International Journal of Engineering & Technology, 7 (2.7) (2018) 473-479

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A Novel Approach to Cyber Hazard Management Intelligence System

B. Bala Bharathi[1]*, E.Suresh Babu[2]

[1]M.Tech, Department of Computer Science & Engineering, &KLEF, Guntur, Vaddeswaram, Andhra Pradesh, India-522502.
[2]Professor, Department of Computer Science & Engineering, &KLEF, Guntur, Vaddeswaram, Andhra Pradesh, India-522502.
**Corresponding author E-mail: bharathi.bollu@gmail.com*

Abstract

Detecting and defending against insider and outsider threats seems to be a major challenge for information security system. such that cyber-attacks pose a silent threat for a company with a havoc likely to be in billions, besides slaughtering investor confidence and denting brand image. Long-established and ongoing solutions target mainly to assimilate many known threats in the form of consistent information such as logical & physical address, etc. into detection and blocking techniques. Our proposed solution elongates forward by using Cyber threat intelligence (CTI) which is used to inform decisions timely regarding subject response to the menance or hazard, where the vulnerable systems are identified using honeypot, through integration of logs for detecting network, host intrusions using SIEM technology which would efficiently manage the occurrence of threat by using cyber hazard management to mitigate the cyber threat actions, fortify incident response efforts and enhance your overall security posture.

Keywords: *Cyber Threat Intelligence (CTI): Cyber Kill Chain Model: Intrusion Detection system (IDS): Security Information and Event Management (SIEM): Cyber Hazard Management.*

1. Introduction

With ever-evolving cyber threat environment, organizations need to take a more proactive approach to cyber security enhancement to protect from unauthorized access [1]. For instance, the average statistical analysis on cyber-attacks in SQL injection over the past three years has occupied 2015 chart with a percentage of 17.5 prior to defacement's. Most seemingly, the second position of defacement's has turned to occupy the first position with a percentage of 34.7 in the year 2016 [2]. Currently malware attacks have chased in prior to the defacement's, which has occupied about 43.7% among the most devastating cyber-attacks in 2017 [3]. The major targeted sectors in 2018 are Organizations, Industry, Health care and Government. Nevertheless, data breaches have similar devastating effect. Some might take days, weeks or even years to detect an attack.

One of the recent data breach Equifax, occurred in mid-May and endured till July. The threat actor's hacked people's names, addresses, social security numbers, birth dates and driver's license numbers. The reason behind this attack was due to a flaw in web application [4].

The WannaCry ransomware struck across the globe. The impact of Ransomware thorns is causing annoyance to the cyber world. This cybercrime is provoking the renowned agencies, cave into digital extortion, where about 34 percent of the people are willing to pay the ransom amount instead of knowing how to defend. Most of the security reports have stated that "the average ransom projected 266 percent with cyber criminals demanding an average of $1,077 per victim." Such figures seem to be stunning to every individual. So, it is high time for every individual to grab the knowledge in right time, at right place and by the right person. In order to detect and prevent insider and outsider threats, organizations rely on cyber threat intelligence, which is used to inform decision regarding menance or hazard based on proper context and cyber hazard management to promote a faster defence in re-mediating the daunting situations [5].

This research aims to develop proactive CTI by using cyber intrusion kill chain system to identify and prevent cyber intrusion activities, whereas intrusion detection system- that monitors and detects network or system, SIEM technology collects centralized logs based on context, decision has been taken with respective of time for efficient threat management to mitigate the threat actions.

The remainder of this paper is organized as follows. First, we present the related work having the overview of cyber-attacks and threats in cyber world. In section 111 we present the overview of CTI. In section 1V we present a proposed architecture with underlying components and architecture principles. In section v we present the testimonial and result. And finally in section V1, we present conclusion and feature enhancement.

