International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 11; Issue: 4; April -2022

Threat Intelligence Framework in Cyber Security

Madhavi Basant, MTech Student, Information Science and Engineering, New Horizon College of Engineering, Bangalore, Karnataka, India
madhavibasant05@gmail.com

Dr. P. Mangayarkarasi , Associate Proffesor, Information Science and Engineering, New Horizon College of Engineering, Bangalore, Karnataka, India
mangaivelu18@gmail.com

ABSTRACT

Threat intelligence is a set of information, which is used by organizations to understand the threats that makes the company vulnerable. These are the data, which are used to identify cyber threats in a company. In an environment where any number of cyber-attacks could harm enterprises to its core, there is no limit of danger these hackers can do to a company. Threat intelligence can gain valuable information about these cyber-attacks, build strategic defense mechanisms and reduce risks that could damage their resources and reputation.

Keywords: Cyber-Attack, Data Privacy, Information Security, Threat Intelligence

I. INTRODUCTION

Threat Hunting is a type of Security Testing designed to identify vulnerabilities, pitfalls and pitfalls that bushwhacker might exploit in software, a network, or a web operation. Threat Hunting examines all possible sins in a software operation to identify and fix them. Pen tests are also known as Threat Hunting. Any system or any data contained within it may be vulnerable to attack by bushwhacker who can disrupt the system or gain access to its data. During software development and performance, vulnerabilities are constantly introduced by accident. These comprise design crimes, configuration crimes, and bugs in software. Vulnerability Assessment and Threat Hunting these are two mechanisms used in Penetration Analysis.

Threat Intelligence is important because threats can get past automated cyber security testing. Although automated cyber security tools and operations center analysts should be able to manage with roughly 85% of cyber threats, although need to worry about the remaining 15%. The remaining 15% of cyber threats are more likely to include cyber threats that can cause damage. They will break into any network/device and avoid detection/highlighted for up to 288 days on an average. Threat hunting helps to mitigate damage done by attackers.

Hackers often eavesdrop for weeks or months, before getting discovered. They wait patiently in hidden mode to steal data and confidential information to unlock device for further access, to perform data breach in the user device. According to the "Total Cost of a Data Breach in the device Report 2021," a data breach costs a organization almost USD 4.1 million on an average. Also the negative effects of a data breach can affect for long terms. The more the duration between system failure and response is deployed, the more it will damage the company financial status of a company.

An efficient threat intelligence framework is based on an organization's environment. Companies must have an enterprise security framework in order for collecting data or resource. The data gathered from it provides valuable information for threat intelligence hunters. Cyber threat intelligence hunters bring a human element to enterprise security framework, which is beneficial for complementing automated device or systems. They are skilled information technology

security professionals who perform many operations such as search, log, and monitor and neutralize threats before they can cause serious problems to the company. They are security threat analysts from within a organization's Information Technology department who knows its operations very well.

The framework of cyber threat intelligence hunting finds the environment is unknown. It uses threat intelligence detection techniques, such as endpoint detection and response (EDR) etc. Threat intelligence hunters goes through security data of the resource or device. They search for hidden malware or threats and look for patterns or sequence of suspicious/irregular activity that a system might have missed. They also help patch an organization's security system to prevent that type of cyber threat attack from recurring in future.

Fig 1.1: Threat Intelligence

Threat hunters begin with a systematic hypothesis based on security data or graphs. The trigger serve as base for a investigation into system/resource risks. And these systematic investigations are of three types: structured, unstructured and situational hunting.

Structured hunting

A structured hunt is based on an indicator of threat/attack. Also the techniques of a threat attacker. Threat hunters are aligned and based on the TTPs of the threat hunters. Therefore, the threat hunter can usually identify a threat actor even before the hacker can cause harm to the system. This type of hunting uses the MITRE framework - Adversary Tactics Techniques and Common Knowledge (ATT&CK) framework.

Unstructured hunting

In this type of hunting, hunt is initiated based on a trigger. This type trigger alarms a hunter to look for pre and post detection incidents. Guiding their approach, the threat intelligence hunter can research the data retention, and previously associated offenses present in the system.

Situational or entity driven

It comes from company's internal risk assessment data and threat vulnerabilities analysis. A threat hunter can search for the specific behaviors within the environment of the company.

