iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.59816

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Strategic Perspectives on Cyber Threat Intelligence: A Comprehensive Analysis

Nikhlesh Singh Janoti[1], Rohan[2], Rida[3], Neerja Negi[4]
Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India

Abstract: ***In the contemporary digital landscape, Cyber Threat Intelligence (CTI) has emerged as an indispensable element. Both organizations and individuals encounter persistent cyber threats from malicious actors seeking to compromise network security and pilfer essential information. This study delves into the prominent challenges of CTI, particularly focusing on Malware and other cyber- attacks, while elucidating the role of data mining within the CTI framework. By leveraging Cyber Threat Intelligence, entities can amass pertinent information pertaining to cyber-attacks. This paper succinctly outlines the intricacies of CTI, addresses associated challenges, and offers insights into the realm of Cyber Threat Intelligence concerning malware and data mining. The primary objective of this paper is to disseminate knowledge for safeguarding the digital realm against cyber threats, shedding light on effective defense strategies against malware and the optimal utilization of mining techniques.***
Keywords: Cyber-attacks, Cyber threat intelligence, Data mining, Malware.

I. INTRODUCTION

Cyber Threat Intelligence (CTI) is a crucial tool for organisations aiming to stay ahead from cyber-attacks and minimise their impact. It is the crucial information that helps us to understand and tackle threats to sensitive data. In cyber security malware takes centerplace as villain, thus CTI framework gives knowledge to detect, prevent and neutralise these digital threats. It is concerned with collection, production, interpretation, and distribution of knowledge on computer-based attacks so as to determine, follow up, and forecast possible threats and offer ways to mitigate the situation for better management decisions making. Therefore, it's important for organisations to move from the reactive approach of prevention detection and response of cyber-attack to a new era of dynamism which involves preemptive and responsiveness of cyberthreats. Organisations would be able to anticipate attacks targeting such weaknesses through the deployment and utilisation of CTI within their networks. However, commercial enterprises face several obstacles when embarking on the implementation of CTI. Threat intelligence has been linked to a military mindset that is often foreign in a corporate world. However, there is always a difference between an organisation's efforts to change its cyber security policy from compliance based to CTI driven to proactive. Thus, routine uses of CTI in practice are crucial for improving cybersurance.CTI has mainly three levels: strategic, operational and tactical.

Fig. 1. Levels of CTI

In the vast landscape of digital information, data mining emerges as a powerful tool of CTI. It transforms raw data into actionable insights. By Understanding this process, organisations can harness the power of data to predict cyber threats. Cyber security is the major challenge that every organisation faces in this digital age. An endless cyberspace war that is fueled by monetary agendas as well as economic purposes makes organisational information and system resources vulnerable. Examples include customer privacy data, company's commercial secrets, strategic plans, and interruptions of operation information technology.

Significantly, the cyber security battlefield is evolving rapidly over the past year or so. These advanced entities have been termed APTs. On the other hand, organisational cyber defences have fallen behindthe rapidly changing threat environment. Although most commercial organisations have developed complex cyber security models to meet the regulatory obligations including industrial standards and best practices, the cyber threat agents remain speedyand aggressive. Due to an asymmetric arms race, organisations exist in a tricky predicament because despite the strongest cyber defences, they still get overcome or overrun.

The study begins with a literature overview in Section II. Section III delivers a thorough examination of current research in the CTI mining domain its methodology along with taxonomy. In Section IV, the paper involves in a discussion surrounding challenges and potential future directions within this field. The conclusion in Section V has been discussed.

II. RELATED WORK

It is quite alarming and unfortunate to observe daily cybercrimes that are happening nowadays. According to thewire.in an estimated 1.3 terabytes of useful data was encrypted[1]. The hackers had made it impossible for AIIMS to access its own data on31 October 2023, a massive data breach, information of several Indians with the ICMRwere sold on the dark web.

Nowadays, the threat-sharing platforms are employed by organizations for the dissemination of threat information. The information comprises indicators of compromise such as the IOC's, threat model, or mitigation methodology. Global threat sharing platforms have enabled many organisations worldwide to strengthen their overall cyber security.

