International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-5, Issue-4, August 2016

Enhancing Security Information and Event Management to Develop Future-Ready Security Operations Center

Steffi Raju

***Abstract*— The threats to the security of networking systems are on the rise. This had led to a continued need to implement effective monitoring of the events and the activities over the information network infrastructure via the Security Operations Center (SOC). It is in this context that Security Information and Event Management (SIEM) gains prominence. SIEM is a network monitoring technology for facilitating real time network monitoring for the Insider threats within a given organization's SOC. It analyses not just the current security events but also evaluates these incidents with historically archived security log data to identify patterns in security threats and to help security architects make the underlying architecture more robust. The aim of this study is to enhance the existing SOC setup by incorporating new enhanced architecture and working procedures. It also aims to automate the testing and analysis of standard security controls using SIEM. All the above developments would help create a future-ready SOC which would greatly strengthen the overall IT security landscape of an organization.**

***Index Terms*— ISO 27001 Security Controls, Security Operations Center, Security automation, SIEM.**

I. INTRODUCTION

Information security is a buzzword in the global IT landscape and is one of the most critical component in an organization. Nowadays, hackers are very advanced in their approach to break organizational information security and sophisticated mechanisms are being utilized to compromise the security over the network in the IT systems. These mechanisms are being launched either from within the network (internal threats) or from outside the network [1]. Previously organizations were passive responders to the threat and used to only react as an when a security breach occurred. However the deep financial, reputational and operational impact of cyber-attacks have prompted organizations to Computer Security Incident Response Teams (CSIRT) teams working as part of Security Operations Center (SOC). These centers proactively monitor security incidents in real time and take requisite action as and when vulnerability is identified by them. Security Information and Event management (SIEM) technology has been extensively deployed as part of SOCs to assist in the whole data collection and analysis process.

SOC has its role to implement the application of the SIEM technology so as handle the enterprise level security. SIEM performs the correlation on the log information and the network's events in order to manage the risks over the network attacks. It helps in tracking the possible threats in the network; and it usually does so during the real time events. The effectiveness of the application of the SIEM technology in the monitoring of the networks threats depends on the ability detect the origin of the attacks or threats. Thus the Insider threats are usually in the network pool, where the organization's network users- managers, workers or the supervisors access sensitive information over the network.

It helps to consolidate and thereby evaluate messages and alerts originating from different IT systems in a centralized platform[2]. The SIEM systems are effective as they can comprehend large amounts of the security data and provide the raw data in a visual form which is comprehensible to the end-user [3]. Visualization is thus an essential part of the SIEM systems. Overall, SIEM help in evaluating the security of computer networks in a real-time or near real-time basis by monitoring security incidents thereby mitigating risk of information leakage due to the security gap [4].

Security logging is an old concept and has been implemented in organizations for quite some time now. However, in a multi-system enterprise environment a security logging mechanism would not be effective if the data produced time consuming to go through and complex to interpret. It is in this context that the quality data is important than the quantity of data produced[5]. SIEM enables to collect, store, find correlation, analyze the complete logs and present it to in a meaningful manner to the end-user.

The current setup of SIEM requires considerable human effort in monitoring security incidents. This can become overwhelming for CSIRT team if the IT landscape is large and varied. Further the incident detection methods also rely upon singular metrics rather than a combination of multiple metrics. Furthermore, the standard security controls testing set in place via compliance standards like ISO 27001, etc. are also manual in nature. Considerable research has been done in each of the above areas. However, existing research has not integrated all the developments in a single platform. The aim of this study is to synthesize all the existing developments in the field of SIEM into an integrated framework which would help to develop a proactive and automated future-proof SOC system. The method of research is literature review based.

The study would singularly focus on the different cores of the SIEM concept and would help identify the enhancements in each domain. It would first look at the concept of SOC and SIEM and what is the need for such an application. It would then delve into the SIEM architecture and how it can be enhanced to make it more effective. Following this, it would focus on the inner working of SIEM in identifying security

Steffi Raju, Department of Information Technology, K J Somaiya College of Engineering, Mumbai University.

incidents and would propose improvements to the detection process. Once these two parts are done, it would suggest ways to automate standard security controls testing using SIEM. In the end, the study aims to provide a standard set of requirements for all SIEMs to have in order to develop a robust SOC.