2. Related work

In this sub session we provide a basic overview of cyber-attacks and threats in cyber world. First we know about Cyber Threat-Cyber Threat is a probability or an opportunity to interrupt a computer network or an organized framework. Mostly threats vary from one organization to another, some organizations neglect to recognize Cyber threats. Usually adapted security metrics handle miss at potentially vulnerable areas, apparently spending long duration on action instead of vulnerability analysis, risk acknowl-

edgment and acclimation issues. Some of Possibilities of threat are- if the malicious actor has intention to attack an association, Capability is their means to do so (such as specific types of malware), Opportunity is the opening which is needed by the actor (such as vulnerabilities in software or hardware personnel). Threats may also occur from unexpected areas such as physical, natural, human, network, host, mobile and application … [6].
Threat Actor is also known as malicious actor. Threat intelligence is mainly categorized into 2 types they are External Threat Actor, Internal Threat Actor. External Threat actor has no trust or previously existed privileges, while the Internal Threat actor has some levels of trust and privileges. They may act as an individual or an organization but the incident would be intentional or accidental and its purpose is either malicious or warm-hearted. It is important to know who did the harm to you, what they want and how they plan to get it [7]. At the same time there would be large portions of risk from many threat actors such as Government sponsored, organized crime, hacktivists, insider threats opportunistic, internal use error [14].
Different types of threats, that CTI handles are Zero day attacks, advanced persistent Threats. Zero-day vulnerability is an advance attack that exploits a unknown security threats and exposes a software or hardware vulnerabilities before any individual understands that something went wrong. In fact there is no opportunity for detecting and preventing threat [8]. Whereas Advanced persistent threats gains unauthorized access and stay undetected for long period and steals data instead of damaging network or organization .In order to avoid detection, attacker rewrite the code and engage advanced bypassing techniques like spear-phishing, social engineering techniques to gain access to the network continuously through authorized way and creates a back door for ongoing access [9]. To overcome this, Threat intelligence mainly performs prevent data loss, Incident response, Threat analysis, Data analysis

3. Overview of Cyber Threat Intelligence (CTI)

Threat intelligence often arises in the form of compromised indicators, Third party feeds, Traffic analysis and other important devices log co-relation along with all reputation services. Once it has been collected, accurate techniques can be used to analyse and evaluate the source with context and that can be used to inform decision regarding menance or hazard [10]. Every Cyber security company mainly focus on providing alerts. The actual alerts are not just detecting the threat but preventing, analyzing and responding to the threat. The challenge that most of the customers facing today is dealing with thousands and millions of alerts. The path they missed through is the context and that is what cyber threat intelligence is all about.
Cyber threat intelligence is all about providing context. Security analyst usually starts with detection especially detecting zero-days or previously unknown malwares. Context is important to understand what you are dealing with and it also helps to formulate your response plan. Context includes things like who the attacker is and what they have done in the past as well as what are the indicators of compromise they typically leave behind. All these things enable you to answer certain key questions and plan your response [11]. When you have an intelligent response plan and you are not just responding to the current threat or the current alert and what they are likely to do in the future.

- who is threat actor
- Risk level associated with this particular threat
- How they operated in the past and what are they likely to do in the future
- we need to get into this model by having a lean forward defense
- Time to detect and respond to today's threats.

CTI is broadly divided into two wide classes. They are Strategic threat intelligence, Tactical Threat intelligence.

Fig.1: Cyber Threat Intelligence (CTI)

3.1. Strategic Threat intelligence

It informs how an organization defends itself and its overall cyber security posture by taking high level information and furthermore it deals with other human-readable items with respect to threat actors, their intentions, affiliations, interests, goals, capabilities, plan and campaigns. By getting situational awareness, Administration people who have knowledge on technology and appropriate skills will enable rapid decisions on automated or manual actions [12].

3.2. Tactical Threat intelligence

Tactical intelligence enlightens on what an organization needs to focus while using the tools and their allocation. It includes indicators of compromise (IOC), malware signatures, IP blacklists, URL blacklists, log files, traffic patterns, spear phishing, ransomware and other APT (Advanced persistent threat). Sometimes it identifies technical (Indicates the specific malware) and operational intelligence (it gives details of specific incoming attack, assess organization ability by using SIEM or Threat intelligence) which possess minute differences in usage. The challenges with tactical threat intelligence requires too much information and it is transferred to SOC (security operation centre),it will continuously monitor and improve the organization's security by preventing, analyzing and responding to Cyber security threats and incidents in real time [13] .
Security resources towards organizations aren't mature enough to give full control over all types of Threat intelligence. So, initially we have to focus on Strategic Threat intelligence. Furtherly, use a Cyber kill chain model for identification and prevention of Cyber intrusion activity. While there are many variations in these attacks, many of them use all attacks. So by knowing attackers tactics and their ways in operating to meet their goals help your association to become more successful and to deploy countermeasures [14].
At industry level, Cyber kill chain model patented by lockheed martin is very common to describe different APT's phases. This model specifies a life cycle of seven steps describing the path followed by the attackers to reach their goals [15]. LogRhythm considers a second APT life cycle model containing five phases [16]. Other actors like lancaster model, SDAPT model, BSI model propose cycles similar to both models with relatively minor difference in titles and number of phases [17] [18] [19] .
Cyber kill chain model exhibits the Cyber-attacks to recognize early stage detection and prevention from unauthorized release of data from computer or network [15]. It also assists to improve network defense by informing ways to prevent Cyber-attacks.