1) The development of cyber threat intelligence tools provide the assistance in gathering, filtering, and sharing threat intelligence between different companies. Theyaid automation in CTI with data collection from various open-source intelligence (OSINT) resources and malware sample analysis among others.

2) The creation of cyber threat intelligence certifications: One example is a CTIA certification by EC-Council which happens to be one among a growing number of cyber threat intelligence certifications. The certifications provide assurance that the analyticsprocess has sufficient expertise in the other rules.

Several recently introduced commercial CTIs describe structured and unstructured threat information. Tsai and Chan [2] examined cyber threat intelligence at a time when there were no standards for conveying threat information. Prior to the development of CTI standards, security experts and researchers shared their cyber security threat findings and insights on web blogs. The authors examined posts on various types of cyber security threats.

The expanding complexity of technology infrastructures, together with the modern era's increased interconnection and the targeted deployment of military-grade cyber weaponry, pose a significant and growing risk to private firms as per Baskerville et al. [3]. Recent industry assessments highlight the growing gap between the ability of "Advanced Persistent Threats" (APTs) to penetrate companies and the ability ofcommercial entities to defend themselves [4][5]. An Advanced Persistent Threat is defined as "an entity that engages in a malicious, organized, and highly sophisticated long-term or repeated network intrusion and exploitation operation to obtain information from a target organization, sabotage its operations, or both" [6].

Furthermore, Tounsi and Rais [7] divided existing types of threat intelligence into strategic, operational, and tactical categories. The primary focus was on tactical threat intelligence (TTI), which was mostly collected from indicators of compromise (IOCs). Their findings provided a thorough examination of TTI challenges, upcoming researchtrends, and standards.

In terms of Artificial Intelligence (AI) breakthroughs, Ibrahim et al. briefly reviewed the use of AI and Machine Learning (ML) methodologies to harness Cyber Threat Intelligence (CTI) to avoid data breaches. Rahman et al. [8] [9] expanded on this discussion by offering a comprehensive overview of several tools in the ML and Natural Language Processing (NLP) sectors, particularly for automatically extracting CTI from textual descriptions.

Recognizing the critical significance of CTI utilization in enhancing its effectiveness, Wagner et al. [10] undertook a study on cutting-edge techniques for distributing CTI. They looked at the accompanying issues, which included both technical and non-technical aspects of automating the sharing process.

Abu et al. [11] conducted a comprehensive survey, covering CTI's definition, concerns, and challenges. Ramsdale et al. [12] also summarized the present landscape of CTI-sharing formats and languages. The Comparative analysis of CTI framework has been shown in table1.

Table 1: Comparative analysis of CTI Framework

CTI Framework	Method	Objectives	Application

A Framework for Generating Malware Threat Intelligence [13]	Procedure 1: Incident response involves capturing data, detecting malware, and reporting on incidents. Procedure 2: Thorough and Definitive Examination includes data acquisition and preparation, malware analysis, threat classification, and threat assessment. Visualization and Report Generation	It includes analyzing and forecasting malware threats, establishingan Early WarningSystem (EWS), andproviding real-timetesting via security-as-a-service.	Malware classification, traffic analysis, and offer security-as-a-service.
Frameworkof Cyber Attack attribution Based on Threat Intelligence [14]	Initiate Analysis, Apply Threat Intelligence, Conduct Attribution Analysis	Collecting threatdata, processing detection, responding to cyber-attacks, attributing occurrences, and finally reversing the security condition.	Introduce the methods and components involved in attributing cyber-attacks using threat intelligence.
CTI Framework [15]	• Gathering and processing data • Analyzing data to generate Cyber Threat Intelligence (CTI) • Sharing and using CTI	Examining domestic and globaltrends in Cyber Threat Intelligence (CTI) technologies.	Framework capable of articulating diverse types of CTI structures.
New Intelligence Lifecycle [16]	Aggregation process withinthe Intelligence Lifecycle.	To improve understanding of the CTI idea by providing a key definition and developing a model for the intelligence production process.	The proposed paradigm and its related definition have the ability to address the issue of the enterprise's perspective about Cyber Threat Intelligenge.

