Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 3950-3956*

Research Article

A Theoretical review on the importance of Threat Intelligence Sharing & The challenges intricated

Sandhya Sukhabogi[a], Dr. M. Anusha[b]

[a] Research Scholor,Department of CSE,Koneru Lakshmaiah Education Foundation,Vaddeswarm,Guntur District, A.P., INDIA
[b]Associate Professor,Department of CSE,Koneru Lakshmaiah Education Foundation, Vaddeswarm, Guntur District, A.P., INDIA
Email: [a]gnitss.sandhya@gmail.com,[b]anushaaa9@kluniversity.in

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: Cyber Threat Intelligence (CTI) is the emerging strategy of cyber defense which helps organizations to combat the latest and more sophisticated cyber threats. Gathering this threat information, analyzing and communicating it between the security teams is very difficult and challenging because of the heterogeneous aspects involved. The necessity of sharing the intelligence related data collected by organizations is increasing day by day to counter the ever changing and highly dynamic threat landscape. In this paper an attempt is made to understand CTI concept and how it is collected and analyzed to form useful actionable intelligence are observed. The importance of Threat intelligence sharing, and various standards working in the area of TIS are also mentioned. Finally the primary challenges in TIS are given a light in a broad view

Keywords: CTI, Threat Intelligence, CTI, CTI Sharing, Challenges of TIS.

1. Introduction

The defense systems which are used by most organizations are built for previous generation attacks and works mostly on signature based pattern matching techniques for detection and prevention. But today's attacks are well-organized, focused, targeted and keep changing their nature in-order to be undetected by traditional security measures. With the growing complexity of networks, zero-day exploit markets, vulnerabilities in the systems, outdated security policies many organizations are becoming the targets for the novel attacks. Hence there is a need for a system which works in collecting the almost real-time information about latest threats and attacks, generates intelligence from the Information collected, and which can be used by the organizations for making decisions. Such techniques are called Threat Intelligence. The primary objective of threat intelligence would be to shorten the time gap between a compromise and its detection.

1.1 Cyber Threat Intelligence:

Threat Intelligence is the information that can aid the organizations in taking decisions, with the aim of either preventing an attack or decreasing the time taken to detect the attack if it happens. Although existing from CTI lacks a standard definition and there are many different versions of defining CTI by different sources. Before defining CTI the general concept of Intelligence and the areas in which it plays a major role should be understood.

According to [11] there are 6 areas of intelligence like

- Military Intelligence
- Nation-State Intelligence
- Business Intelligence
- Threat Intelligence
- Psychological Intelligence
- Artificial Intelligence

These 6 areas can be further classified in to 2 domains as psychological and Artificial intelligence based on their areas of focuses.

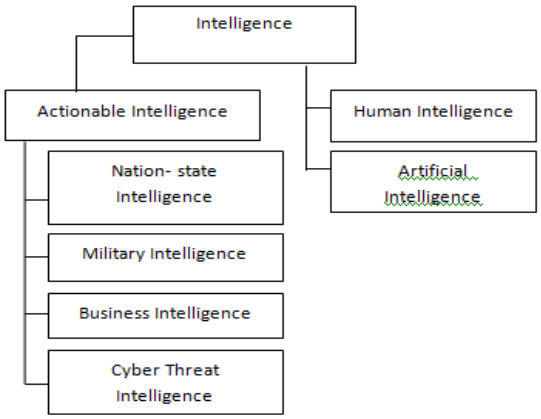

Figure 1: Types of Intelligence

According to GartnerCyber Threat Intelligence (CTI) can be defined as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging threat that can be used to inform decisions regarding the subject's response to that menace or hazard [3] .

Hence it has become crucial for all organizations to be aware of the current threats to be handled by them and make every effort to be protected by implementing or integrating the Threat intelligence strategies.

The intelligence collected should posses the following key principles without which the intelligence becomes useless. The actionable intelligence should be Centralized, responsive, Systematic, Timely, accessible to the intended audience. They should also be continuously reviewed and be shared while protecting the sources when ever it is required.

According to Chismon and Ruks [4], CTI objects can be categorized as 4 types based on their features and consumer role in the organization.

