Incident Response Management

Dr. Digvijaysinh Rathod

Institute of Forensic Science Gujarat Forensic Sciences University

ABSTRACT

Incident Response is an important component of an enterprise business continuity and resilience program. The increasing numbers of information security threats can damage enterprise working business and can harm enterprise information assets. A well configured Incident Response Framework can help reduce the number of Incidents.Understanding the incident and methodologies to effectively manage unexpected disruptive events with the objective of minimizing impacts and maintaining or restoring normal operations within defined time limits should be important part of any companies' business plan. The aim and objective of this paper is to propose and configure an effective incident response management framework to detect, report and eliminate the incident. Same proposed IRM framework is configured and tested with AlienVault named 'OSSIM'.

Keywords:- Incident Response Management (IRM), OSSIM. Alienvoult

1.INTRODUCTION

Keeping the company's data secure isn't an easy job. Modern corporate world is emerging with more and more systems and application than ever before, keeping everything available and running can be a headache for IT security professionals. When it comes to preventing the worst-case scenario in the corporate, having as many help as possible on hand is always what is preferred. Understanding the seriousness of the subject and lack of awareness in the corporate bodies. With this paper, My plan is to do my research in the subject of Incident Response and implementation of Incident response framework and see how much effective a framework can be to prevent real life incidents in enterprise.

According to SANS, There are 6 key phases of an incident response: [1] Preparation, [2] Identification, [3] Containment, [4] Eradication, [5] Recovery, [6] Learning a lesson [1]. There are different type of tools available in the market for each phases. But configuring all of them and making them work together can be a tough job.With this research paper, I am aiming to propose one framework which can work on all of the mentioned phases.

2.METHODOLOGY

Incident Response Process methodology (Figure 1) consists of mainly 4 phases: [1] Monitor, [2] Determine [3] Establish, [4] Action. Incident response is set of procedures focused on identifying, investigating and taking action on potential security incidents with one aim in the mind and that's to minimize the impact and recover the assets as soon as possible. It is said by many security experts around the world that the more an enterprise approach an incident response as a business process the more successful they can be

Monitor

First phase of the methodology is about monitoring. Network and asset monitoring tools are being used at this level to identify abnormal behavior that may require investigation. Logs are the most helpful source to understand what is happening in the network, but monitor needs an incident response framework that can put together all the logs and can come up with proper reports and alerts from it. IDSes monitor server and network activity in real-time. They typically use signature analysis to identify an issue. Network flow analyzers examine actual traffic within a network. If monitor is tracking a particular thread of activity or just getting the idea of what protocols are being used in the network and which assets are transferring data amongst themselves, network flow analysis is an excellent approach. Vulnerability Scanners identify potential areas of threads and provide help to assess the attack surface area of the enterprise, so that remediation task can be implemented as soon as possible. The entire idea of incident response is to avoid downtime as much as possible. That is where availability monitoring systems comes handy, because asset or software outage could be the first sign of an incident. Web proxies can also be helpful as their ability to log what is being connected to be vital. Many threats operate over HTTP, so being able to log HTTP connection can be vital for forensics.

Determine

If organization wants to know which events to prioritize, they need an understanding of all the critical systems in the network and what software are installed on those systems. Importantly, they need to understand their environment to evaluate criticality of an incident as a part of the determination process. The best way to do this is by using automated asset discovery framework and inventory that can be updated when things change.
Threat Intelligence provided a global information about threats from the real world. Things like bad reputation IP Addresses, CoC servers and more, can be applied against enterprise network assets that can provide a full context for the threat.

Establish

Generate a report and document everything from the incident response process, especially all the communications and data collected and the decision-making processes. Organization's security policy are used as tactics on this phase. Such policies are usually stored in hard copies. So, There is no tool that is available for this phase, Organizations are heavily relies on skillful employees and Incident Response team members.