As per the 2022 Crowdstrike threat intelligence report, CTI is gaining increasing recognition as a valuable asset, with 72 percent intending to increase spending on it over the next three months in 2022 [17]. Both government organizations and enterprises are channeling significant resources to enhance their CTI capabilities, acknowledging that maintaining an advantage in the ever-evolving threat landscape necessitates continuous improvement and adaptation. These endeavors involve cultivating in-house expertise, establishing partnerships with other organizations and industry leaders, and adopting cutting-edge technologies and methodologies. The commitments made by government agencies and businesses to improve their CTI capabilities demonstrate their commitment to protecting important assets and limiting the risks posed by cyber threats. CTI is an important component of a comprehensive cyber security strategy, as well as a valuable tool in continuous efforts to safeguard digital systems and networks for businesses and corporations. Thus mining CTI allows enterprises to identify evidence-based threats, update security measures, and detect early signals of dangers.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

III. METHODOLOGY

The Cyber threat intelligence comprises the six-phase technique that includes cyber scenario analysis, data gathering, data processing, analysis and performance evaluation,dissemination and feedback as illustrated in figure 2.

Phase 1-Cyber scenario Planning and analysis: The cyber scenario analysis stage, as the first phase in the threat intelligence lifecycle, is critical because it establishes the basis for subsequent threat intelligence operations. During the planning stage, the team works together to determine the goals and methodology of their intelligence program based on the cyber scenario's requirements, involving a variety of stakeholders in the project. The team's investigation may yield critical information such as:

1) Identifying attackers, their goals, and responsibilities in a specific cyberscenario.
2) Evaluation of sensitive surface areas susceptible to attack.
3) Strategies for strengthening defenses in preparation of probable futureattacks.

Fig. 2. Life Cycle of Cyber Threat Intelligence

Phase 2- Data Gathering: In order to protect enterprises and the security community from rapidly evolving cyber threats, significant initiatives have been launched to facilitate the sharing of threat intelligence. Undoubtedly, public sources play an important role in contributing to Cyber Threat Intelligence (CTI), regardless of the platform used for access. Several systems, such as AlienVault OTX [20], OpenIOC DB [21], IOC Bucket [22], and Facebook ThreatExchange [23], have been developed for the distribution of unclassified CTIs. Information shared on these platforms can help firms detect and mitigate security risks, prioritize security efforts, and respond more effectively to cyber threats. For example, Facebook ThreatExchange [23], which operates as a crowd-sourced platform, encourages participation from any organization, allowing real-time sharing of threat intelligence information, including details about malware and phishing

Phase 3-Data Processing: Following data gathering, it is critical to extract essential material, such as articles, paragraphs, or sentences, on Cyber Threat Intelligence (CTI),in preparation for CTI knowledge acquisition. Classification evolves as a commonly accepted method for categorizing information as related or unrelated to CTI. Researchers have extensively used machine-learning classification models trained on samples from various annotated classes (e.g., CTI-related or non-CTI-related) to predictthe classes of previously unseen data. Alternatively, unsupervised machine learning methods can be used to extract CTI-related information by clustering data based on content similarity.

Phase 4-Analysis: Following the distillation of CTI-related information, the next step is data analysis in the form of CTI knowledge acquisition. This method seeks to locateand get relevant and correct information depending on user requirements. Researchersand the CTI community have used Natural Language Processing (NLP) and Machine Learning (ML) approaches to extract CTI from textual data. In this stage, we evaluate the extracted Cyber Threat Intelligence (CTI) against our predetermined objectives. Evaluation often uses a variety of measures to assess performance. Accuracy, recall, precision, False Positive Rate (FPR), and F1-score are common metrics used inclassification and clustering applications.

Phase 5-Disemmination: Depending on the classification, CTI extraction is useful for decision-making in a variety of sectors. Here is a summary of essential applications inwhich acquired CTI plays an important part in decision-making, including CTI sharing,alert production, threat landscape analysis, search engine optimization, training goals, and countermeasure formulation.

Phase 6-Feedback: Seeking stakeholder comments on the provided report, assessing operational performance, altering priorities and objectives, changing reporting frequency and format, and adopting suggestions for better communication are all necessary elements in the continuous improvement process.