- Strategic Threat Intelligence
- Operational Threat Intelligence
- Tactical Threat Intelligence
- Technical Threat Intelligence

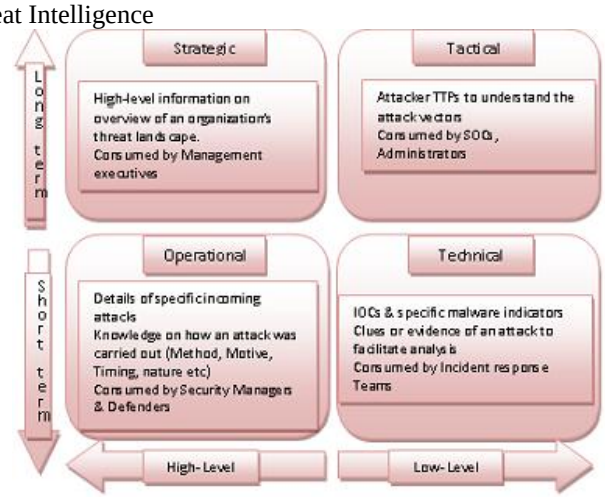

Figure 2: Types of Threat Intelligence

Strategic intelligence is high-level information that is consumed by management personnel to understand the attack trends and the threats that may have impact on the high-level Business decisions. Operational TI information provides the information about specialized, technically-focused, intelligence (mostly from campaigns, malware, forensic reports and/or tools) of the specific security incident of the organization, and it is consumed by the security managers and of the organization; Tactical TI deals with the Tactics, Techniques and Procedures (TTPs) used by various threat actors, IOCs (Indicators of Compromise) for defending signature based compromises. It is consumed by the incident response teams; and Technical Threat Intelligence is the consumed through information feeds, often consumed automatically by enforcement systems or monitoring and analysis systems such as firewalls, Mail filters etc.

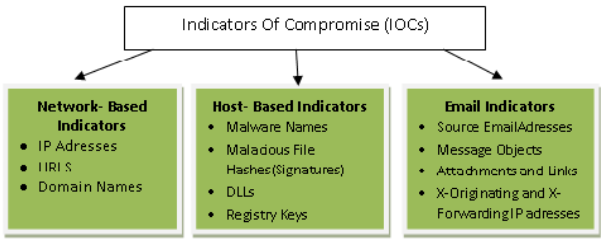

Figure 3: Common Indicators of Compromise (IOCs)

IOCs are the crucial artifact of CTI. They provide the details of the forensic artifacts of the attack and thus they can be used to analyze the attack, after it occurs, or it can defend the attack during its execution itself depending on the circumstances. According to [10] IOCs themselves are not intelligence, but they aid in producing the intelligence. An IOC comprises of evidence of individual data fingerprints involved in a specific attack, such as event logs, an attack domain, the hash of the malware delivered, etc., along with the context of the attack. They also provide valuable information about the analysis of the adversary's behavior, like the type of the attack or the specific technique deployed, which can be used to be prepared for the similar future attacks. To find out such information, CTI gathering process includes identification of the adversary's TTPs (Tools, Techniques and Procedures), along with the evidences , which helps the security team in understanding their position in ensuring security , detect early signs of threats and continuously improve their security controls. **[10]**

1.2 Sources of Threat Intelligence:

Intelligence can be collected from various heterogeneous sources in order to be effective. Hence it can be useful to identify subtypes of threat intelligence based on who consumes the intelligence and what it aims to achieve.

The sources of CTI can be closed, e.g., a corporation's internal logs, firewalls, network traces, or collected from wide range of public sources available from web, technical blogs or online forums, to the markets of the dark web. Threat Intelligence Feeds (TIF) forms the basic component of CTI frame work, which will have large amounts of data related to threats, attacks and incidents. With the increased number of cyber attacks which are becoming complex in recent years, a large number of IOCs and attack artifacts are coming out everyday. These will be collected by different organizations, and mostly reported through the public online sources **[8]**

Wide range of different sources in order to provide the proactive knowledge about the threats that have impact on them. Some of the commonly used sources are

- Open-source feeds
- In-House Threat Intelligence
- Intelligence- Sharing Communities
- Commercial threat Intelligence and security vendors
- Web Intelligence (Deep & Dark webs)
- Social media and messaging platforms

Collecting the intelligence alone does not make it actionable, It is just the huge amounts of data. Actionable intelligence is generated out of the knowledge gained based on evidence of the mechanisms followed, IOCs collected , implications in the organization, and the context related to threats or incidents in the cyber domain. It provides knowledge about adversaries and methods that can assist defenders in the decision making process of responding to threats

2. Threat Intelligence Sharing (Tis) And Its Importance

The need for this Threat intelligence sharing is increased with the increased number, complexity and the nature of today's cyber attacks. Without collaborating with other peers it is highly difficult for the individual organizations to detect those sophisticated threats and attacks. This is the reason most organizations recently showing interest in sharing their available information about incidents, attacks, threat vectors.