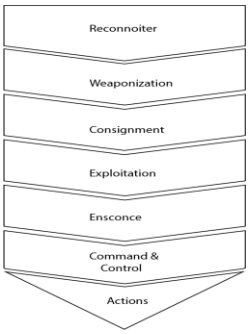

Fig. 2: Cyber Kill Chain (CKI)

Cyber kill chain is also known as Cyber-attack life cycle. Threats must going through a few phases in the model, including:

- **Reconnoiter**
  Threat actor selects target, gathers data about the target and technologies used by target. It also recognizes vulnerabilities in the network
- **Weaponization**
  Malicious actor creates remote access malware weapon, such as virus or worm to pursue vulnerabilities.
- **Consignment**
  Intruder transfers weapon to the target environment.
- **Exploitation**
  Use of vulnerability of a target computer to execute malicious code.
- **Ensconce**
  Malware weapon installs access point used by threat actor.
- **Command and control**
  Adversary requires a communication channel to control its malware and continue their actions.
- **Actions**
  It is the final stage of kill chain in which treat actors achieve their goals by implementing actions like data ex filtration.

4. Proposed Architecture

For effective analysis of threat data, security teams should adopt a cyber hazard management intelligence framework for processing all the information, which also needs to keep the data into proper context in order to react accurately. Implementing threat intelligent framework represents identification and mitigation of major threats for avoiding false positives and threats otherwise it shows its impact in administration of business practices.

The framework offers the following primary components.

- Intrusion detection system
- SIEM technology
- Threat Management

4.1. Intrusion detection system (IDS)

An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations [20]. IDS is a type of security management system for detecting vulnerability exploits against a target application or computer. It provides ability to block malicious activities and alert administrators about threats caused through security policy violations. It retrieves and analyses information from many-sided areas to identify possible security breaches. IDS is primarily classified as

- Network based intrusion detection system
- Host based intrusion detection system.

Network intrusion detection monitors network based traffic and search suspicious activities. It compromises majorly in IP address, URLs, Domain names which may be authorized attack or unauthorized attack [21]. Whereas Host based intrusion detection is accomplished for monitoring and analyzing inside the computer as well as consolidated network [21].

Various mechanisms to secure our own network is, creating honeypot to attract, emulate, research over the strong analysis of hacker activities and a goal is shared to deter atacks [25]. suricata is an open source and free rule based intrusion detection system having the capability of real-time inline intrusion detection system which also includes the features like network security monitoring and offline pcap analysis [26]. Monitoring the Network using Wireshark.

4.2. Security information and event management (SIEM)

Security information and event management is a basic function for centralizing all the security information from various important devices like Firewall, Honeypot, intrusion detection and prevention systems, server. All of these generate thousands of alerts. By using this technology we can collect all the information at one place with one set of reports and one centralized system for generation notification and detect suspicious behaviour and problems before they become breaches [22].

4.3. Threat Management

Cyber threat management allows early detection of threats, precise decision making, analysis of data with respect to time and minimizing threat actions in real time scenario [23].

As the outbreak of threat data persists to whirl on, abundant damage turned up in major sectors like Government, Finance and IT. The quality and quantity of information being hacked, stolen, destroyed or leaked keeps expanding as time goes on. For instance, the data records unconcealed day to day anticipated to be 5,023,801. From this analysis, the frequency of cybercrimes experiencing every hour, minute, second could be 209325,3489,58 approximately [24]. In order to thwart these attacks we proposed cyber threat intelligence as solution.