IV. CHALLENGES

In recent years, social media platforms such as blogs (such as AlienVault and FireEye blogs), vendor bulletins (Microsoft, Cisco, etc.), and specialized forums like Hack Forums (https://hackforums.net) have emerged as powerful channels for the exchange and dissemination of cybersecurity knowledge. Cybersecurity specialists often participate on these networks, offering their findings and ideas [8]. The increase in threat-related posts on social media has become an important source of information, frequently revealing new vulnerabilities, malware, and attack strategies. This influx acts as a primary source of cyber threat intelligence (CTI) [9]. Security companies are progressively extracting indications of compromise (IOCs) from these firsthand threat descriptions in order to proactively improve system protection. Consider the WannaCry ransomware [19]. If security staff have access to threat intelligence revealing that WannaCry uses port 445 to target systems, quickly blocking this port becomes a direct and successful technique to resist the malicious infiltration. The early extraction of CTI requires labor-intensive manual analysis of threat descriptions, which becomes impracticable because to the sheer volume of threat-related content. Several CTI standards and frameworks have been developed to automate the generation and distribution of cyber threat intelligence, including IODEF, STIX, TAXII, OpenIOC, and CyBox [19]. Many existing IOC extraction solutions follow the OpenIOC standard,extracting various sorts of IOCs such as malicious IP addresses, malware, file hashes, and more. Examples of such tools are CleanMX, PhishTank, IOC Finder, and Gartner Peer Insight, among others.

In cyber security there are there are lots of methods in cyber threat intelligence but there are some challenges too that should be addressed to mitigate the cyber threats some of the major challenges are below.

1) The Accuracy of data is critical. Inaccurate information can lead to false positive or false negative information that will affect the security measures.

2) The lack of knowledge of various data standards related to CTI the response can be delayed in cyber threat practices.

3) While sharing CTI information many organisations face privacy related issues establishing trust among organisations and sharing intelligent information on platformit is necessary to timely mitigate the cyber relieve.

4) Little knowledge about platforms such as Malware Information. Cyber Threat Intelligence: MISP leads to less data during cyber-attacks. Specialised training in MISP should ideally be made available for CTI experts to facilitate the proper storage of IOCs,sharing and visualisation of CTI data as well as tracking down the attacks.

5) The CTI process can be unproductive, which may happen due to absence of human expertise that understands and interprets the threat data. The threat intelligence expertsmust accordingly immediately detect the vulnerabilities, collect the proof, outline the TTPs related to threat actor and take prompt actions on security mitigations and effective incident response

6) The CTI process can be unproductive, which may happen due to absence of human expertise that understands and interprets the threat data. The threat intelligence experts must accordingly immediately detect the vulnerabilities, collect the proof, outline the TTPs related to threat actor and take prompt actions on security mitigations and effective incident response The CTI process can be unproductive, which may happen due to absence of human expertise that understands and interprets the threat data. The threat intelligence experts must accordingly immediately detect the vulnerabilities, collect the proof, outline the TTPs related to the threat actor and take prompt actions on security mitigations and effective incident response.

In recent years, the incidence of cyber dangers has continuously increased, with the current number of malwares tenfold greater than a decade ago. Security businesses are increasingly focusing on acquiring precise threat information and taking preventive actions. As a result, the capacity to predict risks is critical for early identification and mitigation of prospective assaults and associated losses.

One option is to aggregate substantial Cyber Threat Intelligence (CTI) reports and forum data from external sources, extracting relevant information such as attack names, characteristics, exploited vulnerabilities, targeted objects, and so on. This information enables the prediction of prospective threats against individual devices [18]. For example, if an attack report discloses damage caused by exploiting a vulnerability anda similar weakness exists in an organization's device, the attack is likely to hurt that device as well. This allows security professionals to proactively create protections before potential assaults occur.

