Understanding & Replacing Security Information and Event Management

Atul Rana and Diksha Kochhar**

Abstract

The importance of Cyber security is growing each and every year, as the Cyber-attacks is getting more sophisticated and less detectable. The only option to make the defense stronger is by utilizing every possible source of information generated by log files of every major applications, services or components within the organization. The need for early detection of targeted attacks and data breaches is driving the expansion of new and existing SIEM deployments, which acts as an important part of every information security system, and provides one extra layer of defense. SIEM is an important and widely used security product and clear understanding of SIEM technology is critical for success in deploying the right SIEM product. Although planning a distributed enterprise SIEM deployment is always a challenge for information security teams at many organizations. This paper will stride you through the entire process of evaluating, selecting, and deploying a SIEM.

Keywords :- SIEM; LogManagement; Cloud SIEM

Introduction

Security information and event management technology has been around for over a decade. In general, SIEM is a combination of two product SIM (Security Information Management) and SEM (Security Event Management).

Security Information and Event Management (SIEM) systems provide centralized logging capabilities for an enterprise and can be used to analyze and report on the log entries it receives. The main function of a SIEM is collection of logs, aggregation, analysis and retention of the logs received. Logs are being collected from the various sources and as there are so many different formats of the logs, it is first normalized using a proprietary

* Information Security Officer- SOC Team, ABN AMRO BANK Ltd., Amsterdam, Netherlands, atulrana20@gmail.com

** Software Engineer, Wipro Technologies, Greater Noida, Uttar Pradesh, dikshakochhar3@gmail.com

format and then aggregated based on either number of events or on the time duration whichever is earlier and then it is analyzed and correlated by keeping different parts of the event like source address, destination address, port used and host involved etc. to get the clear view of the incident. After that information about the organization network and information of common threats that may be from stix and taxii feeds is also very useful. There are many providers that continuously updates the database of malware associated URL's and that information can be added to the SIEM system for the correlation. Alerts are generated as an output of the initial analysis. Reporting and dash boarding can also be created based on the queries to that data. Logs are usually stored within the SIEM system and are known as hot retention of the system and this may be from few weeks up to few months as per the organization architecture requirements and after which it is moved to an archive for complying with regulations and for future analysis. Generally, a SIEM system is a rules-based and has a correlation engine to establish relationships between multiple events from different log sources. In some systems, pre-processing may happen at log collection level, which includes applying filters and aggregating the events, and hence the volume of information that is being communicated and stored to the SIEM system is reduced, which will save the bandwidth and database space. The only issue associated with this approach is that, if an event is filtered out at this level, it cannot be recovered for future analysis.

Now a days the SIEM user's demands have increased, and with this the platform evolution to address them has also increased. Attackers are thinking differently, causing defenders to critically evaluate their current security products to keep a chance up. Zero day, sophisticated malware, pattern based analysis etc. attacks are now the major driver of security product evolution, but it is really difficult to detect these advanced attacks which are based on specific organization and are not know to everybody, so the organization needs to invest on this in terms of time and money in a complete different way as it was done previously.

SIEM is all together growing differently in a big way over the past 5-7 years, but still the real concern is in the case of a security incident where the SIEM is not at all capable to collect all the required information and completely fails to detect the threat. Generally, customers spend a huge amount of resources both in terms of time and money for SIEM implementation for the organization and if in return organization does not see any value of their investment then there are chances that they may move on in search of a better SIEM product.

Key challenges in existing SIEM

Organizations requirements for information security management have changed in last few years. The reasons for SIEM failure varies with the requirements of the customers. Below are the few main points discussed with regards to the SIEM customers, and the main reasons that are currently motivating the SIEM users to search for alternative solutions.

- Scalability: Organizations sometime try to scale and support growing, and often unpredictable log volumes becomes very problematic for lot of SIEM solutions. To address such problems, the systems need to be architected in such a way that it can handle max load volume, which take time to plan, design and build. It may also add up tremendously to the cost, as it may need big storage capacity which remains idle until see an unexpected or large volume.
- Dynamics Analysis: Dynamic Analysis is not only concerned with the real time flow of events but the main concern today is adding the behavior analysis and pattern analysis. This generally helps for the low and slow attacks with the environment. There are different methods for the machine learning and it is expected that machine will take minimum time to get the baseline information so that slow attacks can also be discovered.
- Time to value: Now-a-days, it is expected that SIEM platform should provide complete information along with all the alerts generated by it in order to get a clear picture of the attack. This helps in saving time by allowing us work

on the alerts generated rather than wasting the time in finding and analyzing the required information from other sources and then manually correlating it. Also, many of SIEM platforms are available with lots of out of box use cases which include features like: reports, rules and dashboards that are almost ready to use with a little or no alteration in them.

