WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Importance of SIEM in Organization

Ajay Radhakrishnan Nair

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

ABSTRACT—

This paper delves into the contemporary landscape of Security Information and Event Management (SIEM), highlighting its evolution into a more sophisticated technology. SIEM integrates two distinct technologies, Security Information Management and Security Event Management, to not only detect potential and actual threats but also to manage and propose solutions for them. Its exceptional efficiency has led to the replacement of traditional Intrusion Detection and Prevention Systems, especially in response to advanced security breaches. The paper explores the mechanics of SIEM, its relationship with log management, and the implications of its implementation within modern enterprises. Lastly, it discusses the crucial criteria to consider when selecting an appropriate SIEM solution.

Keywords— Log Management, Security Information, Event Management

1. 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.

2. SECURITY INFORMATION AND EVENT MANAGEMENT

The merging of the two domains: SIEM or Security Information and Event Management, is a comprehensive system made up of two key components: SIM (Security Information Management) and SEM (Security Event Management). SIM focuses on gathering, analyzing, and presenting data from various sources such as host systems, applications, and security devices like firewalls and antivirus software. SEM, on the other hand, deals with the real-time processing of data from these sources, immediately scrutinizing and alerting on any security events detected.

The terms SIM and SEM have become intertwined under the overarching term SIEM, which describes the combined function of both components. Essentially, SIEM works by collecting and correlating log data from across an organization's infrastructure to identify, categorize, and investigate potential security threats. It serves as a vital tool for monitoring and managing security in modern enterprises.

Current State of the SIEM

SIEM, a crucial tool for security researchers, plays a vital role in managing threats within companies. However there are gaps in research, particularly regarding its successful configuration. When examining major security breaches of the 21st century, it's essential to question whether SIEM was deployed correctly. Despite various open-source platforms offering implementation guidance, basic configuration details like time zone adjustments are often overlooked potentially leading to delayed threat identification.

While SIEM is widely endorsed for its effectiveness in organizations, there's a lack of data on those not using it for security. Typically, SIEM is favoured by public companies and large organizations emphasizing compliance and regulations. Due to data sensitivity, on-premises deployment is preferred, although mid-size and small companies may opt for SIEM as a software-as-a-service (SaaS) platform due to financial and resource constraints.

As discussed, SIEM remains in high demand due to its ability to generate reports on failed logins, malware activities, and suspicious attempts. It also issues alerts for any deviations from established rules, highlighting potential security breaches.

3. HOW THE SIEM HAS EVOLVED

Initially, organizations heavily invested resources into detecting and preventing intrusions to identify external security threats. However, relying on signature-based engines in these systems often led to a high rate of false positives. This prompted the development of the first-generation SIEM, aimed at reducing noise and focusing on critical security risks. Through rule-based correlation methods, security breaches were identified more accurately, addressing both the financial and operational costs associated with SIEM implementation while mitigating false alerts.

While log event collection remains vital to SIEM, handling the vast data generated by diverse sources such as applications, routers, switches, and operating systems proved challenging. As a result, a separate log management system emerged to manage this data overload within large organizations. Log management architecture became crucial in efficiently handling large data volumes, complementing SIEM systems to meet organizational security requirements.

While log management tools excel in collecting and archiving data, SIEM tools focus on correlating a subset of this data to identify significant security incidents. The synergy between log management and SIEM solutions forms an efficient organizational computing strategy. SIEM correlates sorted log data and analyzes it through log management tools, leveraging extensive data repositories. This integrated approach ensures companies achieve a favourable return on investment by enhancing security management effectiveness and efficiency.