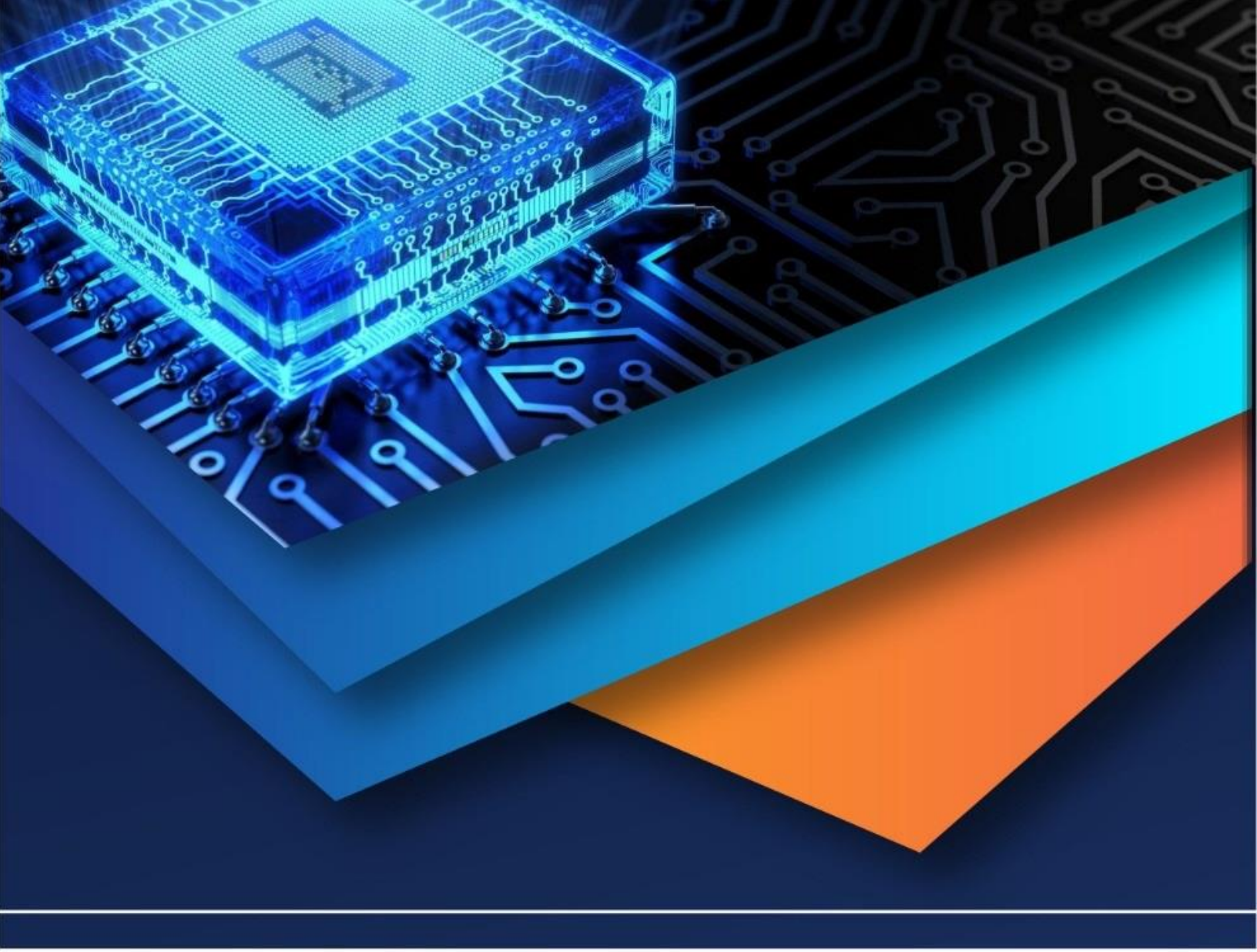
However, this system is only capable of anticipating attacks that have already occurred, i.e., threats documented in the gathered texts. The challenge remains in forecasting attacks that have not yet occurred, which is a continuous issue and area of complexity.

V. CONCLUSION

This CTI provides valuable information for organizations to make informed decisions about managing cyber threats. It acts as a routine security guard and very essential in the fight against zero-day threats. This paper explored the components of CTI, emphasized its importance, and and delves into its current state-of-the-art. In addition, a number of obstacles in CTI have been highlighted that affect many organisations nowadays. Organisations must tackle this aspect when they come again and do several training of CTI, to be able to identify the unknown hazards by integrating advanced technologies like block chain, cloud computing and machine learning to make up for all that will fully automate the procedure, rank and swiftly eliminate cyber-attacks.