Action

Data Collecting and Incident forensics tools cover a broad category of all types of media. They examine digital media with the aim of identification, prevention, recovery, analysis and presentation of the facts and opinions about the information; they are designed to create a legal audit which can be presented in the court of law.

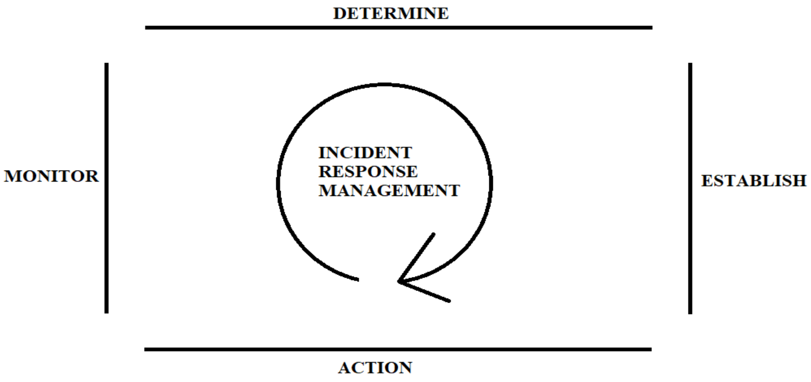


Figure 1. Incident Response Management Phases

3. EXPERIMENTAL SETUP/CONFIGURATION

It is completely possible to use different tools for all the different phase of the Incident Response process but managing a lot of tools requires a lot of resources and human interaction and it might get tricky sometimes to make all the tools effectively work together in one environment. So, It is always nice to have one tool which can work on all the phases of incident response process. Alienvault's OSSIM (Figure 2) is one such tool and can be used in corporate for all-in-one approach for incident response management. OSSIM (Open Source Security Information Management) is an open source security information and event management system, integrating a selection of tools designed to aid network administrators in computer security, intrusion detection and prevention.

The project began in 2003 as collaboration between Dominique Karg, Julio Casal and later Alberto Román. In 2008 it became the basis for their company AlienVault. Following the acquisition of the Eureka project label and completion of R&D, AlienVault began selling a commercial derivative of OSSIM named as AlienVault USM (Unified Security Management).

As a SIEM system, OSSIM is intended to give security analysts and administrators a view of all the security-related aspects of their system, by combining log management and asset management and discovery with information from dedicated information security controls and detection systems. This information is then correlated together to create contexts to the information not visible from one piece alone.

OSSIM performs these functions using other well-known open-source software security components, unifying them under a single browser-based user interface. The interface provides graphical analysis tools for information collected from the underlying open source software component (many of which are command line only tools that otherwise log only to a plain text file) and allows centralized management of configuration options.

The software is distributed freely under the GNU General Public License. Unlike the individual components which may be installed onto an existing system, OSSIM is distributed as an installable ISO image designed to deployed to a physical or virtual host as the core operating system of the host. OSSIM is built using Debian GNU/Linux distribution as its underlying operating system.

OSSIM is really easy to setup and start working with in the network. For this experiment, I will be using a Virtual Box. First thing first, We will download an ISO from their official website and then configure it in the virtual box. ISO can be downloaded from the official website without any cost. The System requires 4GB of RAM, 2 core processor and minimum 20GB free harddisk space to run. Once opened in the virtual box. You will be prompted with easy select and next type of installation. You will need provide details like language, country, OSSIM host's IP address, network mask, gateway of the network, password for ROOT user which will be used later on to log in to the system. Once this all information is given. Installation process with start and within few moments, it will be done. You will then be able to see command line system from where system settings can be accessed using command, OSSIM requires one guest system on which, It's interface can be accessed using HTTPS protocol. We will be using one windows guest machine on different virtual box to access the web interface of the OSSIM. On the first access, User will be needed provide basic details like Name, password and E-mail ID. Once it is done, user can login to the web interface using admin user and start configuring all the devices from the network into the OSSIM. For configuration. User is prompted with mainly 4 steps. [1]Network Interfaces, [2] Asset Discovery, [3] Deploying HIDS, and [4] Log management.

[1] Network Interfaces

All the different type of network interfaces can be configured on the OSSIM on this step. Mainly for network monitoring, log collection and scanning. Once the network is configured, OSSIM can get the network data passively or can reach out to the desired device in the network.

[2] Asset Discovery

Once the network interfaces are configured, OSSIM must be aware of the assets in the network in order to start the monitoring. There are mainly three ways to add assets to monitor: Either OSSIM can scan the network to find the assets, Or we can import the CSU file for assets or we can add all the assets manually. User can add mainly three type of assets: Windows, Linux, and Network.

[3] DEPLOYING HIDS

Very interesting feature that OSSIM provides is the ability to remotely install HIDS on all the assets. HIDS can perform file integrity monitoring, rootkit detection and can even collect event logs for OSSIM. So, user can easily manage all the assets from one place. HIDS is locally installed on windows and for Linux, HIDS monitoring is configured for remote monitoring.

[4] Log Management

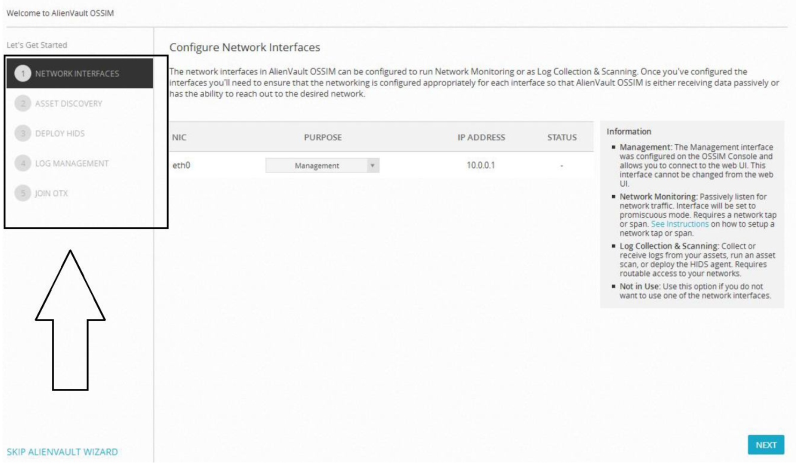
Once All assets are configured, OSSIM will start monitoring the device in the network and Log will be started generating. Here, User can configure certain settings related to log management.

Once all the configuration is done, HOME screen of the OSSIM is available for users to see stats and logs for the network. All the information is available in 2 options: Live & Stored.

It mainly has 5 different Tabs for certain tasks:[1]Dashboard, [2] Analysis, [3] Environment, [4] Reports, [5] Configuration

[1] Dashboard

It provided in general information about the network including recent alarms, top 10 events , hosts with multiple events, event sorted by sensors or data sources and chart of on what time the logger got most events.



Welcome to AlienVault OSSIM

Let's Get Started

Configure Network Interfaces

The network interfaces in AlienVault OSSIM can be configured to run Network Monitoring or as Log Collection & Scanning. Once you've configured the interfaces you'll need to ensure that the networking is configured appropriately for each interface so that AlienVault OSSIM is either receiving data passively or has the ability to reach out to the desired network.

NIC	PURPOSE	IP ADDRESS	STATUS
eth0	Management	10.0.0.1	-

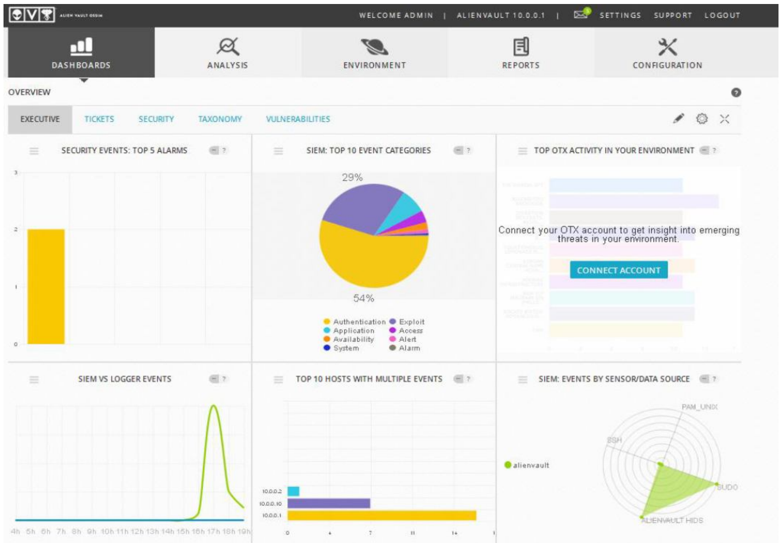
Information

- **Management**: The Management interface was configured on the OSSIM Console and allows you to connect to the web UI. This interface cannot be changed from the web UI.
- **Network Monitoring**: Passively listen for network traffic. Interface will be set to promiscuous mode. Requires a network tap or span. See Instructions on how to setup a network tap or span.
- **Log Collection & Scanning**: Collect or receive logs from your assets, run an asset scan, or deploy the HIDS agent. Requires routable access to your networks.
- **Not in Use**: Use this option if you do not want to use one of the network interfaces.

Figure 2 Configuration of Alienvault's OSSIM

[2] Analysis

It provided a place from where user can do in-depth detailed analysis (Figure 3) of the captured information by the OSSIM monitoring tool. So that user can have knowledge about all the events that has taken place in the network along with the details like which device it was generated from and what kind of event it was.



Connect your OTX account to get insight into emerging threats in your environment.

Figure 3 OSSIM Analysis Report

[3] Environment

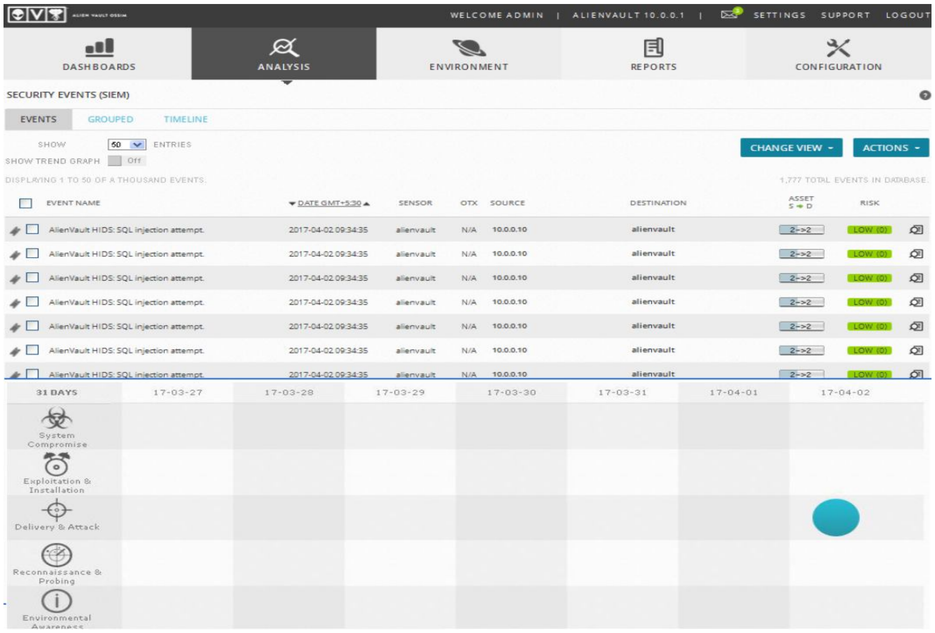
It provided details about network flow in the form of graph to know which device generated the most network traffic and which protocol/Service/Process is being used the most.

[4] Reports

OSSIM also provides a facility to directly generate a report from the tool itself and either download it or send it via E-mail. User can download entire report or can select certain options from filter and get the report accordingly.

[5] Configurations

User can make changes to the configuration (Figure 4) of the assets and network from here. User can also configure custom policy for certain host or port according to the company's needs from here. OSSIM also provides settings about which port should be ignored and which port should get more priority by the monitoring service. That can also be set from here.



SECURITY EVENTS (SIEM)

SHOW 50 ENTRIES
SHOW TREND GRAPH Off

DISPLAYING 1 TO 50 OF A THOUSAND EVENTS. 1,777 TOTAL EVENTS IN DATABASE.

EVENT NAME	DATE GMT+5:30	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK
AlienVault HIDS: SQL injection attempt.	2017-04-02 09:34:35	alienvault	N/A	10.0.0.10	alienvault	2->2	LOW (0)
AlienVault HIDS: SQL injection attempt.	2017-04-02 09:34:35	alienvault	N/A	10.0.0.10	alienvault	2->2	LOW (0)
AlienVault HIDS: SQL injection attempt.	2017-04-02 09:34:35	alienvault	N/A	10.0.0.10	alienvault	2->2	LOW (0)
AlienVault HIDS: SQL injection attempt.	2017-04-02 09:34:35	alienvault	N/A	10.0.0.10	alienvault	2->2	LOW (0)
AlienVault HIDS: SQL injection attempt.	2017-04-02 09:34:35	alienvault	N/A	10.0.0.10	alienvault	2->2	LOW (0)
AlienVault HIDS: SQL injection attempt.	2017-04-02 09:34:35	alienvault	N/A	10.0.0.10	alienvault	2->2	LOW (0)
AlienVault HIDS: SQL injection attempt.	2017-04-02 09:34:35	alienvault	N/A	10.0.0.10	alienvault	2->2	LOW (0)

Figure 4 OSSIM Configuration

4.RESULT ANALYSIS

I decided to test how well the OSSIM manages the logs and generate events when some incident occurs in the network. So, I configured a kali Linux in the network with one windows machine as a victim and tried performing SQL-Injection on the victim machine using SQLMap.

SQLMap is an open source penetration testing tool. It automates the processor of detecting and exploitation of SQL Injection flaws. I entered this command in the terminal.
"sqlmap -u https://10.0.0.1/ossim -f"
Where –u is used to provide target in the form of URL and –f is to command SQLMap to perform fingerprinting.

OSSIM was successfully able to detect the attack and log the event. The tool was even able to tell what kind of attack it was, from where it was generated, which system was the victim and when the attack took place. It also uses a blue dot to show the severity of an attack on the calendar. The bigger the dot, the more dangerous the attack is.

Once the attack is identified, User can take necessary steps to mitigate the incident and can generate the report for further investigation. The OSSIM tool can be found really useful in such scenario as it can work as all-in-one tool in such incidents.

5.CONCLUSION

Incidents are not something any Corporate can underestimate. Having an intelligent approach towards incidents before they even occur is always a smart move. As we have discussed, It requires certain types of tools to work together in order to have an affective incident response management. But, making all different tool work together is going to be so much costly as well as hectic. That is why, having all-in-one solution is better in the terms of time consumption in configuration and easy to manage. There aren't many such tools available in the market and even fewer which comes at free of cost. That is what makes the AlienVault's OSSIM so unique. AlienVault also have a reach community, and they are always ready to help others and share if there is any new attack found. That makes the tool so much effective against new attacks.

REFERENCE

[1] https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
[2] https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response
[3] https://github.com/meirwah/awesome-incident-response
[4] https://www.us-cert.gov/government-users/reporting-requirements
[5] https://www.first.org/_assets/resources/guides/csirt_case_classification.html

[6] https://en.wikipedia.org/wiki/Computer_security_incident_management

[7] https://en.wikipedia.org/wiki/Incident_management

[8] https://www.alienvault.com/products/ossim

[9] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Incident-Management-and-Response.aspx