Volume 9, Issue 9, September– 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP430

The Future of Cyber Threat Intelligence: Anticipating and Preparing for Evolving Threats

Rajesh Kumar
Cyber Security Professional, USA

Abstract:- Modern cybersecurity protocols face unprecedented hurdles from the dynamic cyber threat ecology. In this context, the value of cyber threat intelligence as a prophylactic protective strategy increase (Abu, Selamat, Ariffin , & Yusof, 2018). This study provides a futuristic analysis of cyber threat intelligence, emphasizing the vital role that it will play in anticipating and becoming ready for evolving threats. This article also looks at threat actor methods, attack paths, and emerging technologies in an attempt to illustrate the dynamic nature of cyber threats and the need for adaptive intelligence solutions (Abu, Selamat, Ariffin , & Yusof, 2018). Ethical and legal considerations are also explored to highlight the necessity for a thorough and responsible approach to the gathering and implementation of cyber threat intelligence (Wagner, 2019). Through this thorough examination, readers will get a substantial comprehension of the technical developments and strategic requirements that will impact how cyber threat intelligence is developed (Abu, Selamat, Ariffin , & Yusof, 2018) (Wagner, 2019). This will provide enterprises with the agility and resilience to predict, mitigate, and respond to future cyber-attacks.

Keywords:- *Cyber Threat Intelligence, Cybersecurity, Strategic Imperatives, Risk Mitigation, Cyber Threats, and Evolving Threats.*

I. INTRODUCTION

The cybersecurity landscape is always changing due to the quick development and improvement of technology, which brings with it new and challenging issues (Abu, Selamat, Ariffin , & Yusof, 2018). The increasing interconnectedness of people and companies is leading to an increase in the frequency and sophistication of cyber-attacks. The dynamic nature of the digital landscape has led to the emergence of cyber threat intelligence as a crucial element in protecting digital assets and reducing associated risks (Abu, Selamat, Ariffin , & Yusof, 2018). Numerous organizations are impacted by organized crime groups who use ransomware and demand ransom payments in order to access vital data and systems. One notable instance is the ransomware attack that was dubbed "the most serious incident of its kind leveled against a U.S. health care organization" and targeted a significant U.S. health care payment processor (Abu, Selamat, Ariffin , & Yusof, 2018).

We seek to shed light on the proactive defense methods necessary for enterprises to remain ahead of developing threats by exploring the changing strategies and tactics used by threat actors as well as the technological breakthroughs that define the digital landscape (Abu, Selamat, Ariffin , & Yusof, 2018).

An extensive analysis of cutting-edge technologies like big data analytics, machine learning, and artificial intelligence is necessary to comprehend the direction that cyber threat intelligence is taking (Wagner, 2019). These technological developments give enterprises the chance to strengthen their security protocols while simultaneously giving threat actors more leverage. To guarantee responsible and legal procedures in the gathering and application of cyber threat intelligence, ethical and legal issues will also be covered (Wagner, 2019). Through a critical analysis of industry best practices, real-world case studies, and emerging trends, this paper aims to highlight the strategic imperatives for organizations to adopt proactive and adaptive cyber threat intelligence strategies (Wagner, 2019). By doing so, organizations can anticipate and respond effectively to the ever-changing threat landscape, fortifying their defenses and minimizing potential damages (Wagner, 2019). This paper explores the future of cyber threat intelligence (CTI) by examining the trends, advancements, and challenges that lie ahead in this field.