The information related to latest attacks, incidents and new malwares is available in many forms such as Threat feeds, forums, knowledge bases, and reports on the web. But this information is huge, generic and lacks specific details useful for the organization. For using this information effectively as threat intelligence there should be proper mechanisms that are capable of collecting, analyzing and evaluating the threat data. New automated systems with the ability to consume a vast amount of data, provide sophisticated defense capabilities and respond to various security incidents in real-time are evolving and commonly referred to as Threat Intelligence (TI) platforms.

Tools and data feeds that are available in the market cannot by them-selves provide threat intelligence from the data without human intervention. Intelligence of any type requires analysis. Majority of the analysis is

performed by the humans in the security field. Automation and usage of tools and analytics in the process of analysis of TI collected can increase the effectiveness of the analysis process.

Considering CTI to be a security measure from which even the smallest companies can benefit from, the threat feeds provided by the vendors has to be converted into intelligence by the security analysts of the organization or by a third party to make them suitable and specific for the organization.

Currently many organizations are collecting and analyzing threat related information individually. There is a little or no cross-organizational information exchange on TI. But the concept of TIS (Threat Intelligence Sharing) is very important for effective and efficient Threat detection and response. Sharing the CTI objects between different organizational entities is the effort to improve the organization's cyber defense posture by leveraging the capabilities, knowledge, and experience of the broader community. Some of the advantages of TIS is

- It improves the understanding of information about the actual and potential threats
- More efficient usage of the IT resources of an organization
- Reduces the IT security costs of the individual organizations

According to Gong [1] "A more efficient cyber defense strategy against current and future threats requires early detection, prevention, and collaborative Cyber Threat Intelligence (CTI) sharing."

In recent times many organizations are getting motivated for threat intelligence exchange by understanding the need for collaboration. Many national and international organizations are encouraging the threat information/intelligence sharing by supporting cooperation and coordination aspects between threat defenders. Some organizations focus on vulnerabilities and incident response, Others focus on identifying intrusions and potential threats. When all these are combined together, they provide the current stature of the security to the members of the community.

3. Threat Intelligence Sharing Platforms (Tisps) / Standards

Threat Intelligence sharing platforms are inter-organizational systems that enable companies and public authorities to collaboratively collect, aggregate, analyze and share threat-related information [8]. TISPs have become a useful tool helping organizations to share TI more effectively.

Several efforts are made to facilitate threat information sharing in a standardized manner. TLP(Traffic Light Protocol), IODEF (Incident Object Description Exchange Format), RID (Real-time Inter-network Defense), STIX (Structured Threat Information eXpression), TAXII (Trusted Automated eXchange of Indicator Information), OpenIOC (Open Incident of Compromise), CyBox (Cyber Observable Experssion), VERIS (Vocabulary for Event Recording and Incident Sharing), CAPEC (Common Attack Pattern Enumeration and Classification), Resource-Oriented Lightweight Indicator Exchange (ROLIE), Common Vulnerability Enumeration (CVE), MAEC (Malware Attribution and Enumeration Characterization) and ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) are popular examples of such standardized efforts.

Trust issue in cyber threat intelligence sharing has been addressed by the Mitre group with its sharing protocol TAXII (Barnum, 2014) and STIX. These are used for representation and sharing of IOC, respectively. Both are copyrighted by MITRE to ensure change control.

Trusted Automated eXchange of Indicator Information (TAXII ™) is a set of technical specifications and supporting documentation to enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII defines protocols and data formats for securely exchanging CTI over HTTPS which can be used to detect, prevent, and mitigate of cyber threats in real time. The basic design principles of TAXII are minimizing operational changes that are needed for adopting, easy integration with the existing sharing agreements between the organizations, and providing support for all widely used threat sharing models.

