Security Information and Event Management: An Analysis on Present Day Involvement and Clarification

Drashti Bhavsar[1] Krunal Joshi[2]
[1]PG Student [2]Assistant Professor
[1,2]Sal Institute of Technology & Engineering Research, Ahmedabad, India

Abstract— Security Information and Event Management systems depend upon a lot of planning before performance begins. The procedure to SIEM success is not an easy one, but done right it can play a demanding role in analysing and classifying security breaches. Security information and event management (SIEM) technology guides threat detection and security incident response through the real-time collection and historical resolution of security events from a wide variety of event and provisional data sources. It also supports compliance reporting and incident investigation through investigation of historical data from these sources. The root capabilities of SIEM technology are a broad scope of event collection and the skill to correlate and analyze events across disparate sources.

Key words: Security Information Event Management System

I. INTRODUCTION

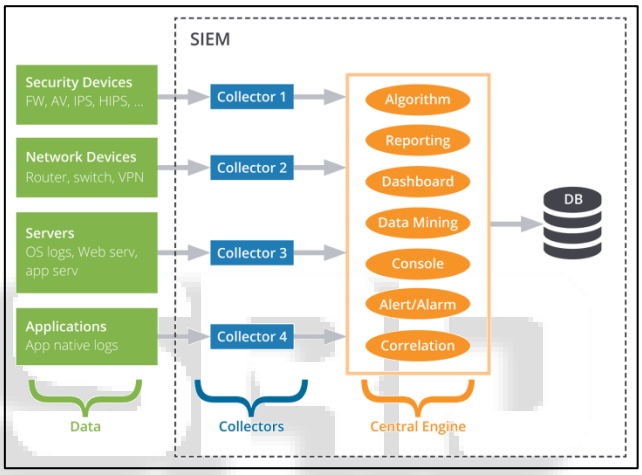
Security information and event management (SIEM) is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system. The acronym SIEM is pronounced "sim" with a silent e. The elemental fundamental of every SIEM system is to mix relevant data from multiple sources, identify modification from the norm and take appropriate action. For example, when a probable issue is detected, a SIEM might log additional information, generate an alert and instruct other security controls to stop an activity's progress. An SIEM Solution set up security/network administrators to collect log data (of all events) from a wide variety of network devices across the whole network to (mainly) identify and report on security threats and suspicious behavior. SIEM solutions also facilitate Forensic Investigation (Who did what where and when, and perhaps even why!) and comprehensively manage the collection, storage and archival of all log data generated by multiple network devices over a long period of time.

II. SCOPE OF SIEM

Before the start of a SIEM environment installation, it is very important to set a scope and a focus. The outlook is the operator behind SIEM and can be related to compliance, security or operations. It can be a combination of all three and should encircle the entire company. If there is a compliance scope needed for one part of the company and a security scope needed for another, the work for a SIEM environment should take both into account. It might be that the company is too large to start implementing SIEM everywhere at once. If that is the case, the focus should be limited. The target defines an area where SIEM is applied: a certain subset of the entire company. This target can be as narrow as needed as long as the primary process of the organization is present. Some examples of such a focus are:

- Focus on a location, such as a store, a region or an entire country
- Focus on the chain of a specific product, such as dairy products.
- Focus on a certain channel, such as web based or phone based customers. The scope and the focus can be chosen separately although they are connected.

III. SIEM OVERVIEW OF ENVIRONMENT



A. Data Sources

SIEM system gets data feed from various devices which not only include networking devices but also some physical security devices like bio metric devices, card readers.

B. Data Collectors

Primary function of data collector is to do normalization. This normalization happens in two ways it first normalize the values such as time zone, priority, severity in to common format, then they normalize the data structure in to common format. Sometime collector do aggregation for example if there are 5 similar events in less than 3 second then collector can send only one such event. This filtering increases efficiency and accuracy and reduce processing time.

C. Central Engine

This is heart of SIEM system which mainly does applying data mining algorithm. This engine writes events in to database as they stream into the system. It simultaneously processes them through data mining engine where correlation happens. It also has user interface to display result of data mining algorithm. It enables end user to change certain properties of algorithm. Some of other component of this engine is reporting, alerting, and dashboards.

D. Data Base

As events stream in to central engine they are written in database with normalized schema. This storage helps us to do forensic analysis on historic data. By storing the events we can test new algorithm on historic data.

IV. KEY FEATURES OF SIEM

A. Real-Time Event Correlation

A lag in detecting and responding to security threats can be costly for businesses of all sizes. Receive instant notification and quickly remediate threats by processing log data in-memory.

B. Threat Intelligence

IT security threats are dynamic, and attack vectors are ever-changing. Alert on suspicious security events via threat intelligence feed that inspects for matches against known bad hosts and other risks to your environment.

C. Active Response

Continuous IT security requires swift action at the first sign of concern.
Mitigate threats instantly with automated actions that block IPs, stop services, disable users, and more

D. Advanced Search and Forensic Analysis

Your ability to prove the limited impact of a security incident could save your business from fines, penalties, and even legal action. See value instantly with built-in defaults, correlation rules, reports, and active responses.

E. USB Device Monitoring

USB flash drives pose an ongoing risk to IT security—whether by aiding data leaks or introducing threats to your network. Gain valuable insight into USB device and file activity while enforcing USB policies.

F. IT Compliance Reporting

Demonstrating continuous IT compliance to auditors can be both challenging and time consuming. Streamline compliance with out-of-the-box reporting for HIPAA, PCI DSS, SOX, ISO, NCUA, FISMA, FERPA, GLBA, NERC CIP, GPG13, DISA STIG, and more.