II. CYBER THREAT INTELLIGENCE

Cyber Threat Intelligence (CTI) refers to the information and insights gathered about potential and existing cyber threats. It involves the collection, analysis, and dissemination of intelligence to assist organizations in understanding and mitigating cyber risks effectively (Abu, Selamat, Ariffin , & Yusof, 2018). There are three significantly different types of CTI. The first one is Strategic Threat Intelligence; this is a type of CTI that focuses on making decisions and planning for the long term. Strategic threat intelligence provides a good picture of the threat landscape which includes their future motives, actions and how they are equipped with new technologies (Wagner, 2019). It assists businesses in developing security plans, allocating resources appropriately, and making well-informed choices to improve their overall security posture and second one is Operational threat intelligence which involves more tactical and real-time information (Abu, Selamat, Ariffin , & Yusof, 2018) (Wagner, 2019). It

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP430

provides actionable data about ongoing cyber threats and attacks, such as indicators of compromise (IOCs), threat actor tactics, techniques, and procedures (TTPs), and vulnerabilities. Operational threat intelligence helps security teams detect, respond to, and remediate attacks promptly (Wagner, 2019). It enables organizations to enhance their defense measures, patch vulnerabilities, and block malicious activities effectively and last is Tactical Intelligence Threats, this type of threat intelligence concentrates on campaigns, occurrences, or threat actors. It offers thorough insights into threat actors' tools, methods, and infrastructure as well as their targets and exploitable weaknesses (Abu, Selamat, Ariffin , & Yusof, 2018). Security teams may detect patterns, thwart specific attackers, and proactively fix system vulnerabilities with the help of tactical intelligence.

Fig 1 Types of CTI (Patsavellas, 2021) (Splunk., n.d)

By combining these three types of CTI, organizations can get a proper knowledge of CTI, encouraging them to enhance the effective security strategies, respond promptly to threats, and reduce overall risk exposure (Abu, Selamat, Ariffin , & Yusof, 2018).

III. THREAT INTELLIGENCE SOURCES

Threat intelligence sources refer to the various channels and platforms from which organizations gather information and insights about potential and existing cyber threats. These sources provide valuable data and analysis to enhance cybersecurity defenses (Ramsdale, Shiaeles, & Kolokotronis, 2020).

Open-Source Threat Intelligence Feeds are one of a kind where feeds are frequently offered at no cost, open-source threat intelligence feeds offer up-to-date data on cyber risks. Raw threat data or processed and evaluated threat intelligence may be included in these feeds. Open-source threat intelligence feeds include those from The Spam Haus Project and the National Council of ISACs. Many businesses provide threat intelligence services (Ramsdale, Shiaeles, & Kolokotronis, 2020). To deliver thorough and current information on cyber dangers, these services gather and examine enormous volumes of data. They frequently provide operational and strategic threat intelligence services that are suited to the individual requirements of their customers (Ramsdale, Shiaeles, & Kolokotronis, 2020).

ISACs are industry-specific organizations that gather and share threat intelligence. They facilitate collaboration and information exchange among organizations to address cyber threats in their sector. Security researchers, vendors, and government agencies often publish reports and research on emerging cyber threats and trends (Ramsdale, Shiaeles, & Kolokotronis, 2020). These reports provide valuable insights into new attack vectors, vulnerabilities, and threat actor tactics and online platforms such as GitHub provide community-curated threat intelligence resources (Ramsdale, Shiaeles, & Kolokotronis, 2020). These platforms enable the sharing of indicators of compromise (IOCs), malware analysis, and other threat intelligence information among the cybersecurity community.

It is important for organizations to assess their specific needs and resources when choosing a threat intelligence source. A combination of different sources may provide a more comprehensive and well-rounded view of the threat landscape (Ramsdale, Shiaeles, & Kolokotronis, 2020).

IV. LIFE CYCLE OF CYBER THREAT INTELLIGENCE

The process of gathering, creating, and disseminating intelligence so that others can use it. The US Insight People group utilizes a five-step process; different countries could utilize an alternate method. Along with planning and direction, the phases of the intelligence cycle are collection, analysis, processing, production, and distribution (Tounsi, 2019).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP430

