Cheatography

Security & Event Management (SIEM) Cheat Sheet

by [deleted] via cheatography.com/2754/cs/12179/

Introduction

Security information and event management (SIEM) systems is an approach to get a centralized view of the information coming out of multiple defense mechanisms, end user devices, applications and servers of the organization in most understandable and standard format. It serves multiple purposes like auditing, reporting, log retention, incident response and most importantly real-time monitoring which provides a capability to alert at the initial stages of cyber-attacks to your organization. In Summary, it will show what you want to see. Hence, to get most out of it, it should be managed properly.. Most companies buy SIEM tool and deploy it to infrastructure setup. As a practice, the next course of action is to point as many data sources as possible to it. This approach undermines the true capability of SIEM systems. We have to keep in mind that SIEM is not just for logging infrastructure data. Its primary and most useful capability is - real-time monitoring which makes it capable of alerting while the organization is under ongoing targeted cyber-attack.
Based on some hands-on experience on SIEM from both Operations as well as Infrastructure Implementation side, below are few suggestions that can be followed as best practices for SIEM:

Credit:
https://securitycommunity.tcs.com/infosecsoapbox/articles/2017/03/09/security-information-and-event-management-siem-solution-best-practices

Consider Network Modelling:

It is important to know “that” everything in your environment. More specifically, the zones a network is divided into. This helps in identifying critical assets and business impacting sections. Even though identifying all the assets might a time-consuming task, but this one-time activity is crucial while performing the investigation or reporting the data. Proper asset modeling increases the quality of events by providing more granular details about the hosts involved for example, if zoning is done in a most proper way it can identify if type of asset is from Citrix server farm, a domain controller or a DMZ machine etc. along with the geographical view of the IP location. It is like knowing your audience or I can say, victims..

Roles should be defined in SIEM for users

This way we not only implement access controls to SIEM but also maintain the integrity of content built in tool. For example, a critical rule has been created to alert for a suspicious activity targeted on your organization. Now, if every user will have same access in tool then anybody can mistakenly tamper the rule while exploring the SIEM functionalities and you might not get this critical real-time alert while cyber-attack are underway.

Roles should be defined in SIEM for users (cont)

Hence, access based on roles should be set, so that only authorized member can make any changes to resources of SIEM..

Integrate SIEM with the ticketing system

This will ensure the automatic creation of records, and also initiates a formal & effective follow-up process. Automation saves analyst’s valuable time which can be used for further digging into the alerts and getting finer details. These records can also be used in incident response for reference. For instance, a correlated event identifies a machine with malware; as a follow-on and predefined action assigned to this event SIEM triggers ticketing system to create a priority 1 ticket and assign it to end user or technology desk team in order to take the machine out of network. Hence you can save some time of yours due to this automation and spend it for gathering further info on malware or something more important related to this event..

Don’t let the logs define your requirement

Have the use cases and requirements in place first and then decide on the type of logs you need to be pointed to SIEM. For e.g. You have just set-up SIEM in your organization and you have pointed all IDS logs to it without any use case or requirement for same. Now, Millions of logs coming to the tool and not being used. Suddenly, for instance, there is a requirement to have a real-time alert for botnet traffic towards your environment. That is when thinking what logs you need in SIEM to detect Botnet traffic and at that point, you might realize that IDS logs are not of much use. But what you might need is Antivirus and firewall logs in SIEM to correlate and generate a real-time alert for this suspicious activity. Hence, before integrating any resource with the tool your approach should be reverse like What you want to achieve, How you want to achieve (logic) and What resources /data you need to achieve the goal. This helps us out in avoiding the undesired overload on SIEM and to bring the more value add events to it..

Dedicated Teams to focus on

Dedicated Teams to focus on operational, infrastructure and response tasks: SIEM is a huge system in itself and when it comes to a big organization which has the big infrastructure and involves humongous data. We should make sure that tasks related to SIEM have been properly structured and divided. Dedicated teams for Operations, Delivery and Incident response for handling the multilevel and focused end to end activities related SIEM as a whole.

Use Most Recent SEIM Tool

SIEM tool should always be at Latest and greatest version possible: We should make sure that tool we are using is getting latest releases applied, this not only helps in keeping the tool free from vulnerabilities and but helps you by making all the latest added functionalities introduce by the vendor in the tool available for you.

Continuous capacity review & optimization

As we point a large amount of data to SIEM; performance assessment should be regularly executed. A large amount of data correlation, heavy reports etc. can cause slowness and degrades the performance of SIEM. Hence, one must consistently perform the capacity analysis of the tool to make sure we are not overloading the SIEM infrastructure with a heavy load of events. If not followed, this may lead to data leakage or event loss originating from the data source to SIEM. Also, one should have the baselines define and communicated within teams as well so that existing infrastructure could be upgraded to accommodate future needs. Additionally, for existing data, regular fine tuning is a must and additional aggregation or filtering should be added based on the post-integration observ-ations. This reduces the load on SIEM, retains the more relevant events and also maintains the performance of the tool..

SIEM should not be treated as log database

As SIEM tool has multiple functionalities like real-time monitoring, auditing, forensics & reconnaissance, reporting. Data logging should be done through a dedicated log management tool or appliance which is compatible to existing SIEM in your environment for having better data retention as well as data retrieval.