TAXII is not a specific information sharing initiative or technology, and it does not attempt to define trust agreements, governance, or non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to gain an improved situational awareness about the emerging threats, and enables organizations to easily share the information they choose with their partner organizations.

STIX (Structured Threat Information eXpression) is a fast evolving and works collaboratively to develop a language to represent the threat information in structured way. It enables organizations to share CTI in a consistent and machine-readable, semi-structured format based on JavaScript Object Notation (JSON). STIX plays a major role in automating the TIS process, and it also helps in automated detection and response.

The advantages of STIX are that it is modular and can describe different indicators and fields and it can incorporate other standards efficiently. The disadvantage of STIX is very complex to implement.

4. Challenges Of Threat Intelligence Sharing (Tis)

Although it is advantageous to share the threat information among organizations, there are some barriers for limiting the cooperation among them. Sharing threat intelligence information is challenging because of many reasons. Some of them are

- CTI information is highly sensitive, and if it is not handled properly it may cause reputation damage to the organization. If leaked CTI information may also expose some of the vulnerabilities present in the organization to other organizations and Hackers too.
- Trust between the organizations and the TISP provider is one of the most important concerns for sharing CTI.
- Quality of the CTI data and its completeness is another major issue which is under study. [7]
- The threat information shared is generally huge in terms of volume. The overloaded information collected through various means like open source, commercial sources, is very difficult to find the actual required intelligence that is of use for the organization.
- Costs of implementing the TI is very huge, thus making it difficult for some small and medium budgeted organizations to opt for it.
- Believing that the organization has not been attacked because the analysts doesn't experience any such incidents.
- Natural instinct for not sharing the breaches are also observed in some cases.

In general CTI information is collected and shared between the organizations which have well-established procedures to handle the information collected. The interoperability and security issues that should be faced by an organization before sharing the CTI information can be categorized into 4 types according to [2].

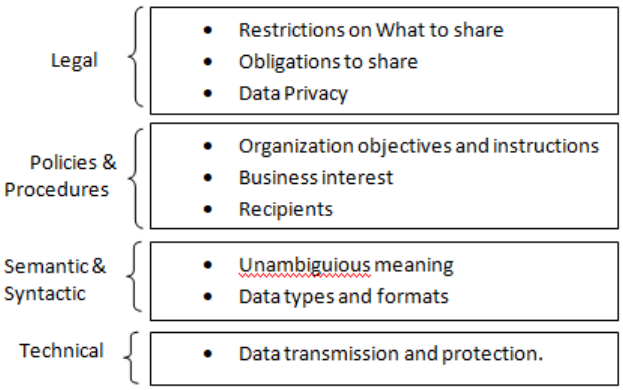

Figure 3: Interoperability and security issues in CTI Sharing

Legal issues involved in sharing the CTI information should address the constraints involved in the controlled sharing of the CTI data that involves personal identity information. Organizations should ensure that they are sharing this information within the legal frameworks of the respective organizations and nations.

Organizations have to carefully scrutinize the data that is being shared, and identify if any legally liable data is present. If such data is found proper policies and procedures under information security policy have to be framed by specifying the objectives of the organization in sharing such information. In general CTI data is collected from various sources and the data gathered is unstructured. Adopting Standards and applying semantics will help in ensuring the policies and organize the shared data.

The extent to which the TISP platforms provide the capabilities needed by the organization depends on the particular vendor. Some of the examples of TISP vendors are OASIS, Alienvault, Crowdstrike, Anomali Threat Stream, FireEye iSIGHT, IBM X- Force IRIS, palo alto, Solar Winds, Facebook Xchange, Mimecast, Sophos UTM, McAfee, Recorded future, LookingGlass cyber solutions and lot more.