- Planning: The planning phase involves defining the threat intelligence program's goals, scope, and requirements. It entails determining the key stakeholders, the kind of threat intelligence that is required, and the procedures and resources that are necessary for the efficient collection, analysis, and distribution of threat intelligence (Tounsi, 2019).
- Collection: During the Collection stage, threat intelligence is gathered from multiple sources, including open-source feeds, commercial providers, ISACs, research reports, and community-driven platforms (Tounsi, 2019). The collected data may include IOCs, malware samples, vulnerabilities, threat actor profiles, and other relevant information.
- Processing and Analysis: Once the threat intelligence data is collected, it needs to be processed and analyzed to extract meaningful insights. This stage involves aggregating and normalizing the data, identifying patterns, trends, and correlations, and assessing the credibility and relevance of the information (Tounsi, 2019). Analysts use various techniques, tools, and methodologies to transform raw data into actionable intelligence.
- Actionable Knowledge: After the examination stage, the danger insight is changed over into noteworthy insight. Interpreting the findings, putting threats in order of likelihood and potential impact, and offering suggestions for reducing the risks that have been identified are all part of this stage. Noteworthy knowledge ought to enable associations to go to proactive lengths to safeguard their frameworks, organizations, and information (Tounsi, 2019).

Fig 2 Life Cycle of Cyber Threat Intelligence (Splunk., n.d)

- Dissemination: After the actionable intelligence has been produced, it must be distributed to the appropriate stakeholders (Tounsi, 2019). The findings, insights, and recommendations must be effectively communicated to decision-makers, incident response teams, security operations centers (SOCs), and other relevant personnel during this stage. Reports, alerts, briefings, and automated feeds integrated into security tools are all examples of dissemination (Tounsi, 2019).
- Feedback and Iteration: The threat intelligence program's effectiveness can only be improved through constant feedback and iteration. This stage includes dissecting the effect of danger knowledge on security activities, episode reaction, and by and large gambling on the board. Criticism recognizes holes, refine assortment and investigation techniques, and improve the quality and idealness of the danger knowledge conveyed (Tounsi, 2019).

V. TECHNIQUES AND TOOLS IN CYBER THREAT INTELLIGENCE:

Structured automation of information exchange is critical for efficient intelligence sharing among organizations. The development of standard protocols, such as CybOX, STIX, and TAXII, and threat intelligence sharing platforms, such as MISP and OTX, has sped up this process. As of today, STIX has emerged as the de facto standard for describing threat intelligence data and is widely used by threat intelligence sharing platforms (Conti, 2018).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP430

➢ *Techniques:*

Organizations can select from various standards to fulfill their specific needs. MITRE has developed a package comprising of three standards or techniques, CybOX, STIX, and TAXII, which are designed to work together for managing Cyber Threat Intelligence (CTI) system. CybOX refers to the Cyber Observable expression XML schema, which is used to represent Structured Threat Information Expression (STIX) observable that describes cyber artifacts or events (Conti, 2018). STIX leverages CybOX vocabulary and comprises nine constructs, including indicators, incidents, tactics, techniques, and procedures (TTP), exploit targets, courses of action, campaigns, threat actors, and reports (Conti, 2018). Indicators such as IP addresses for command-and-control servers and malware hashes are frequently used by the community. TAXII or Trusted Automated exchange of Indicator Information is an open-source protocol and service specification that enables the sharing of actionable cyber threat information across organizations.

TAXII provides common, open specifications for transporting cyber threat information messages, with capabilities such as encryption, authentication, addressing, alerting, and querying between systems in a secure and automated manner (Conti, 2018). MILE established three standards, including Incident Object Description and Exchange Format (IODEF), Structured Cyber Security Information (IODEF-SCI), and Real Time Inter-Network Defense (RID) (Conti, 2018) (Conti, 2018).

IODEF, defined by RFC 5070, standardizes data from various sources for human analysis and incident response. IODEF-SCI extends the IODEF standard by adding support for additional data, while RID serves as a communication standard in CTI (Conti, 2018). The Open Indicators of Compromise (Open IOC) framework, introduced by Mandiant, characterizes static information. Lastly, the Vocabulary for Event Recording and Incident Sharing (VERIS) developed by Verizon allows organizations to share incident data and contribute to the analysis of a broader dataset (Conti, 2018).