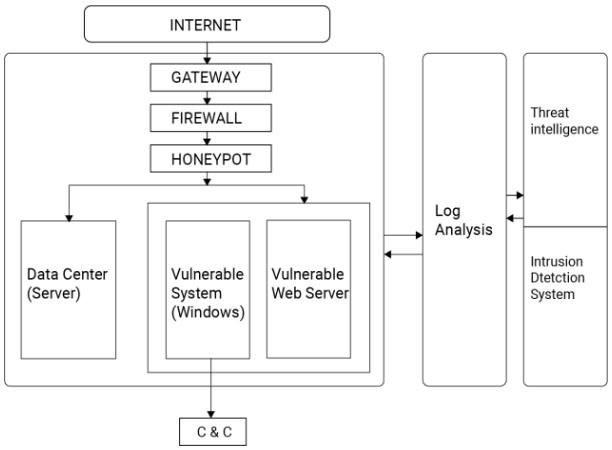

Fig.3: Proposed CTI architecture

Usually Threat actor, which internally connects to organization gateway and firewall through internet. There are certain threats which can even bypass the firewall; so in order to secure our infrastructure from such threats, a technology of honeypot is implemented, where the malicious traffic will be redirected to it. Honeypot will detects and emulates all the attacker motives, tactics and countermeasures for making use of system or device unauthorizedly.

In addition to this, we even implement a mechanism to detect the malicious or unauthorized entry using an effective Intrusion Detection System. The log correlation can be done by embedding

centralized logging structure. So that, the various logs from honeypot, IDS, Firewall will be analyzed using SIEM tool.
In parallel to this efficient detective system, packet sniffing will be carried out at the server end to identify any malicious backdoor arriving towards the victim machine or device. Based on the analysis of the identified malicious packet & malware signatures, the impact of existing & future possible threats can be defined which represents the concept of Threat Intelligence.
Based on the type of incident happened, the security rules can be updated for preventing such kind of threats in future which indicates an effective Intrusion Prevention Mechanism.
The concerned authority or admin will be alerted for the incident by the network security agent deployed at the server. The target machine or device can be isolated for performing various Digital Forensic approaches to identify the actual culprit behind the incident.

5. Implementation and performance analysis

The implementation of this architecture will secure the infrastructure not only from the external threats but also from the possible insider threats. we also deploy the IDS in the DMZ network.
The honeypot will detects and emulates all the attacker motives, tactics and countermeasures for making use of system or device unauthorizedly [25]. Even if honeypot got compromised with new unknown attacks, the footprint information regarding the attack will be stored.
Honeypot systems are mainly classified according to level of interaction they are Low interaction honeypot, Medium interaction honeypot, and High interaction honeypot. Low interaction honeypot is easy to install, configure, deploy and maintain. It serves up basic content and are not interactive when once breached. Normally these technologies emulate some important services like SSH, HTTP, or FTP. They are mainly used for demonstration and education [26]. KIPPO honeypot is the medium interaction honeypot that resembles real services and provides limited functionality when once breached. These are the most commonly used honeypots. In this article we explain how to install such a system using a KIPPO software [27]. Whereas High interaction honeypot imitates real systems or modifies real hosts to act as a honeypot in order to verbosely log attacker activity and capture all network and related flow data [26].
Depending up on implementation criteria we classify honeypots into the following categories

- Production honeypots
- Research honeypots

Production honeypots help in securing the environment by detecting attacks. Commercial honeypots often use production honeypots to mitigate the risk of attackers. Production honeypots are easy to deploy and gather less information about the attack or attackers due to lack of functionality .It also adds value to security measures of an organization. These are mainly used in production network which in turn improves overall security [25].
Research honeypots play major role in accumulating information about hacker tactics and motives. one can learn about how to protect in a better way from those attacks. Research honeypots are difficult to deploy and maintain. They are mainly used in research, military and government organizations. These honeypots do not add profits to organization [25].

5.1. Important aspects of implementation

In this session [27] Kippo is a medium interaction honeypot installed in Ubuntu virtual private server (VPS) in the cloud and setup to have SSH port open. Majority of Attackers will scan ip addresses and perform bruteforce attacks against KIPPO and we will change port 22 as 3389. By default kippo listens to port 2222 . so we also need to change this one to 22

5.1.1. Update and upgrade the Ubuntu cloud VPS

```
bharathi@ubuntu:~$ sudo apt-get update
[sudo] password for bharathi:
Reading package lists... Done
```

5.1.2. Editing the SSH configuration

First we have to install open SSH server & client and edit the SSH configuration file by using command nano /etc/ssh/sshd_config and we need to change the configuration

```
ubuntu@ubuntu: /etc/ssh
moduli  ssh_config
ubuntu@ubuntu:/etc/ssh$ nano /etc/ssh/ssh_config
ubuntu@ubuntu:/etc/ssh$ sudo apt install openssh-client
```

```
#   IdentityFile ~/.ssh/id_dsa
Port 445
#   Protocol 2,1
#   Cipher 3des
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3$
```

5.1.3. Installing KIPPO dependencies

Dependencies that we need to install python-dev, pyasn1, python-pip and apt-get install subversion.

