IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER THREAT INTELLIGENCE

Unnimaya V S, Jasmine Jose

MSc Scholar, Assistant Professor
Department of computer science,
St. Joseph's college (Autonomous), Irinjalakuda, Thrissur, India

Abstract: Threat intelligence is an information used by many organizations to discover the threats that are faced by the organizations. The threat intelligence is helpful to identify, prevent the cyber threats. It also explains how and why the attackers may be attacking the organizations and how to respond to the attacks that are faced by the organizations. Cyber Threat Intelligence (CTI) is an information about threat and threat actors and is helps in reducing the vulnerabilities in cyber space. The cyber threat intelligence provides value for other experts such as security officers, accountants, and terrorism and criminal analysts**.**

Index Terms **- CTI, Levels of CTI, Intelligence Cycle, and CTI use cases.**

I. INTRODUCTION

Cyber Threat Intelligence (CTI) has become a hot topic and being under consideration for many organizations to counter the risk of cyber-attacks. The CTI is an advanced process that enables the cyber defenders to explore their threat intelligence capabilities and helps to understand their present position against the ever changing cyber threat landscapes.
The CTI can make a significant difference to the organizations ability to discover the attacks before they occur and it will helps in providing a variety of mechanisms to respond quickly against the threats. It also provides the defense mechanisms during the attacks.

The CTI provides more proactive approaches**.**

II. LEVELS OF CYBER THREAT INTELLIGENCE

There are three different levels in cyber threat intelligence and they play an important role in each and every steps of CTI. Operational, Tactical and Strategic are the three levels of CTI.

Operational: It is an information and a trend analysis that enables the defender to understand the direction in which the attacker's capabilities are evolving.

Tactical: It is an analysis which is based upon known actors or network behavioral patterns and is a host based security system alerts.

Strategic: It is an analysis and exists to inform senior decision makers of broader changes in the threat landscape.

CTI combines both the strategic and tactical intelligence for the better performance. The strategic intelligence helps to understand and prepare for threats (principle I &II). The tactical intelligence enables to respond against to dynamic threat situations (principle III).

III. PURPOSES OF CTI

- Preventive functions such as Security Operations Center (SOC) support, alerting and triage.
  - Triaging alerts.
  - Providing information to vulnerability and risk management.
- Response functions such as Incident Response Support
  - Facilitating information sharing.
- Strategic Support Function
  - Supporting business decisions.
  - Informing resource prioritization.

The CTI helps to reduce harm by improving decision making before, during, and after cyber threats. The CTI provides answers to questions such as who are the attackers, what adversaries use including their capabilities, where the adversaries target, when they act, why they are attack including their motives and intent and how they operate.

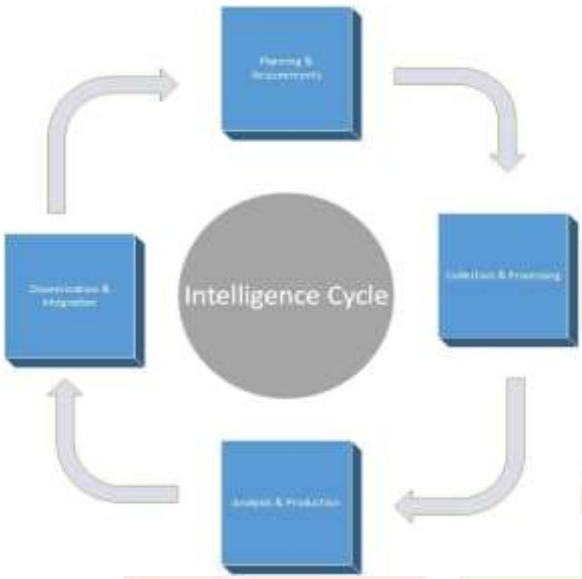
.

IV. THREE PRINCIPLES OF CTI

Principle 1: Threat understanding.
Principle 2: Preparing.
Principle 3: Responding against the threats.

V. THE INTELLIGENCE CYCLE

The intelligence development can be represented as a cyclic process which is used to reduce the risk and uncertainty.



It is a four step continuous process and is conducted by the Intelligence team. The intelligence team required feedback and evaluation from the management.

VI. BENEFITS OF CTI

Benefits of threat intelligence include improved efficiency and effectiveness in security in terms of detective and preventive capabilities

- Immediately understand the threats faced by the organizations.
- Access to information on new and emerging threats and threat actors.
- Identifying and preventing security breaches.
- Minimization of fraud and theft.
- Improve the efficiency of the security team.
- Lowers the risks.
- Monitors the online communication.

VII. CYBER THREAT INTELLIGENCE USE CASES

CTI use cases helps organizations to prevent an attack, and also a useful part of risk analysis, vulnerability management and wide scope decision making.

- **Vulnerability Prioritization**

  It is used for evaluating vulnerabilities. It discovers the problem and fix them. Many organizations give priority to new threats instead of focusing on improving their fundamentals. It makes clear that any organization's top priority should be the already known vulnerabilities rather than the worrying about new threats.

- **Brand Monitoring**
  It is important to choose a threat intelligence solution that will monitor open sources as social media channels. Identifying threats in this area requires an awareness of the organization's brand and many ways a threat actor may seek to exploit it. Attacks that can be identified through social media and brand monitoring include phishing, domain fraud or trolling attacks.
- **Fraud Detection**
  Threat intelligence gives an advanced awareness of who is stealing data, how they are doing it, what motivate them and whether our organization has been exposed.
- **Threat Intelligence Analyst Augmentation**
  Augmentation intelligence mitigates the shortage of skilled security analysts by increasing their effectiveness.
- **Dark Web Monitoring**
  The dark web (also called darknet) is often associated with images of midnight hackers and secretive villain working in solitude. This area of internet is both used by the illicit people and good people. The darknet/dark web deals with many activities including illegal goods sales, human exploitation and discussion around illegal topics happens there. The threat intelligence in dark web allows organizations to detect and prevent threats of all kinds. By monitoring the dark web with threat intelligence can help you to boost the security and identifies breaches, threats and vulnerabilities.

VIII. ACKNOWLEDGEMENT

I would like to take this opportunity to acknowledge the contribution of certain people without which it would not have been possible to complete this paper work. I am thankful to the Principal Dr. Sr. Lissy Anto P, Head of the Department Sr. Siji P D, Guide and Coordinators for their support, encouragement and suggestions. I would like to express my special appreciation and thanks to my guide MS. Jasmine Jose, you have been a tremendous mentor for me.

IX. CONCLUSION

Cyber Threat Intelligence is not a concept. It is a method of improving security of different organizations such as banking systems and other payment service markets. CTI is an ecosystem which supports the decision making process ensuring from the various stages of intelligence cycle of threats and vulnerabilities to an organizations and its individual assets. CTI services including security operations, monitoring and reporting cyber threats. A Cyber Threat Intelligence capability provides actionable intelligence that allows security managers to priorities the security measures according to the prevalent threats.

REFERENCES

[1] https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/

[2] https://www.forcepoint.com/cyber-edu/threat-intelligence

[3] https://www.crowdstrike.com/epp-101/threat-intelligence/

[4] https://www.recordedfuture.com/threat-intelligence/

[5]https://securitytrails.com/blog/cyber-threat-intelligence

[6]https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

[7]https://www.ey.com/Publication/vwLUAssets/EY-how-do-you-find-the-criminal-before-they-commit-the- cybercrime/$FILE/EY-how-do-you-find-the-criminal-before-they-commit-the-cybercrime.pdf

[8]https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1492186050.pdf

[9]https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-jun2019.pdf