➢ *Tools:*

The interest of organizations and security professionals in collecting and processing threat intelligence data is increasing (Keim & Mohapatra, 2022). However, without the assistance of threat intelligence tools, this data can become overwhelming. As a result, various parties have developed tools to help organizations and security professionals manage threat information sharing (Keim & Mohapatra, 2022) (Conti, 2018).

Nomenclature and dictionary tools for hardware and software configurations include Common Platform Enumeration (CPE) and Common Configuration Enumeration (CCE), respectively. REN-ISAC's Collective Intelligence Framework (CIF) is a client/server system for sharing enterprise threat intelligence data (Keim & Mohapatra, 2022). The server component collects and stores data, such as IP addresses, ASN numbers, email addresses, domain names, URLs, and other attributes (Keim & Mohapatra, 2022). Alien Vault's Open Threat Exchange (OTX) is a public platform for sharing research and investigating new threats. OTX cleanses, aggregates, validates, and enables the security community to share the latest threat data, trends, and techniques (Keim & Mohapatra, 2022).

McAfee Threat Intelligence Exchange has introduced a 'pull' service for subscribers to access up-to-date virus signatures and other information that McAfee anti-virus products use to protect Linux, Windows, or Mac computers against harmful software circulating each day (Keim & Mohapatra, 2022) (Conti, 2018). Additionally, the Malware Information Sharing Platform (MISP) developed by The Computer Incident Response Center Luxembourg (CIRCL) is a trusted platform designed for the collection and sharing of important indicators of compromise (IoC) of targeted attacks and threat information such as vulnerabilities or financial indicators used in fraud cases (Keim & Mohapatra, 2022).

Techniques and tools streamline threat intelligence, improve information sharing, and enhance threat detection and response (Conti, 2018).

VI. MORAL AND LEGAL CONTEMPLATION IN THREAT INTELLIGENCE

Organizations must follow privacy laws and regulations when handling PII or sensitive data for cyber threat intelligence (Bromander, 2021). This includes compliance with laws like GDPR in European union, HIPAA in United States, and other relevant data protection laws in different regions. Sharing threat intelligence requires adherence to legal frameworks and information sharing agreements (Bromander, 2021). Organizations should be mindful of any limitations or requirements for sharing specific types of threat data, especially in cross-border collaborations.

To safeguard sensitive threat intelligence data, cyber threat intelligence analysts and organizations must implement robust data protection measures, access controls, and encryption to prevent unauthorized access and disclosure of sensitive information (Bromander, 2021). Ethical use of intelligence is crucial for organizations and analysts. It involves utilizing threat intelligence responsibly to improve cybersecurity, support incident response, and prevent malicious activities. It's important to refrain from using intelligence for unauthorized or offensive purposes (Bromander, 2021).

When collecting threat data, organizations should ensure that data collection practices adhere to ethical norms, including obtaining informed consent when necessary (Bromander, 2021). This is particularly relevant when gathering threat information that may involve individuals or entities that are not directly related to cybersecurity operations (Bromander, 2021). Organizations should have

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP430

clear policies and oversight mechanisms in place for managing and sharing threat data.

Cyber threat intelligence activities should be carried out with respect for human rights, such as the right to privacy and freedom of expression (Bromander, 2021).

- *Economic Benefits:*

Cyber Threat Intelligence (CTI) provides significant economic benefits by enabling organizations to preemptively identify and mitigate cyber threats, reducing the potential financial impact of cyber incidents (Saeed, 2023). The papers in this special section collectively highlight the importance of CTI in safeguarding infrastructure and societal operations from the economic toll of cyber threats. Enhancing risk management, particularly in sectors such as higher education, CTI helps institutions like Saudi universities to mitigate cyber risks, which can be extrapolated to suggest similar benefits for organizations in the USA (Saeed, 2023). The integration of machine learning with CTI further suggests that the efficiency and effectiveness of cybersecurity measures can be significantly improved, potentially leading to economic benefits through the prevention of costly breaches (Saeed, 2023). In summary, while this section of the papers does not directly quantify the economic benefits of CTI for the USA, they collectively highlight the importance of CTI in enhancing cybersecurity measures. The ability of CTI to inform and improve risk management strategies, coupled with the potential for integrating advanced technologies like machine learning, suggests that CTI can lead to substantial economic benefits by preventing cyber incidents and minimizing their financial impact on organizations (Saeed, 2023).