II. THEORETICAL FOUNDATION

In order to understand the concept of SOC and SIEM, it is essential to understand the foundation behind it. This section aims to provide the brief overview of both concepts and what is the motivation behind implementing them in organizations. It also explains the architecture of SIEM and the background of how security evaluation of an attack is identified and evaluated in SIEM presently.

A. Security Operations Center (SOC)

A SOC is a centralized unit security monitoring unit in an organization which monitors security incidents on a real-time basis. It monitors the security events around the IT assets including network, firewalls, intrusion detection/prevention systems, application servers, database systems and lastly user accounts in an organization[6]. Each of the above assets are monitored constantly and SOC receives periodic logs which are then analyzed for any security incidents. It also proactively flags malicious events on a real-time basis which allows CSIRT teams to swiftly react and defend the infrastructure from attacks.

The effectiveness of SOC depends heavily on its analytical and forensic abilities and how quickly it can analyze the data and report events back to end-users [6]. This requires an in-depth understanding of the entire IT infrastructure in order to perform correlation analysis. SOC is able to perform all the logging and monitoring due to SIEM systems which are integral to it.

B. Security Incident and Event Management (SIEM)

As mentioned in previous section, SIEM forms the inner core of the SOC architecture. As the name suggests, SIEM is a combination of Security Information Management (SIM) and Security Event Management (SEM). SEM performs data aggregation of the security logs in management information. It then creates security incidents which are tackled by the CSIRT. While SEM focuses on data aggregation, SIM on the other hand focuses on analyzing historical data and performing trend analysis on them to identify trends. These trends would help SIEM to flag events even before their occurrence, thereby improving the long-term effectiveness of information security systems [5].

SIEM help to consolidate and evaluate messages and incidents from individual systems components in a timely manner. They collect logs from disparate sources and normalize them into common standard representation. They further store these event in their rule engine which then send alerts once a rule is activated[6]. These security alerts are not only specific to single applications but can perform correlation analysis which makes it integrated across the complete IT platform. However all the advance in SIEM has led to an exponential increase in the number of security incidents. This, as per past experience in multiple organizations have shown that SIEM systems are complex to operate and require high resource effort to analyze all events. Thus in long term, security analysts end up neglecting SIEM systems on an operational level [2].

C. SIEM Architecture & Working

A typical SIEM infrastructure has the below mentioned six core components as is described by [7]:

a. Source Device: The source systems are the data sources that provide security runtime logs from the components within the entire enterprise infrastructure. It can be anything from application servers to firewalls, databases, IDS/IPS systems, etc. Since different systems have different syntax in data storage, the logs are made interoperable by SIEM.

b. Log Collection: The logs from the data sources are collected by SIEM by one of the two techniques of PUSH or PULL. Push technique involves logs being proactively pushed by data sources into SIEM on a real-time basis, whereas PULL technique involves SIEM pulling data from source device on a periodic basis. PULL technique is safer as SIEM then understands what kind of data is collected.

c. Normalization: The normalization engine is one of the most important component of SIEM. Different source devices lead to different syntax of log files for every source device. In order for these logs to be analyzed in correlation to each other, it is important for them to be normalized into a standard format. Normalization ensures that the original data from source devices are standardized to a common format.

d. Rule/Correlation Engine: It consists of the rule and correlation engines. The rule engine is a repository of all the rules that are required to evaluate specific security events. A rule engine evaluates logs in the 'what-if' format which usually returns a Boolean value. While rule engines are the repositories for storing rules, correlation engines are the analytical backbone of SIEM. Based on the defined rules, the correlation engine analyzes log data to identify patterns of security events. Most attack types are not simple in order to be flagged on basis of specific rules. Correlation engines analyze the logs in the context of the entire infrastructure and thereby correlate events to flag the correct security events. Correlation engines use Artificial intelligence to reduce the false-positives increasing the efficiency of the event detection [7].

e. Data Storage: Data storage involves storage of both security logs along with the storage of SIEM related data. This data is critical in order to perform historical trend analysis along with maintaining the audit logs for future security audits [7].

f. Monitoring: Monitoring allows the SIEM administrators to interact with the application in order to access the data and also to independently analyze the data. This is normally a visually front-end for visualizing data in a more compact and comprehensible manner.