- Management Overhead: Managing of the execution environment requires a lot of work and resources. Even after procurement of hardware and software and deployment at critical infrastructure points, still there are lot of tasks that need additional efforts including establishment of user access, setting up databases and optimized for the expected performance and load, creating of use cases and providing data to the top management in terms of reports and dashboard which requires some more additional time.
- Cost: The SIEM is one of the most costly solution in the Information Security domain and its cost may varies based on the needs in term of the users required to access it or the space used to store the data in the database or in terms of EPS(event per second) received from the log sources. Hence it is purely based on the requirements of the organization deploying it.
- SIEM in the Cloud: Organizations may look to the cloud for standard services delivered according to a pricing model that scales in a linear way with their consumption of those services. In such cases Organization may want their SIEM to fit in the outsourcing model. SIEM typically requires significant data storage that client organizations are challenged to provide; has high scaling requirements with respect to event collection; provides third-party device data interoperability that outsourcers can leverage across multiple customers; often requires a 24 x 7 security operations center approach, and may involve a compliance mandate such as PCI DSS, ISO or HIPAA with tightly defined technical requirements where outsourcers can demonstrate core competency across multiple customers in the same vertical.

SIEM Evaluation and Selection

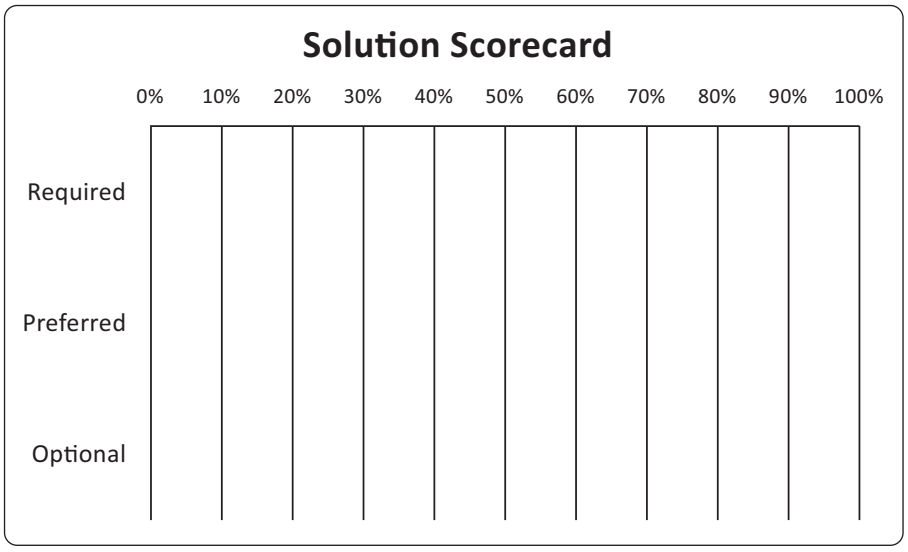
For the evaluation the present SIEM platform, organization needs to consider the issue from two different ways. First is the requirement is to analyze the current SIEM platform and future requirements of the organization. Secondly look at the use cases described in the earlier SIEM and weigh the impact of a newer platform on the organization. It is not like that the vendor offers more features and performance of their SIEM product, the organization should replace their current SIEM.