- *Future of Cyber Threat Intelligence:*

The future of Cyber Threat Intelligence appears to be oriented towards integrating advanced analytical techniques and expanding intelligence sources to combat increasingly frequent and sophisticated cyber threats (Security, 2024). The reviewed papers suggest a trend towards using AI, ML, and NLP to enhance CTI systems. These technologies are expected to improve threat detection, analysis, and prediction efficiency and accuracy, leading to a more proactive and informed cybersecurity posture (Security, 2024). While the adoption of AI and ML in CTI is widely acknowledged as beneficial, challenges such as high-quality data requirements, system integration complexity, and ethical considerations exist (Security, 2024). The use of fuzzy logic as a novel approach to managing CTI data's uncertainties is also highlighted, indicating potential future research and application. The use of structured languages like STIX for information sharing and ontology-based semantic knowledge modeling suggests a move towards standardized and effective threat intelligence communication (Security, 2024). In summary, the future of CTI is expected to be shaped by the incorporation of advanced computational methods and the standardization of threat information sharing, with AI, ML, and NLP integration significantly enhancing threat identification, analysis, and mitigation, despite the challenges that may arise (Security, 2024).

VII. CONCLUSION

Cyber threat intelligence (CTI) is a vital aspect of the cybersecurity domain, offering organizations critical information to proactively identify and mitigate cyber threats (Abu, Selamat, Ariffin , & Yusof, 2018). However, concerns such as reputation damage, legal implications, and data misuse often deter organizations from sharing sensitive information. Despite these challenges, advancements in privacy-preserving solutions and frameworks are being developed to facilitate secure CTI sharing (Abu, Selamat, Ariffin , & Yusof, 2018). Although frameworks like MITRE ATT&CK and STIX are essential for structuring CTI, they do not fully address the execution of activities for leveraging CTI data (Wagner, 2019). Additionally, integrating machine learning and artificial intelligence with CTI promises to automate threat analysis and enhance cybersecurity strategies. However, the effectiveness of these technologies depends on the quality and specificity of the data they process. In conclusion, CTI is a vital tool for cybersecurity, and its effectiveness is contingent upon the ability to share and analyze threat data collaboratively and securely (Wagner, 2019). The development of frameworks and the application of advanced technologies like machine learning are enhancing the utility of CTI. Further research and development in this field must address the challenges of secure information sharing and refine analytical tools to ensure that CTI remains a robust asset in the fight against cyber threats.

REFERENCES

[1]. Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 371-379.

[2]. Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.

[3]. Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats, and languages. Electronics, 9(5), 824.

[4]. Tounsi, W. (2019). What is cyber threat intelligence and how is it evolving? Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT, 1-49.

[5]. Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber threat intelligence: challenges and opportunities (pp. 1-6). Springer International Publishing.

[6]. Keim, Y., & Mohapatra, A. K. (2022). Cyber threat intelligence framework using advanced malware forensics. International Journal of Information Technology, 14(1), 521-530.

[7]. Bromander, S. (2021). Ethical considerations in sharing cyber threat intelligence. Understanding Cyber Threat Intelligence-Towards Automation, 45.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP430

[8]. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors, 23(16), 7273. https://doi.org/10.3390/s23167273

[9]. Security, M. (2024, April 24). What will cyber threats look like in 2024? CSO Online. https://www.csoonline.com/article/2095115/what-will-cyber-threats-look-like-in-2024.html

[10]. Patsavellas, J., Kaur, R., & Salonitis, K. (2021). Supply chain control towers: Technology push or market pull—An assessment tool. IET Collaborative Intelligent Manufacturing, 3(3), 290–302. https://doi.org/10.1049/cim2.12040

[11]. What is Cyber Threat Intelligence? | Splunk. (n.d.). Splunk. https://www.splunk.com/en_us/blog/learn/cyber-threat-intelligence-cti.html