case, General Electrics, a Fortune 500 company, is subordinated to not only SOX but HIPPA, FISMA and further. Each of its commercial division is under obligation to produce compliance reports for every regulation.

VI. CONCLUSION

Integrating two different technologies, SIEM is a complex tool yet necessary for any association. Still, there is change in terms of request member because it requires immense specialized chops. Further, there's expansive training requirements and instrument merchandisers ' part. When log- grounded exertion data and correlation inspired from any security event is applied to different business issues, SIEM demonstrates relatively effectiveness. As a matter of fact, SIEM is important beyond the nonsupervisory compliance, exertion monitoring or business intelligence. numerous informed guests are extending the mileage of tools to security of Web2.0 operations, mobile bias and pall services. The point is establishing a centralized record of exertion pertaining to stoner and the system. With open armature, different business druggies can access the data for working numerous of their organizational problems. therefore, SIEM can be an effective result making the process of intrusion discovery and response better.

VII. REFERENCES

[1] D.F. Carr "Security Information and Event Management". Baseline No. 47 2005 pp. 60-83

[2] 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-logintegration.html. [Accessed: 20-Feb-2019

[3] 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

[4] 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

[5] 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

[6] 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

[7] A.Williams "Security Information and Event Management Technologies" Siliconindia Vol. 10 No. 1 2006 pp. 34-35

[8] "6 point SIEM solution evaluation checklist," ComputerWeekly.com. [Online]. Available: https://www.computerweekly.com/tip/6-pointSIEM-solution-evaluation-checklist. [Accessed: 19-Feb-2019].

[9] "SIEM Product Selection Criteria in 2018," Huntsman, 28-Nov-2018. [Online]. Available: https://www.huntsmansecurity.com/blog/siemproduct-selection-criteria-2018/. [Accessed: 19-Feb-2019].