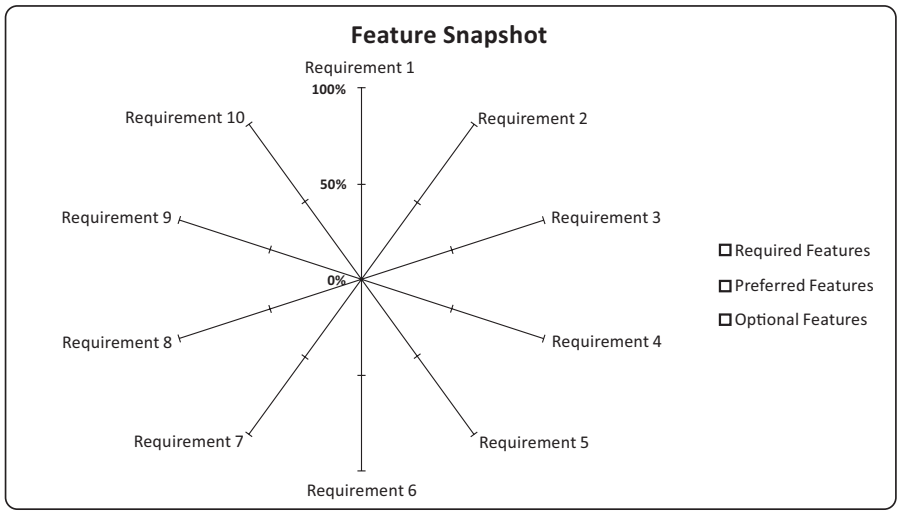
Even with today's mature product choices and proven deployment approaches, choosing an SIEM product is difficult due to the inherent complexities of its security-monitoring mission. To ensure successful deployment, enterprises must take several steps in their evaluation criteria. Organization must analyze the SIEM on the basis of its functionality, implementation effort, and maintenance effort, ease of operation, cost and maturity of the SIEM solution. The process of comparing and selecting SIEM tools is a complex task which requires both clear requirements and detailed knowledge of the SIEM technology. This task has been made even more demanding by the inherent challenges with monitoring complex and evolving IT environments. Consequently, the enterprise needs to evaluate not only the SIEM capabilities themselves, but also SIEM in the context of the larger security-monitoring architecture. Once the decision has been made to go with SIEM, the enterprise customer cannot just pick up any vendor segment based on broad categorizations. It must examine the technology to see which product provides the best fit in terms of cost of ownership, performance, usability and enterprise maturity.

A. Criteria Defined

- Required: An SIEM product which is built to be deployed at a large, global enterprise must satisfy all of these criteria. SIEM tools which does not qualifies with these required criteria may still be employed, but for a very specific purposes in which there is some work-around for a missing requirement.
- Preferred: Although not truly essential, these criteria make enterprise SIEM deployment, administration and operation much more effective and efficient and should be considered strongly while evaluating the product.
- Optional: These are the requirements that are considered nice to have as they are often those features that separate or differentiate the best solutions from average solutions. When evaluating SIEM, customers should see the future road maps which specify the organizations plan to meet desired criteria on the optional list.

The criteria of the requirement can be based upon Real-time monitoring, Deployment, Normalization, Scalability, Analytics and behavior profiling, Threat intelligence or Incident management support etc. There can be lot more other requirements depending upon the organization needs and hence all these requirements can be consolidated for SIEM evaluation and scoring.



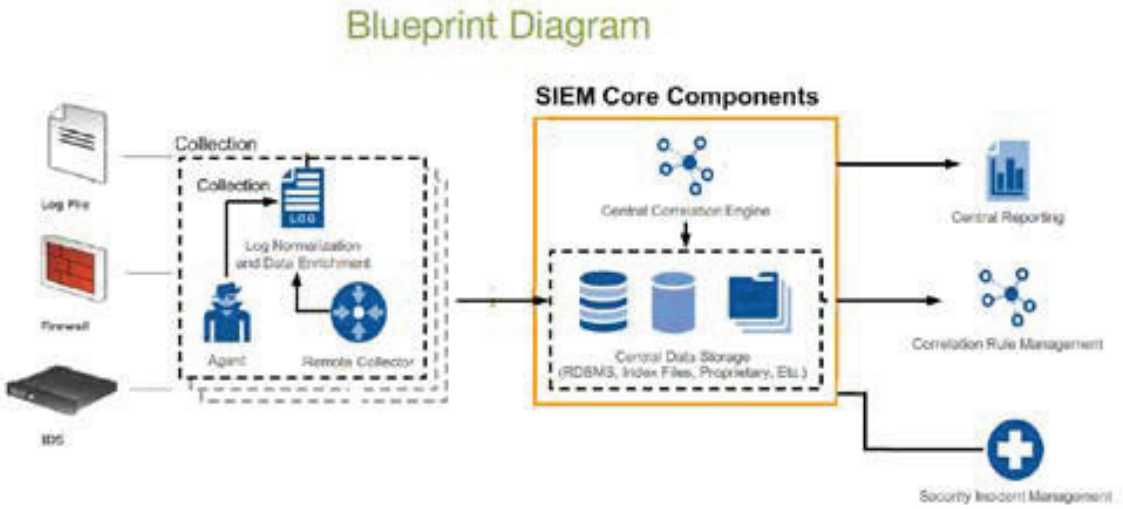


Once the vendor evaluation process is completed, organization is in a position to differentiate between all the vendors, and which vendor is the best fit. Successful decision-making on SIEM replacement is not only concerned with the vendor evaluation but also requires the self-evaluation as organization requirements. It is always important to differentiate between the self-evaluation and vendor evaluation because the organization cannot make the best choice without having a look at its available resources. Vendor selection is far more complicated than only matching the needs of the organization against the capabilities of the SIEM product demonstrated by the vendor. The output of the replacement of SIEM project is not a decision making but a recommendation to the top management about the SIEM evaluation. The final decision will likely be made by Top level Management. This decision generally isn't about objectives or technical facts, rather the decision could be based on the budget of organization that they have for that particular year or some external factors that may influence the decision.