Threat intelligence system is a data set about successful intrusions detection system, usually analyzed and reported by automated security framework systems with machine learning and AI technology. Threat hunting framework uses this intelligence report to carry out a thorough search for bad users. Threat hunting begins where threat intelligence ends in the organization's environment. A successful threat hunt can identify threats that have not yet been identified in the organization.

Threat intelligence hunting framework uses threat indicators as a hypothesis for a hunt in the system. These threat indicators are virtual fingerprints left by an hacker such as an unidentified IP address and phishing emails etc

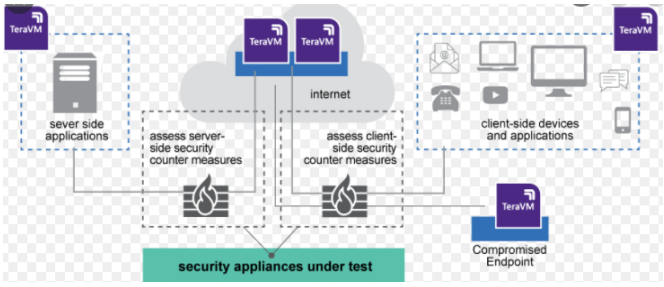

Fig 1.2: Workflow of Threat Intelligence

II. Literature Survey

The literature review of this paper begins with the status of threat intelligence in Canada and the US government, followed by a review of the rewards and risks of cyber attacks. It identifies risk management strategies through negotiation of key contract terms and SLAs[4]. The main goal of the research was to identify

major contract terms needed to mitigate risks as organizations move to better threat hunting tools.

The threat hunting framework provides key terms to organizations, a checklist of threat hunting tools services policy to add in the contract in order to protect their interests from a business and legal contracting point of view. This paper also includes key points important for negotiation of threat intelligence services contracts, which included governance, project management and vendor performance management. [7]

Threat Risks can be mitigate during many stages from selection of the threat hunting tool, pre signing of the policy and post signing of the contract. Below are the mentioned stages for risk management mitigation :
Due Diligence Stage

Company can use the internal detection system as main source to gather information to provide higher visibility into their environment. It will lead to a better definition of system data. While pulling information from a other sourced platform as an option to give a better view of the overall cyber threat.

Threat Intelligence framework can add up company effort to develop requirements that support project operation in planning and mitigate threat to the system [9]. Hence, we can say that there are 3 category of threat intelligence framework source which are internal, external and community.

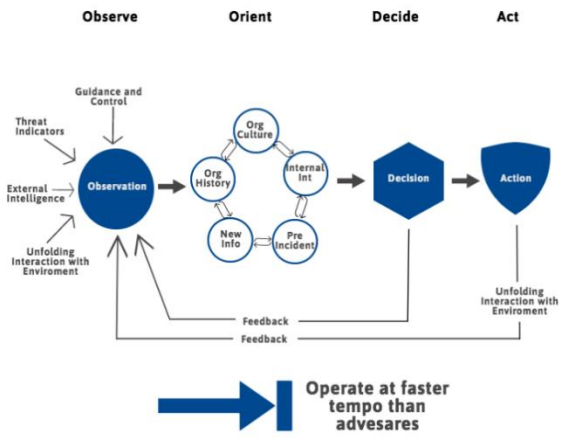

Figure 2.1: Process of Threat Intelligence system

Situational Awareness Driven

In this threat hunting tool the pattern of a company can be calculated using assessments of threat, which indicates how much threat they are running in the system. AI Engine, YETI are some of the examples of situational awareness driven tool that has driven threat hunting tools framework.

Artificial Intelligence Engine or AIEngine:

In this threat hunting tool the system's intrusion detection system can be modernized using Artificial Intelligence Engine or AIEngine. User interaction is not necessary for its learning and forensics of the system; detecting threats can be done using the same.

YETI:

In this threat hunting tool user share the details all over the company. Organization acquire the information from partners whom they trust and share the information to tell everyone regarding the latest threats. These threat-hunting tools are not available for free.

III. Proposed Methodology

The threat intelligence framework is very important. It includes a wide range of systems information, tools, standards, formats and platforms. These tools perform calculation which is necessary to define a strategy of intrusion detection system. User should focus on open source standards and platforms. A literature review was conducted targeting to obtain a complete overview of the threat intelligence framework tool. Some internet search engines were used for this task. The below mentioned policies were added to find accurate results:

Threat Intelligence framework or Cyber Threat Intelligence. The searching mechanism shows a large number of information. Some of them were shortlisted based on their relevance to the data and number of occurance. For the shortlisting mechanism added to the searching process, initiatives of threat intelligence framework tools were collected. To mitigate the number of information found, based on search results of the internet were excluded and not considered for the selection process.