D. SIEM Attack modeling security evaluation

In order to identify security incidents, SIEM solutions use multiple evaluation techniques to evaluate and identify incidents in a real-time and accurate manner. They help to find and correct gaps in the network configuration, reveal possible security attacks actions for different security vulnerabilities, determine the critical network resources thereby choosing an effective security policy and mechanisms appropriate to current threats [8]. There are many approaches and algorithms for identifying threats such as malefactor's behavior, generating a common attack graph,

calculating different security metrics and providing risk analysis procedure [8].

III. ENHANCEMENTS TO SIEM FOR A ROBUST SOC

Having explained all the concepts around SIEM, this section aims to propose the enhancements which would help to develop a robust future-proof SOC infrastructure. Raydel et al. mention the main challenges that IT security professionals face in the security setup of their organizations[9]. The critical technical challenges outlined by Raydel et al. are listed below [9]:

a. Variety of Source devices to secure: In a diverse IT landscape with multiple applications performing specialized tasks, it becomes challenging to ensure security of all applications. It is complicated to analyze basis the results in SIEM to ascertain the security changes required for different applications in a consistent and standard manner [9].

b. Quick Response to new threats: CSIRT members need to ensure that security vulnerabilities identified within SIEM are plugged quickly before they are exploited by hackers. This would mean a variety of security measures like installing system patches to big changes like re-configuring the security parameters of the application. These are time-consuming tasks and a quick response is not always possible.

c. Lack of interoperability and integration of security tools: There is no standard tool which addresses all the security requirements of an organization. Teams have to rely on multiple security tools, each with their own distinctive format and usage requirements to get all corners covered in the security infrastructure.

In view of the above challenges, it is essential to create a single standardized solution which eliminates the challenges and provides a robust solution to the security needs of any organization. This study proposes a three-staged approach in enhancing the SIEM solution. The three stages are mentioned below:

A. Implementation of Distributed SIEM architecture

Conventional SIEM architecture as described in above section is a centralized architecture with six components. This architecture becomes very difficult to management in a large organization. One of the main challenges in a centralized architecture is the problem of log maintenance. A large number of source devices can lead to large volume of logs generated from numerous sources which are inconsistent in content, format, timestamp, etc. [10]. SIEM greatly reduces the impact of the challenge by normalizing the data. However, the primary of large volume of logs still remains unsolved. In order to solve this problem, the SIEM architecture has to be decentralized and distributed as per the 'Hierarchical Managers Model' outlined by Anastasov et al. in [10]. The 'Hierarchical Managers Model' extends the traditional centralized SIEM architecture by creating a hierarchy of SIEM servers that are connected hierarchically to a central SIEM server. Thus, the central SIEM server acts as a parent node and communicates with the child SIEM servers named 'Child Managers' instead of directly communicating to the source devices for log data[8][10]. The entire process of collecting, normalizing, storing and monitoring of logs is done on the child level and only for data aggregation, correlation and reporting is normalized log data sent to the parent node. Fig. 1 illustrates the architecture of the "Hierarchy Managers Model as proposed by Anastasov et al [10]

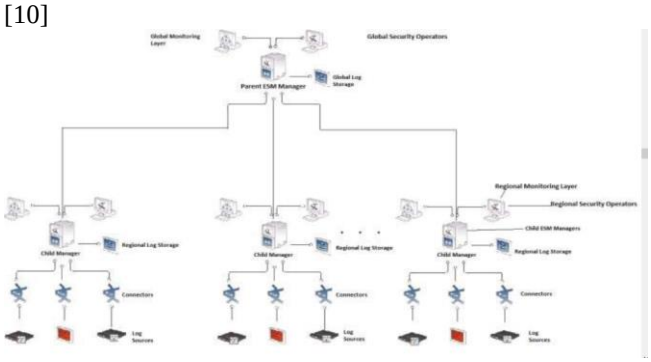

Fig. 1. Hierarchical Managers Architecture by [10]

The main advantage of this architecture is that it introduces the advantages of distributed computing to SIEM. The data management is done by distributing the load across multiple correlation/rule engines thereby reducing the effort at the central node. Only the data for aggregation and correlation which is a subset of the data at the child manager level would be sent to the parent node for analysis thereby reducing load on the central node and thereby increasing the efficiency of their throughput leading to quicker computation times. Along with the SIEMs, the SOCs too needs to be distributed at regional level and only data required for correlation analysis needs to be sent to parent SOC[10]. This also leads to ease of installation and deployment of SIEM systems.