Deployment

The new SIEM deployment process is not at all easy, as it takes effort to move it from current platform to new platform. It is generally recommended to start the deployment the new SIEM platform long before removing the old SIEM solution as the organization would like to have a fallback system until all the new SIEM functions have been tested against all the functionalities. The new deployment plan to the new security SIEM platform covers logs collection as well as logs migrating that are connected to the old SIEM solution and also include reviewing the old policies associated, reports, dashboards and deployment architectures. This new SIEM deployment process can be divided into two sub processes i.e. planning and implementation.

B. Architectural Steps



A. Deploy SIEM core components: Based on the deployment planning, SIEM requirements and particular product functionality, deploy SIEM core components that include the database for log data and normalized data, log indexing (to enable fast search), real-time rule-based correlation, and other SIEM components. It is expected to size the components based on the intended use cases and the environment. The organization should aim for 2 to 5 times the estimated ongoing load to support peaks in event volume, as well as future increases in data volume (if sustained usage is 1,000 events per second [EPS], peaks of up to 5,000 EPS are likely and should not lead to data loss).

B. Configure SIEM collectors and collection policies: Configure log collection policies for the SIEM collectors and agents, enable and configure local log retention. There can be multiple options available at this level. It can either

send data directly from Log Sources to the SIEM Solution for analysis or by collecting all data and gather it in local storage and then, send a filtered subset of the data to central correlation components and central retention, this approach allows a SIEM deployment to scale globally. It also enables context collection, such as vulnerability data and threat intelligence.

C. Define and then refine incident management workflows: SIEM alerts will sometimes cause a security incident to be triggered, and the basic incident response process needs to be in place before SIEM alert is implemented. The triage process should be alert to enable the organization to act on the alert by declaring an incident, tweaking the alerting criteria, etc. The security incident response process should be updated based upon the early alert handling experience to ensure that the alerts which are indicating a major incident are never buried. An effective SIEM deployment will lead to more and better malicious activity detection and thus there is often an initial increase in workload.

D. Select Use Cases based on desired usage: Assuming that the incident response process is in place, than the correlation rules should be picked, and alerts and notifications should be configured. Focus on correlation rules that will trigger alerts with lower false positives (such as rules tuned to focus on specific key systems), and design response processes to execute upon receiving those alerts. Also reports and dashboards should be created and customized based on the intended usage and planned log sources.

Conclusion

This paper of understanding and replacing SIEM provides the recommendations for deciding whether an Organization needs to replace its existing SIEM platform, and if the answer is yes, then how can it take place. Organization needs to learn how to analyze data, from multiple sources, with better analysis capabilities, so that they can defend their organization from the latest threats. Only basic correlation of events is now a days insufficient for security analysis. It is needed to do more with data so that SIEM solution can also as well. It would be unwise to assume that SIEM replacement is always the answer as that is simply not the case every time.

References

Consumption Economics, The New Rules of Tech, by J.B. Wood, Todd Hewlin and Thomas Lah.

Demand More from Your Log Management Solution by Mark Bouchard, published -AimPoint Group 2009

Gartner lists the following five vendors as leaders in the Magic Quadrant for SIEM, published July 2015

IBM, HP, Splunk, Intel Security and LogRhthymG. Eason, B. Noble, and I.N. Sneddon (1955), "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," *Phil. Trans. Roy. Soc. London*, *A*(247), 529-551.

IBM QRadar Security Intelligence; Independently conducted by Ponemon Institute LLC, February 2014

IBM Security - IT executive guide to security intelligence, published June-2015

NETFORENSICS SOLUTIONS BRIEF- SIEM in the Cloud - Cost-effective Solutions for Taking Control of Data Overload and Scaling Security, published 2015

Overcoming Common Causes for SIEM Deployment Failures, 21 August 2014, G00260858

SIEM 2.0 Its time to replace the SIEM by Securosis -www.securosis.com