5. Conclusion

There are many vendors and platforms already existing in the market which provides threat intelligence but majority of them are focusing on only collecting the data rather than analyzing the collected data. Analyzing the threat data and sharing threat information in an effective way requires common representation, standard formats and protocols required for sharing. If automation of the most tedious tasks of analysis of IOC can be achieved, and if it can aid the security teams in providing the actionable intelligence by suggesting supporting reactions in faster and more targeted way, then organizations may respond to these threats quickly and efficiently. To achieve this state, TISPs will be the efficient solution - provided the information exchanged should justify multiple aspects like legal, infrastructural, standardization and integration of different technologies must be in the acceptable from. In recent times more and more number of organizations are turning towards sharing the TI, which helps them in obtaining and sharing high quality Threat Intelligence information using TISPs. This can also accelerate the process of automating the Actionable Threat Intelligence to the maximum extent in the near future

References

Gong N.(2019) Barriers to adopting Interoperability Standards for Cyber threat Intelligence Sharing: AN Exploratory Study. In Arai K., Kapoor S., Bhatia R.,(eds) Intelligent Computing. SAI 2018. Advances in Intelligent Systems and Computing, Vol 857. Springer, Cham. He=ttps://doi.org/10.1007/978-3-030-01177-2 49.

MDPI and ACS Style; Rantos, K.; Spyros, A.; Papanikolaou, A.; Kritsas, A.; Ilioudis, C.; Katos, V. Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. Computers 2020, 9,18.

V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing standards, and Ontologies within Cybet Threat Intelligence", 2017 European Intelligence and Security Informatics Conference(EISIC), Athens, 2017, pp.91-98; doi:10.1109/EISIC.2017.20.

Chismon D, Ruks M. Threat Intelligence: Collecting, Analysing, Evaluating. Basingstoke,UK; MWR Infosecurity Ltd,2015.

MDPI Article: A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence ; Alessandra de Melo e Silva, Joao Jose Costa Gondim, Robson de Oliveira Albuquerque, and Luis Javier Garcia Villalba, June 2020.

Tundis A., Ruppert S., Mühlhäuser M. (2020) "On the Automated Assessment of Open-Source Cyber Threat Intelligence Sources". In: Krzhizhanovskaya V. et al. (eds) Computational Science – ICCS 2020. ICCS 2020. Lecture Notes in Computer Science, vol 12138. Springer,Cham. https://doi.org/10.1007/978-3-030-50417-5_34I.

Li Qiang, Yang Zeming, Liu Baoxu, Jiang Zhengwei YJ. Framework of Cyber Attack Attribution Based on Threat Intelligence. ICST Inst Comput Sci Soc Informatics Telecommun Eng 2017. 2017;190:92–103.

Skopik, F.; Settanni, G.; Fiedler, R. A problem shared is problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computer Security. 2016, 60, 154–176, doi:10.1016/j.cose.2016.04.003.

H Tounsi, W., Rais, H.: A Survey on technical threat intelligene in the age of sophisticated cyber attacks. Computer Security, 72,212-233(2018).

Liao, X,et al.: Acing the IOC game: Towards Automatic Discovery and Analysis of open-Source Cyber Threat Intelligence. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security- CCS 2016, pp. 755-766(2016)

D Planque, Cyber Threat Intelligence : From Confusion to clarity;

ENISA, " Exploring the opportunities and limitations of current Threat intelligence platorms" 2017.

OASIS CTI TC, "Structured Threat Information Expression(STIX)2.0", https://oasis-open.github.io/cti-documentation/, 2017.

MS Abu, SR Selamat,A Ariffin,R Yousof: Cyber Threat Intelligence-Issues and Challenges. In Indonesian Journal of Electrical Engineering and Computer Science, Vol 10, No1 April 2018.pp 371-379.

T Schaberreiter , V Kupfersberger, K Rantos, A Spyros et.al: A Quantitative Evaluation of trust in the Quality of Cyber threat intelligence sources. In proceedings of 14th international Conference on Availability, reliability, and Security,ARES 2019.

T.D Wagner, E Palomar, K Mahabub, Ali E. Abdallah, : A Novel Trust Taxonomy for shared Cyber Threat Intelligence.Security and Communnication Networks, 2018.

P Amthor,D Fischer, W E kuhnhauser,D Stelzer,.: Automated Cyber Threat Sensingnad responding: Integrating Threat Intelligence into Security-Policy-Controlled Systems. In proceedings of 14th international Conference on Availability, reliability, and Security,ARES 2019.

Cabaj K., Kotulski Z., ksiezopolski B. et al: Cyber security: Trends, Issues and Challenges. EURASIP J. on Information Security, 2018.

E.W. Burger, M. D. Goodman, P Kampanakis, and K. A. Zhu.: Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. In proceedings of the 2014 ACM workshop on Information Sharing and Collaborative Security WISCS '14