B. Common Framework for Attack Modeling and Security Evaluation in SIEM

One of the challenges outlined by Raydel et al. in [9] is the quicker and accurate response to new threats. The key to a quicker response to new security threats is to accurately pinpoint the threat in the fastest manner. It is in this context that the work of Kotenko et al. finds significance [8]. Conventional security evaluation algorithms rely on one technique for identifying security threats. Kotenko et al. proposed the Attack Modeling and Security Evaluation Component (AMSEC) architecture which uses multiple algorithms in a parallel manner to achieve near to real-time accurate identification of security threats [11]. The techniques proposed by Kotenko et al. as part of the AMSEC architecture for achieving this are mentioned below[8]:

d. Usage of security repository and open security databases containing system and network vulnerabilities, attacks, configuration, weaknesses, countermeasures, etc.

e. Generation of attack trees considering service dependency graphs and zero-day vulnerabilities reports based on Topological Vulnerability Analysis (TVA). In TVA, the graph generator computes the attack scenarios possible due to the vulnerabilities identified in the system. It would be based on both forward and backward analysis in order to cover all combinations of attack sequences. This would help to model critical attack scenarios which when occurred in sequence should be flagged as a possible attack.

f. Application of anytime algorithms to provide near to real-time attack modeling. This would make the system effective to detect vulnerabilities at run-time.

g. Usage of the generated attack graphs to predict possible malefactor's actions: it does this by first creating the attack graphs for the profile of the malefactor selected by the user.

Following this, it would predict the future actions of the malefactor based on its actions.

h. Calculation of a multitude of security metrics, attack and response impacts: Based on the skill level of the malefactor, the system would calculate the various metrics for the impact of possible attack along with the impact of the possible counter-response. The level of counter-response depends on the skill level of the malefactor.

i. Interactive decision support to select the security solutions: In the final step, the AMSEC framework deploys a decision support center which incorporates data from all the above metrics and creates a decision support model which would assist users in taking the appropriate counter-measures based on the severity of the attack.

The AMSEC framework provides a complete rounded platform for computing security incidents. It creates attack graphs which helps to compute all the possible attack scenarios which help in predicting and taking necessary countermeasures to preempt the attack. It would allow for accurate and faster evaluation of system and network security. AMSEC can be integrated into the rule and correlation engines to perform effectively. Coupled with this, the distributed nature of the SIEM would make computations within AMSEC faster, accurate and more manageable.

C. Automate Security Controls testing using SIEM

Until now all the steps mentioned involved proactive involvement of the CSIRT members in the effective working of the SOC. All the above measures coupled with the large and varied IT landscape would make the SOC implementation a very complex and resource-intensive system. To make it financially viable and less resource intensive, the SOC system needs to be made effective by reducing complexity of the overall architecture [9]. This can be done by automating the security controls in the framework as proposed by Raydel et al. in [9]. Security automation as defined by Raydel et al. involves *"the automatic operation and monitoring of security controls by existing hard – and software security tools, reducing human intervention to a minimum"*[9]. According to them, for a security to be automated, it needs to be completely in machine readable format with no requirement for human intervention for decision making. For e.g. security training cannot be automated as it involves the human component. Furthermore, for a system to be automated all the security tools must be managed via a centralized architecture. All these are factors which are the inherent characteristics of the SIEM architecture which thus makes it a prime platform for automating security controls. The security controls are derived from the standard security compliance frameworks like ISO 27001, compliance Audit Guidelines, ISAE SoX standards, etc.