REFERENCES

[1] Sun, Nan, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, Yonghang Tai, and Jun Zhang. "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives." IEEE Communications Surveys & Tutorials (2023).
[2] Tsai, Flora S., and Kap Luk Chan. "Detecting cyber security threats in weblogs using probabilistic models." In Intelligence and Security Informatics: Pacific Asia Workshop, PAISI 2007, Chengdu, China, April 11-12, 2007. Proceedings, pp. 46-57. Springer Berlin Heidelberg, (2007).
[3] Baskerville R, Spagnoletti P, Kim J, Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management 51(1):138-151(2014)
[4] Microsoft Corporation. (2020). Microsoft digital defense report. https://www.microsoft.com/en-us/download/ details.aspx?id=101738 (2020)
[5] Verizon Corporation. (2018). Data breach investigations report. https://www.verizonenterprise.com/verizoninsights-lab/dbir/
[6] Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. Computers & Security, 86, 402–418 (2019).
[7] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," Computers & Security, vol. 72, pp. 212–233 (2018).
[8] M. R. Rahman, R. Mahdavi-Hezaveh, and L. Williams, "What are the attackers doing now automating cyber threat intelligence extraction from text on pace with the changing threat landscape: A survey," arXiv preprint arXiv:2109.06808 (2021).
[9] M. R. Rahman, R. Mahdavi-Hezaveh and L. Williams, "A Literature Review on Mining Cyberthreat Intelligence from Unstructured Texts," 2020 International Conference on Data Mining Workshops (ICDMW), Sorrento, Italy, 2020, pp. 516-525.(2020)
[10] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," Computers & Security, vol. 87, p. 101589,(2019).
[11] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence–issue and challenges," Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 1, pp. 371–379 (2018).
[12] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, "A comparative analysis of cyber-threat intelligence sources, formats and languages," Electronics, vol. 9, no. 5, p. 824 (2020).
[13] E. Gandotra, D. Bansal, and S. Sofat, "A Framework for Generating Malware Threat Intelligence," Scalable Comput. Pract. Exp., vol. 18, no. 3, pp. 195–205, 2017.
[14] Y. J. Li Qiang, Yang Zeming, Liu Baoxu, Jiang Zhengwei, "Framework of Cyber Attack Attribution Based on Threat Intelligence," ICST Inst. Comput. Sci. Soc. Informatics Telecommun. Eng. 2017, vol. 190, pp. 92–103, 2017.
[15] N. Kim et al., "Design Of A Cyber Threat Intelligence Framework," vol. 5, no. 6, 2017.
[16] J. van de B. D. P. Sergei Boeke, "Cyber Threat Intelligence - From confusion to clarity; An investigation into Cyber Threat Intelligence," 2017
[17] "What is cyber threat intelligence? 2022 threat intelligence report." 2022. Accessed: Feb. 13, 2023. [Online]. Available: https://www. crowdstrike.com/cybersecurity-101/threat- intelligence/
[18] Abu, Sahrom, et al. "An enhancement of cyber threat intelligence framework." J. Adv. Res. Dyn. Control. Syst 10, 96-104 (2018).
[19] Menon, P. S. Analysis of Ransomware for Prevention of Attacks, Doctoral dissertation, University of Maryland, Baltimore County (2022).
[20] "AlienVault open threat intelligence." 2022. Accessed: Oct. 10, 2022. [Online]. Available: https://otx.alienvault.com/
[21] "A community OpenIOC resource." Accessed: Oct. 10 [Online]. Available: https://openiocdb.com/ (2022)
[22] "IOCbucket." Accessed: Oct. 10. [Online]. Available: https:// www.iocbucket.com/ (2022)
[23] "Facebook ThreatExchange." 2022. Accessed: Oct. 10 [Online]. Available: https://developers.facebook.com/products/threat-exchange (2022)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY