THREAT INTELLIGENCE: IDENTIFYING SECURITY THREATS

Vaibhuv Sharma[1], Vansh Sharma[2], Raman Solanki[3]

[1,2,3]IT, Guru Gobind Singh Indraprastha University, (India)

ABSTRACT

Threat Intelligence is well analyzed information used by Security Analysts to identify and act on threats which may produce uncertain bizarre results. Technology is being upgraded day by day, similarly cyber threats are reaching their vintage, in order to stop or act on such threats some classes needs to be followed while working on Threat Intelligence plans.

Keywords: Data Compromise, Threat Intelligence

I. INTRODUCTION

Threat Intelligence helps to update ones knowledge in the field of Information Technology and also enables a researcher to get handful of information regarding a specific threat which may be useful for an organization to use it as counterintuitive. There are various classes which are being used while working of Threat Intelligence. These classes explains how a organization can improve their security and behavior to further enhance their security systems, it also provides an insight to company's external links and infrastructure.

II. THREAT INTELLIGNECE CLASSES

We divide Threat Intelligence into five distinct classes, as they confront security issues faced by Security Analyst.

2.1 Internal Intelligence

It is related to organization's assets and behavior based on analysis of organization's activities. Today, many companies are providing security solutions in order to deal with risks that may affect financially. The "G4S Security Services India Private Limited" is an example of this.

2.2 Network Intelligence

An Intelligence obtained after analyzing a company's network that connects it to the outside world. Network Intelligence India provides such services to deal with network security flaws.

2.3 Edge Intelligence

To make sure what other hosts are doing at the edge of the network government, ISP's, and Telcoms monitors the organizations network by checking their Network Traffic, Network status and look for problem spots.

2.4 Open-Source Intelligence

An Intelligence that glean information from various sources such as websites, feeds, channels in order to gather as much information for their personal use.

2.5 Closed-Source Intelligence

This is the most difficult to acquire, as authentic information is required to make Threat Intelligence Plans, and this intelligence requires to check underground websites which can be only accessed by Government or Law Enforcements.

While working on Threat Intelligence Plans, one should go through these classes, as many security agencies can offer two or three Intelligence plans.

III. WHY DO WE NEED THREAT INTELLIGENCE

For an organization, threat does not mean competition. It could be Internal or External threat in terms of security. A company is always under pressure of maintaining their financial information from begin leaked or confidential data that may hinder their performance. For this, an organization may use Threat Intelligence in order to identify threats.

The following table shows some issues of compromise that can be identified with the help of Threat Intelligence.

Category	Indicators of Compromise	Examples
Network	• IP addresses • URLs • Domain names	Malware infections targeting internal hosts that are communicating with known bad actors
Email	• Sender’s email address and email subject • Attachments • Links	Phishing attempts where internal hosts click on an unsuspecting email and “phone home” to a malicious command and control server
Host-Based	• Filenames and file hashes (e.g. MD5) • Registry keys • Dynamic link libraries (DLLs) • Mutex names	External attacks from hosts that might be infected themselves or are already known for nefarious activity

TABLE: Identifying Indicators of Compromise using Threat Intelligence

IV. THREAT INTELLIGENCE WITH SIEM

Cyber Terrorists are upgrading their skills and methods and they can attack in every possible way, whether it’s a attack on Application based Infrastructure of an organization. The most common attacks are SQL Injection, DDOS, Phishing, Cross Site Scripting.

To detect and respond with such attacks an organization needs to implement SIEM (Security Information and Event Management) which provides real time analysis generated by network application. SIEM is a software and product service which helps an organization to identify threats and possible breaches, collects logs.

With the help of SIEM, you can detect bad links and block them by blacklisting bad IP's. You can also prepare for unknown attack attempts that can be made on your network.

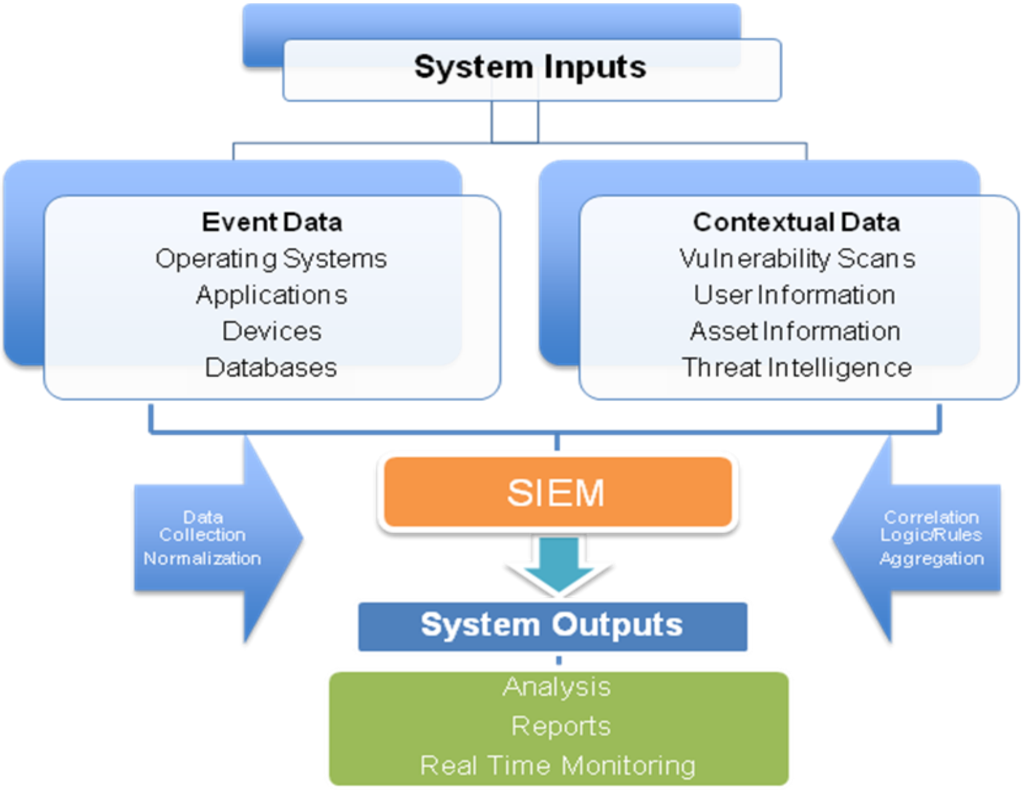

Fig. Architecture of SIEM

4.1 Feature of Siem

1. **Collection of Log:** To collect logs from heterogeneous sources such as Windows, Unix/Linux Systems, Databases and other application devices.
2. **Activity Monitoring:** SIEM has a unique way of monitoring their users. It records what action was taken by whom and what was the result?
3. **Real Time Event Correlation:** It means dealing with threats proactively.
4. **Log Retention:** SIEM also ensures that the gleaned data from various sources is archived in a centralized repository.
5. **Reports:** It is the core of SIEM, as reports are generated to ensure the future acts.
6. **File Monitoring:** This feature helps to monitor important files and folders and records the changes made on files and folders.
7. **Log Forensics:** It allows security professionals to search for a specific log easily.
8. **Dashboard:** The dashboard shows everything that is related to the organization's network such as flow of traffic, users activity.

V. CONCLUSION

For an organization it's important to think what might happen in future, especially when it's related to Security. Using products and services such as SIEM helps an organization to identify and acknowledge the threat and then act as per requirement. The increase in the rate at which the big organisations are being targeted is ascending and will ascend in the recent future. The formal and other informal organisations can prevent big mishaps and therefore be secure.

REFERENCES

[1] http://www.ibef.org/industry/india-automobiles.aspx

[2] http://www.siamindia.com/scripts/industrystatistics.aspx

[3] http://thehackernews.com/2015/11/what-is-cyber-threat-intelligence.html