To illustrate the nature of an automated control, consider the A.10.5.1 from ISO/IEC 27001which looks into information backup. Automating this control via SIEM would mean that all the logging and monitoring of backup logs would be automated. Furthermore, in the event of a backup failure, the system would reschedule the backup without human intervention [9]. Raydel et al. have grouped the security controls that can be automated from the ISO 27001 framework and are enumerated below [9]:

a. *Asset inventory (hardware and software):* This control involves maintaining the inventory of all the network components of the organization. SIEM would help to track the inventory, its patch history, version history and installed software within it. It would perform automated patch installations and any deviations from the normal would be analyzed, prioritized and then reported to CSIRT team.

b. *Account management:* This control requires the presence of an Identity and Access Management (IAM) system which creates, modifies, deletes and performs recertification of user and technical accounts on a periodic basis. SIEM can be integrated into the IAM system to automate the monitoring of user accounts activities along with the maintenance of Segregation of Duties (SOD) matrix and automated deletion of accounts on disable.

c. *Log management:* Audit logs record events like network activities, security exceptions, user activities, exceptions, and other events. These logs need to be maintained for forensic analysis and audit reasons. SIEM can automatically collect, aggregate, analyze, correlate and provide proactive security alerts in case of any deviation.

d. System monitoring: This involves proactive monitoring of all information security events and for detection of system attacks. This is the primary task of SIEM as it supports near to real-time analysis of event and also correlate data from multiple source devices.

e. Malware protection: Organizations need to have malware detection systems at the critical entry and exit points in the infrastructure. They should daily check all systems to detect malicious code signatures and alerting the users. SIEM supports malware detection programs and can help in detecting zero-day attacks, backdoors, worms, Trojans, etc. via behavior analysis.

f. Vulnerability scanning and patch management: Organizations must scan their network components for vulnerabilities and must apply security patches on detection of one. SIEM can take it a level further and can automate the complete process. It can also perform correlation analysis based on the vulnerabilities identified and develop attack scenarios for exploiting the vulnerabilities and thereby preemptively stops an attack in its starting stages itself.

g. Security assessment and compliance checking: Organizations need to periodically assess their infrastructure vis-à-vis the compliance standards and industry best practices in order to maintain the most updated security infrastructure. This is done by implementing a configuration monitoring system which would perform remote testing for secure configuration elements. SIEM integration with these scanners would lead to centralized analysis of the system reports and also dynamically alerting any event or incident that would cause non-compliance. SIEM can generate detailed dashboards with evaluation scorecards for tracking these checks.

h. Information backup: As mentioned previously, SIEM can automate the backup process for all workstations in the organization and also take required steps to handle failed backups.

i. Physical security: Physical security is in the context of restricting employees to only those areas of the company to which they need to have access to. Critical environments such as datacenters, development centers, etc. need to be off limits for employees. SIEM can integrate with physical security devices to perform security event analysis. It can alert CSIRT team in case there is a security breach and also identify the target for the breach. This would help in restricting unauthorized malicious access in its starting stages.

j. Incident management: Organizations should implement incident management systems that would effectively track creation of incident ticket for detecting, analyzing, containing the impact, eradicating and recovering the system from a security breach. Integration of SIEM to incident management would lead to creation of incident tickets directly once a pattern of an attack emerges and notifies the CSIRT personnel before the attack reaches its full-maturity. This helps to preemptively stop an attack and take steps to reduce impact of an attack.

Fig. 2. illustrates the implementation of the above mentioned security automation architecture using SIEM as proposed by Raydel et al. in [9]. Currently all the mentioned security controls are managed in separate security applications. SIEM would lead to integration of all systems in a centralized place and help to be a one-stop source for all compliance activities. It would also automate the controls to a greater extent thereby reducing the complexity of the entire architecture. It can also perform correlation analysis across security controls which can lead to attack scenarios being computed from different security issues which otherwise would seem disparate and unconnected. This would make SIEM to become information security hubs to not just automate controls but also centralize all the security controls activities.