Types of Threat Hunting Tools

Analytics-Driven
This threat-hunting tool create hypotheses by using behavior analytics and machine learning technology of the system. Maltego CE, Cuckoo Sandbox, automater

are some of the examples of analytical driven threat hunting tool.

Maltego CE:
In this threat hunting tool link analysis is created by using interactive graphs rendered using Maltego CE, a data mining tool for the system. This tool is used for online investigations for the system. The relationships between data and resource is found to be a threat, then an alert is raised.

Cuckoo Sandbox:
In this threat hunting tool disposal of suspicious files results can be done using a cuckoo sandbox tool, It is an open-source malware analysis tool. The cuckoo sandbox tool provides the information on the operation of malicious files to understand them and stop them too.

Automater:
In this threat framework, automated tools provide hunting tool the data on an intrusion detection system. User can choose the target, and results are reviewed by the automated intrusion detection system from sources that are popular.

Intelligence Driven
In this threat hunting tool all the data and resources are pulled together and it is applied to threat intelligence hunting tool by using intelligence driven threat hunting tools framework. The examples of intelligence-driven threat hunting tools are YARA, CrowdFMS, Botscout, and Machine.

YARA: In this threat hunting tool malware are classified using a multi-platform tool called YARA. The details of malware belonging to the same category based on patterns are created by YARA. The Boolean expression creates the description of the resource , and the expressions determines the identity of the resource.

CrowdFMS:
In this threat-hunting tool collection and processing of resource from internet that displays the phishing emails details are done by an automated application called crowdFMS. An alert will be raised if a match to a phishing mail crosses the network in the system.

Botscout:
In this threat hunting tool spams, server abuse, database pollution are caused by bots. It can be prevented by not allowing these bots to register on forums using botscout. Details of IP address, email can be tracked, and elimination of these bots can be done by identifying the source in the network.

Machinae:
In this threat hunting tool the intelligence is compiled from the internet and rely on data related to security. Machinae is a free software. It has good compatibility when compared to other security intelligence software. It has a well-optimized configuration. It is user friendly.

IV. CONCLUSION

Threat Intelligence framework can be based on the basis of its effectiveness on a mitigating threat. Selecting best threat Intelligence system is very important. The need for research and development is required to reduce the drawback of Threat Intelligence framework tool. This paper examines available literature that discuss the existing information of Threat Intelligence framework and the current state of development. We also identify many challenges for information quality and threat intelligence framework tool sharing platform. It is not a new for data quality but with the growing adoption of Threat Intelligence framework tool, it is important to look at this as future research.Company can apply threat intelligence framework toll for sharing platform to manage a large volume of threat information. They should hire a qualified threat intelligence analyst to analyze the threat information to mitigate damage. There is an initiative between community member to analyze the threat information and assure that threat information which is shared have true data. MITRE threat intelligence framework is in developing standards format for threat intelligence tool sharing to handle interoperability issue between threat sharing company.

REFERENCES

[1] Kurt Baker, " https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/" March 2022
[2] Micheal Cobb, " https://whatis.techtarget.com/definition/threat-intelligence-cyber-threat-intelligence" February

2018

[3] Giuseppe Cascavilla "https://www.sciencedirect.com/science/article/pii/S0167404821000821" June 2021

[4] Benjamin Turnbull, " https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8374422" April 2018

[5] Dniel Schlette," https://link.springer.com/article/10.1007/s10207-020-00490-y" March 2020

[6] Shikha Gupta," https://www.diva-portal.org/smash/get/diva2:1568547/FULLTEXT03 ", August 2021

[7] Shivangi Gupta " https://www.ijrte.org/wp-content/uploads/papers/v8i3/C5675098319.pdf ", September 2019

[8] Dr. Aswami Affrin " https://www.researchgate.net/publication/322939485_Cyber_Threat_Intelligence_-_Issue_and_Challenges", April 2018

[9] "https://www.digitalshadows.com/blog-and-research/threat-intelligence-a-deep-dive/ "December 2019

[10] "https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf " March 2019