5.1.4. Creating KIPPO user

```
ubuntu@ubuntu:/etc/ssh$ sudo adduser honeypot
Adding user `honeypot' ...
Adding new group `honeypot' (1001) ...
Adding new user `honeypot' (1001) with group `honeypot' ...
Creating home directory `/home/honeypot' ...
```

With the following command, create user in home directory and give sudo permissions to user.

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
kippo   ALL=(ALL:ALL)ALL
# See sudoers(5) for more information on "#include" directives:
```

5.1.5. Changing KIPPO server port 2222 as 3389 and create ip tables to redirect from port 22 to port 3389

```
# Port to listen for incoming SSH connections.
#
# (default: 2222)
ssh_port = 3389
```

```
[database_mysql]
host =honeypot@localhost
database = kippo
username = root
password = root
port = 3306
```

5.1.6. Download and configure KIPPO and move kippo.cfg.dist file to kippo.cfg

```
honeypot@ubuntu:/home/ubuntu$ sudo git clone https://github.com/desaster/kippo.g
it
Cloning into 'kippo'...
remote: Counting objects: 1544, done.
```

Create database kippo;

```
mysql> create database kippo;
Query OK, 1 row affected (0.09 sec)

mysql> GRANT ALL PRIVILLEGES ON kippo.* To 'kippo'@'localhost'
    -> IDENTIFIED BY 'root';
```

5.1.7. Starting KIPPO

Before starting KIPPO, we have to restart mysql and apache2 server and run the kippo by giving permissions to execute.

```
ubuntu@ubuntu:~/kippo$ ./start.sh
twistd (the Twisted daemon) 15.2.0
Copyright (c) 2001-2015 Twisted Matrix Laboratories.
See LICENSE for details.
Starting kippo in the background...
```

```
ubuntu@ubuntu:~/kippo$ sudo chmod -R 777/
[sudo] password for ubuntu:
chmod: missing operand after '777/'
Try 'chmod --help' for more information.
```

5.1.8. KIPPO logging capabilities

All the activities of the honeypot is logged and located in /kippo/log. From it we read and understand the timestamps, ip combinations of usernames and passwords that we have tried. By installing the kippo graphs we visualise statistics from KIPPO graph.

After detecting the attack, administrator will take the necessary precautions to isolate the compromised system or devices to make sure no other system will get compromised. The security rules in Firewall or IDS will be updated according to the type of attack.

Fig. 4: kippo Graph

5.2. Suricata

Suricata is an opensource and free rule based intrusion detection system, having the capability of real-time inline intrusion detection system which also includes the features like network security monitoring and offline pcap analysis [28] [30]. Though snort is common alternative tool for most of the admins, Suricata is the new and future enhanced tool which improves overall performance of network traffic analysis by using muti-threade feature [29].

For example when attacker enters with brute force or SQL injection and it is encountered then the attacker is transfered to the honeypot. Now in the honeypot, the request of the attacker is traced and the attackers ip is stored in the database of the honeypot. A script written in suricata on the webserver will add the new "alert or drop" rule to deny the access to coming on the webserver again.