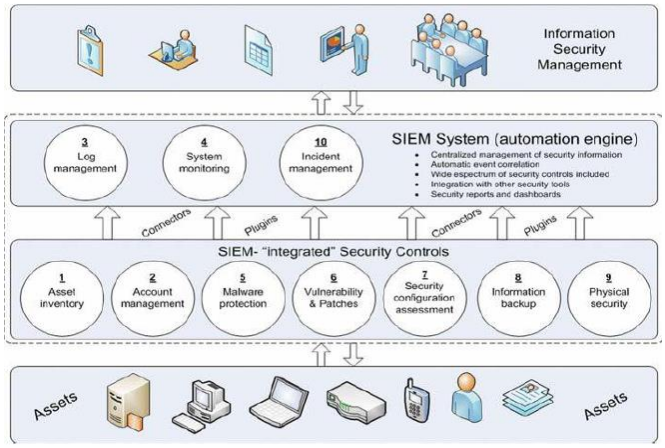

Fig. 2. Security Automation architecture using SIEM by [9]

IV. CONCLUSION

This study looks at the concept of SIEM implemented in organization and proposes a framework for enhancing it in order to build the SOC of future. Security infrastructure has to move beyond the logging activities and look at information retrieval and processing from logs. It needs to evolve from a log-centric approach to a information security data-driven approach. The study proposes a triad of enhancements in the existing SIEM setup. Firstly the SIEM architecture need to move from a centralized processing environment to a distributed computing environment for effective and faster process of security event. It then proposes the revamp of the security metrics calculation and attack graph creation from a single algorithm based approach to a more integrated approach by implementing multiple security calculation techniques in a single architecture. This can be done more effectively using the distributed architecture proposed for SIEM. Once the SIEM architecture and internal working is optimized, the study then proposes to build SIEM as a strategic centralized security monitoring and response application by automating most of the security controls defined within standard compliance standards like ISO 27001.

All these enhancements would help positioning SIEM as a more information processing and security intelligence system rather than a log collection application. There is a great scope for SIEM to develop further thereby creating a robust, less complex and almost automated SOC system.

ACKNOWLEDGEMENTS

This study would not have been possible without the support of my supervisor at K J Somaiya College of Engineering along with the faculty of the department of Information Technology at K J Somaiya College of Engineering. Also this paper is a result of the previous done by the SIEM research community without whom this paper could not have been written.

REFERENCES

[1] A. Azodi, D. Jaeger, F. Cheng, and C. Meinel, "Pushing the Limits in Event Normalisation to Improve Attack Detection in IDS / SIEM Systems," in *International Conference on Advanced Cloud and Big Data*, 2013, pp. 69–76.

[2] K. Detken, T. Rix, C. Kleiner, B. Hellmann, and L. Renners, "SIEM Approach for a Higher Level of IT Security in Enterprise Networks," in *The 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, 2015, no. September, pp. 322–327.

[3] E. Novikova and I. Kotenko, "Analytical Visualization Techniques for Security Information and Event Management," in *21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing*, 2013, pp. 519–525.

[4] I. Kotenko, I. Saenko, O. Polubelova, and E. Doynikova, "The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems," in *2013 International Conference on Availability, Reliability and Security*, 2013, pp. 638–645.

[5] R. Gabriel, T. Hoppe, A. Pastwa, and S. Sowa, "Analyzing Malware Log Data to Support Security Information and Event Management : Some Research Results," in *First International Conference on Advances in Databases, Knowledge, and Data Applications*, 2009.

[6] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The Operational Role of Security Information and Event Management Systems," *IEEE Security & Privacy*, no. October, pp. 35–41, 2014.

[7] J. Pavlik and V. Sobeslav, "Security information and event management in the cloud computing infrastructure," in *15th IEEE International Symposium on Computational Intelligence and Informatics*, 2014, pp. 209–214.

[8] I. Kotenko and A. Chechulin, "Common Framework for Attack Modeling and Security Evaluation in SIEM Systems," in *2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing*, 2012, pp. 94–101.

[9] M. Raydel, F. Stefan, and W. Baluja, "SIEM-based framework for security controls automation," *Information Management & Computer Security*, vol. 20, no. 4, 2014.

[10] I. Anastasov and D. Davcev, "SIEM Implementation for Global and Distributed Environments," *IEEE Software*, 2014.

[11] I. Kotenko and A. Chechulin, "Attack Modeling and Security Evaluation in SIEM Systems," *International Transactions on System Science and Applications*, vol. 8, no. December, pp. 129–147, 2012.

Steffi Raju, Department of Information Technology, K J Somaiya College of Engineering, Mumbai University.