V. SECURITY PROBLEMS

Weaknesses in policy definitions? These weaknesses include both business and security policy weaknesses. A simple example of this type of weakness is not having a written security policy. If you do not have a policy, how can you enforce it?

Weaknesses in computer technologies? These weaknesses include security weaknesses in protocols, such as TCP/IP and IPX, as well as operating systems, such as UNIX, Novell NetWare, and Windows. An example of a computer technology weakness is the Back Orifice attack, which allows a hacker to remotely control a Windows-based system.

Weaknesses in equipment configurations? These weaknesses include the setup, configuration, and management of your networking devices. An example of equipment configuration weakness is not assigning a password to a Windows 2000 server's Administrator account or to a Cisco router's console port.

VI. MAJOR EVENT PLANNING PROBLEMS AND HOW TO SOLVE THEM

Arranging a corporate event is a massive task and as an event professional, you surely knows how demanding it can get. However, with the help of a cautiously devised plan and the right kind of tools in your hands, you can be the event ninja.

A. Overspending or Not having Enough Money

Getting into the black hole of poorly crafted event fund is not something new. I am certain that every event planner has faced this problem at some or the other time. The idea of 'plan and spend as you go' is what most of the event planners are incorporating and hence, they wind up either spending more then the actual budget. Or sometimes it is too late to realize what mistake they have made. And hence, framing an event budget and deciding where and how to spend your event funds as soon as the planning incepts is recommended. Do your research regarding your event supplies, create a spreadsheet of estimated costs and sit with the team to finalize your budget.

B. Not considering Little Things

And by little things, I mean those last minutes tasks and details that fall in-between at the end moment. Though, when you fail to do them, they hit really hard. For instance, forgetting to take the specific technical equipment that you'd need or changing the seating arrangement. Therefore, it would be appreciated if you form a team. The benefit of having a great team is that you'll not have to remember every single detail and do every little task by yourself. Assign tasks to your team and follow up with them every week to know how things are falling. This is a productive way to get things done without letting them fall into the cracks at the last moment.

C. Choosing the Venue

Selecting the perfect venue which suits your event is arguably one of the most important things in event planning. An event venue sets the theme for the event and many other subsequent details like whether you'll need decor or transportation and such things. It is recommended to choose a venue which fits to your event and adds a lot of value too. Value can be anything of importance which is being facilitated with the venue like projectors, free Wi-Fi or other tech products. Choosing a venue which adds value to your event will drastically bring down your event planning time and spending.

D. Uncooperative Weather

Uncooperative weather is an instant epidemic which can totally break your event within a few seconds. And hence, preparing yourself with the backup supplies is recommended. You might not be able to face snowstorm or extreme heat wave but you can surely tackle rain showers, light snowfall or moderate heat with a little homework and having extra supplies on hand.

For example, prepare yourself with umbrellas and ponchos in case rain is in the forecast. Or maybe you can stock up juices, water bottles and sunglasses. Your attendees will surely appreciate your forward thinking.

Also, this way you get an extra opportunity to market your event through event merchandise.

E. Running Out of Time

I remember an event planner friend who always used to think that he had enough time to pull off his next event. And he always ended up thinking why didn't he start planning sooner? Are you also like my friend?

Therefore it is advisable to plan as soon as possible by outlining your short term vs. long term goals.

Depending upon the complexity of your goals, figure out a specific time to touch base your progress on the calendar. Here is a sample timeline for you to incorporate.

- 1 Year From Event—Define goals, event schedule, external schedules, define budget
- 8 Months From Event—Make sure venue, speakers, topics are defined and revisit goals
- 6 Months From Event—Revisit budget, refine messaging and purpose, reconfirm with all participants
- 4 Months From Event—Finalize invitation strategy (mail, online, calls, other outreach)
- 2 Months From Event—Begin invitations and external messaging as appropriate
- 1 Month from Event—Confirm attendee list, continue outreach as necessary. I coming weeks send "reminder" to guests make sure they know the purpose of your event and all pertinent information.
- 1 Week Post Event—Meet with organizing time to discuss success / failures of event and if goals were met. Document all and develop success plan for next time. Begin any outreach follow up needed.

F. Too Many People

If you've got a larger than expected crowd, well your marketing tactics did wonders! Congratulations! *applause*While a large crowd is what every planner dreams of but having them at the same place would require some kind of crowd control and hence it is important to understand the dangers of it. Be ready with adaptive strategies that can keep a large crowd organised with proper signage in the entire event venue.

Also, keep a track of how many people are planning to attend your event through the discussions, engagement and panels through the event app. Figuring out these things will not only create a stress-free environment but will also rise the level of trust among your attendees regarding your planning skills!

REFERENCES

[1] Nicolett, M. and Kavanagh, K. M. (2012a). Critical Capabilities for Security Information and Event Management. Gartner RAS Core Research, (ID:G00227900).
[2] D. R. Miller, e. a. (2011). Security Information and Event Management(SIEM)Implementation. TheMcGraw-Hill Companies.
[3] Gostev, A. Kaspersky Security Bulletin: Statistics 2008, https://securelist.com/analysis/kaspersky-securitybulletin/36241/kaspersky-security-bulletin-statistics-2008/
[4] Overcoming Common Causes for SIEM Deployment Failures, 21 August 2014, G00260858
[5] Consumption Economics, The New Rules of Tech, by J.B. Wood, Todd Hewlin and Thomas Lah
[6] IBM QRadar Security Intelligence; Independently conducted by Ponemon Institute LLC, February 2014
[7] Gartner lists the following five vendors as leaders in the Magic Quadrant for SIEM, published July 20, 2015: IBM, HP, Splunk, Intel Security and LogRhthym