```
alert tcp any any -> $HOME_NET $PORT_HTTP (msg: "SQL Injection Attempt - and
1=1"; content: "GET"; http_method; uricontent: "and 1=1"; nocase;
classtype:web-application-attack; sid:3000001; rev:1;)
```

Some suricata rules for which are utilized for detecting probe attacks

- **FTP attacks**

Attacker requests access to ports indirectly through victim machine by using the port command as a middle man for the request [34].

alert tcp $HOME_NET any -> any 20(msg :"social security number detected in plain text over FTP."; pcre:"/([0-6]\d\d|7[0-256]\d|73[0-3]|77[0-2])-\d{2}-\d{4}/";reference:url,en.wikipidea.org/wiki/File_Transfer_protocol; classtype:policy violation; sid:30000002; rev:1)

- **SMB (Server message Block) attack**

SMB is the transport protocol which is used by windows machines. It is used to deal with different types of motives such as file sharing, printer sharing and access through windows sharing services. It operates over tcp ports 139 and 445. the recent wannacry ransomware took advantage of this vulnerability [35].

alert tcp $EXTERNAL_NET any -> HOME_NET 445 (msg:"possible buffer overflow attempt over port 445"; content: | port 41|"; sid:30000003; rev:1;)

alert tcp $EXTERNAL_NET any -> $ HOME_NET any (msg:"possible microsoft shell connection detected."; flow:established; content:"copyright |28| c |29| 2009 Microsoft corporation"; sid:30000004; rev:2;)

- **Heart bleed Bug**

Heart bleed bug steals data protected under standard conditions by SSL/TLS encryption used to secured the internal based on the vulnerability in open SSL cryptograghic software library [36].

alert tcp $EXTERNAL_NET 443 -> $ HOME_NET any (msg:"plaintext HTTP headers user-Agent and Host detected over port 443 (response from server)."; flow:from server. Established; content:"user|2d|Agent"; content:" HOST |3a|; sid:30000005; rev:1;

Suricata is compatible with a range of third party Snort tools and the generated results would either be in the formats of YAML or JSON. Upon integrating the resulted outcomes with log analyzer tools like SIEMs, Splunk, Logstash/Elasticsearch, Kibana would help one to analyse the attack on vast sets of compatible databases.