4. HOW DOES THE SIEM WORKS

Although SIEM solutions offered by different vendors may vary in specifics, they share common core functions. The primary process involves collecting and analyzing data, often referred to as aggregation and retention, abbreviated as "CAR." For SIEM to work effectively, it must securely transport log data from various sources to its destination to minimize the risk of false logs. Various standard data collection protocols like system logs, SNMP, SFTP, IDXP, and OPEC are used. If these protocols are absent, software agents are installed to standardize collected data into a format that SIEM understands, a process known as normalization or consolidation. Normalization is critical because log data come in different formats from different sources. This consolidation allows SIEM to correlate data from all devices, offering a comprehensive view of potential threats. Successful correlation relies on understanding the network environment and common attack patterns. Analysis results are typically generated through alerts and reports, with log data stored online in SIEM for a brief period before archiving. Archived data serves various purposes, including forensic investigations and compliance with regulations. SIEM employs two main data collection methods: "pull" and "push." In the pull method, SIEM retrieves data from a source or agent, while in the push method, the source device or agent sends logs periodically without SIEM intervention.

The correlation process within SIEM involves combining various log events to understand and visualize security incidents or attacks. It's a complex task that demands careful identification of threats. Contextual data, including directory structures, physical locations, and device details, helps enrich the understanding of the network environment. This data can be sourced from online databases and updated with information from security events, although this may increase computational demands. Ideally, contextual information should be integrated into SIEM systems to ensure regular updates without causing disruptions.

Detection of attacks can be accomplished through two commonly used approaches in intrusion detection systems: anomaly-based and abuse-based. In the anomaly-based approach, anything that deviates from the norm is considered an attack, while the abuse-based approach reacts to anything identified as "bad" behaviour. Despite the thoroughness of the anomaly approach, there remains a risk of categorizing legitimate activities as threats. However, the anomaly approach has proven effective in identifying license abuse, insider attacks, and unusual user activities. Once detection is complete, the information is communicated to the administrator through one of three methods: immediate notification upon threat detection, inclusion in periodic reports, or real-time monitoring by the manager to stay informed of threats as they arise. Reporting can be done using standard templates to generate quick reports, typically detailing login activity over a defined period. Real-time monitoring, while effective, often requires significant resource investment and is not extensively supported in the literature. During analysis, data is stored online and archived when no longer needed. For legal purposes, data may be required in its original raw form, while at other times, normalization and aggregation may be applied for quicker processing. SIEM devices boast extensive storage capacities, ranging in terabytes, allowing them to store millions of events. Additionally, data can be compressed or encrypted for added protection.

5. WHAT THE CRITERIA FOR THE SELECTION OF SIEM

When choosing an SIEM solution, it's crucial to define the intended purpose clearly. If log operations are the primary concern, the ability to import data from all relevant sources effectively becomes pivotal. Understanding the purpose behind log usage, whether for vulnerability identification, compliance reporting, or investigative purposes, is essential. Additionally, determining whether data will be recorded in real-time is important. Achieving effective trouble identification often requires correlation, connection, or aggregation capabilities beyond 99%, which can be attained with proper tuning. Organizations, especially those like General Electric, a Fortune 500 company, are subject to various compliance regulations such as SOX, HIPPA, and

FISMA. Each commercial division within such organizations must produce compliance reports for the applicable regulations, emphasizing the need for an SIEM solution that can meet diverse compliance needs effective.

6. CONCLUSION

Integrating two distinct technologies, SIEM serves as a complex yet indispensable tool for any organization. However, its implementation requires substantial technical expertise and significant investment, including extensive training and support from vendors. SIEM proves highly effective when log-based data and correlation derived from security events are applied to various business challenges. Beyond mere regulatory compliance, operational monitoring, or business intelligence, SIEM plays a pivotal role in addressing emerging security concerns such as those related to Web2.0 operations, mobile devices, and cloud services. The centralization of operational data allows different stakeholders within the organization to access and leverage it for addressing various organizational issues. In this regard, SIEM enhances the process of intrusion detection and response, making it more efficient and effective.

7. 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-siemlogintegration.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] 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 Conference 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" Silicon India 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-pointSIEMsolution-evaluation-checklist. [Accessed: 19-Feb-2019}.

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