```
bharathi@bharathi-VirtualBox:/var/log/suricata$ sudo tail -f suricata.log
[sudo] password for bharathi:
24/1/2018 -- 09:59:51 - <Info> - Threshold config parsed: 0 rule(s) found
24/1/2018 -- 09:59:52 - <Info> - 17845 signatures processed. 1136 are IP-only ru
les, 6036 are inspecting packet payload, 12700 inspect application layer, 103 ar
e decoder event only
24/1/2018 -- 09:59:54 - <Info> - fast output device (regular) initialized: fast.
log
24/1/2018 -- 09:59:54 - <Info> - eve-log output device (regular) initialized: ev
e.json
24/1/2018 -- 09:59:54 - <Info> - stats output device (regular) initialized: stat
s.log
24/1/2018 -- 09:59:54 - <Info> - Going to use 1 thread(s)
24/1/2018 -- 09:59:54 - <Info> - Running in live mode, activating unix socket
24/1/2018 -- 09:59:54 - <Info> - Using unix socket file '/var/run/suricata/suric
ata-command.socket'
24/1/2018 -- 09:59:54 - <Notice> - all 1 packet processing threads, 4 management
 threads initialized, engine started.
24/1/2018 -- 09:59:54 - <Info> - All AFP capture threads are running.
```

Fig. 5: Suricata log file

5.3. Hostbased intrusion detection system

Host based intrusion detection is accomplished for monitoring and analyzing inside the computer as well as consolidated network [21]. To secure your host based computer along with your network, probably it is better to go with commercial honeypot. Otherwise samhain is the best tool with respect to open source. Apparently, It also provides the centralized client-server host monitoring system as well. It Mainly checks file integrity verification, log file monitoring, login/logout monitoring, Hidden process detection and open port detection.in the worst scenario there is also a chance to choose THUG honeypot or Web Defender, a browser based plug-in to be added which majorly defends against visiting malicious sites [32].

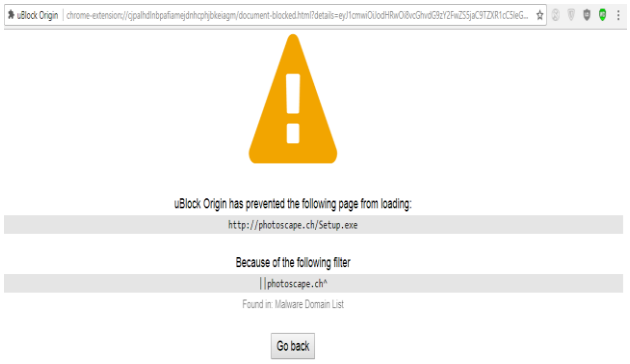

Fig. 6: Web defender

5.4. SIEM Technology

Security information and event management is a basic function for centralizing all the security information from various important devices like Firewall, Honeypot, intrusion detection and prevention systems, server. All of these generate thousands of alerts. By using this technology we can collect all the information at one place with one set of reports and one centralized system for generation notification and detect suspicious behaviour and problems before they become breaches [22]. The most significant and useful tool for log co-relation is SPLUNK. It produces effective search, monitoring, and analysis to eliminate blind spots [33].

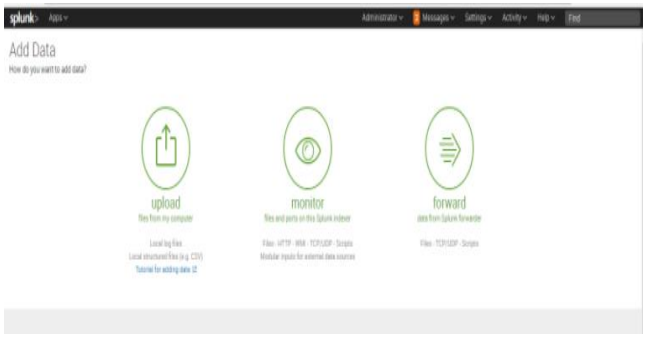

Fig. 7: Getting started with splunk

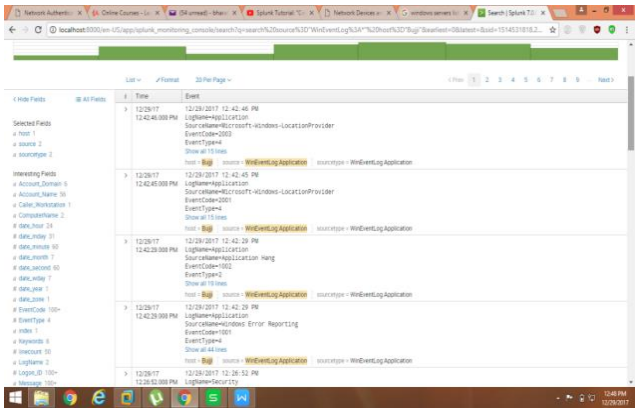

Fig. 8: Splunk Real-Time Output

Cyber Threat intelligence plays a major role to prevent and secure our environment from catastrophic attacks. For thwarting those attacks we must understand the organization's infrastructure security standards and it adversaries. By using it we can identify the attacker and attack risk to the particular threat by gathering attacker previous experiences. So that it is possible to detect and respond for efficient threat management in real time.

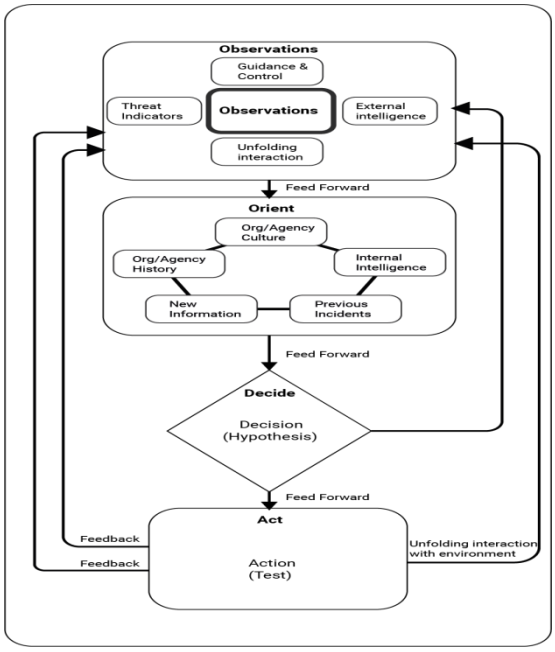

Fig. 9: Cyber Hazard Management (CHM)

The organizations observe External Intelligence, threat indicators, important devices logs to identify malicious actors, unfolding interaction with environment in-order to improve overall cyber security posture. The only difference between known attacks and unknown attacks is time. The time-delay of information on more worldly-wise attacks is comparatively long. Because of Advanced Persistent Threats (APT's) of this method is becoming limited as they possess a high-risk profile range and are hardly ever known. So Expert threat analysts will orient organization's history, culture, previous indicators, new information and internal intelligence. This enables to identify, investigate and thwart attacks in real time. Taking all this information into consideration, a decision has to be made to act accordingly to the incident [23] . CTMF is like a blueprint to organize cyber threats in a sophisticated manner. The major benefits are early detection of threats, instant recognization, and faster decision according to the incident or damage[37-40].

6. Conclusion and future Enhancement

The proposed CHM framework solution will secure the organization's infrastructure from insider and outsider threats, while Honeypot detects and emulates the attacks, Intrusion Detection System monitors network traffic and provides real time detection and prevention of intrusions, the centralized log correlation will make the administrator or incident responder to enact quickly for the damage caused. Whereas, Cyber threat intelligence detects and prevents catastrophic attacks based on context and manages the threat efficiently by responding in time. So we can improve the security level from such catastrophic attacks.

My future enhancement is to collaborate artificial neural networks with the existing technology, where a machine learning language derived from mimic of human brain for reducing false positives and improves the accuracy of intrusion detection.

REFERENCES

[1].http://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf
[2].http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/
[3]/https://www.netskope.com/blog/september-2016-cloud-report-43-7-percent-cloud-malware-ransomware-delivery-vehicles/
[4].https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do
[5].https://www.symantec.com/about/newsroom/press-releases/2017/symantec_0426_01
[6].https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/
[7].https://ebrary.net/26640/computer_science/security_threats
[8].http://searchsecurity.techtarget.com/definition/zero-day-vulnerability
[9].http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT
[10].https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/
[11].https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767
[12].https://www.cisecurity.org/what-is-cyber-threat-intelligence/
[13].http://www.securityweek.com/ciso-perspective-how-tactical-cyber-threat-intelligence-fits-your-security-program-
[14].https://www.csoonline.com/article/3203804/security/know-your-enemy-understanding-threat-actors.html
[15].https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html
[16].https://arxiv.org/ftp/arxiv/papers/1712/1712.00841.pdf
[17].http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.464.2990&rep=rep1&type=pdf
[18].https://www.researchgate.net/publication/299666817_Detecting_and_Preventing_Data_Exfiltration_Executive_Summary
[19].https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2
[20].https://en.wikipedia.org/wiki/Intrusion_detection_system
[21].https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
[22].https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/what-is-a-siem/
[23].https://www.ioctm.org/What-is-Cyber-Threat-Management
[24].http://breachlevelindex.com/
[25].http://www.it-docs.net/ddata/792.pdf
[26].http://www.omnisecu.com/security/infrastructure-and-email-security/low-interaction-honeypots-and-high-interaction-honeypots.php
[27].https://www.digitalocean.com/community/tutorials/how-to-install-kippo-an-ssh-honeypot-on-an-ubuntu-cloud-server
[28].https://suricata-ids.org/
[29].https://www.aldeid.com/wiki/Suricata-vs-snort
[30].https://media.readthedocs.org/pdf/suricata/latest/suricata.pdf
[31].https://webtechdevx.qualcomm.com/swe/docs/articles/en/web-defender.html
[32].https://webtechdevx.qualcomm.com/swe/docs/articles/en/web-defender.html
[33].https://www.splunk.com/
[34].https://en.wikipedia.org/wiki/FTP_bounce_attack
[35].https://en.wikipedia.org/wiki/SMBRelay
[36].https://en.wikipedia.org/wiki/Heartbleed
[37] Vudatha, C.P., Nalliboena, S., Jammalamadaka, S.K.R., Duvvuri, B.K.K., Reddy, L.S.S., Automated generation of test cases from output domain of an embedded system using Genetic algorithms, ICECT 2011 - 2011 3rd International Conference on Electronics Computer Technology
5,5941989, pp. 216-220
[38] Sastry, J.K.R., Ganesh, J.V., Bhanu, J.S., I2C based networking for implementing heterogeneous microcontroller based distributed embedded systems, Indian Journal of Science and Technology, Volume 8, Issue 15, 2015
[39] Sastry, J.K.R., Naga Sai Tejasvi, T., Aparna, J., Dynamic scheduling of message flow within a distributed embedded system connected through a RS485 network, ARPN Journal of Engineering and Applied Sciences, Volume 12, Issue 9, 1 May 2017, Pages 2809-2817
[40] Sastry, J.K.R., Suresh, A., Bhanu, S.J., Building heterogeneous distributed embedded systems through rs485 communication protocol, ARPN Journal of Engineering and Applied Sciences, 2015, 10(16), pp. 6793-6803