Cyber Threat Intelligence Sharing: A Survey

Rufus Muchiri*, Dr. Shem Mbandu, PhD, Dr. Charles Katila, PhD

Department of Computer Science and Information Technology, School of Computing and Mathematics. The Co-operative University of Kenya, P.O. Box 24814-00502, Karen, Nairobi, Kenya

* E-mail of the corresponding author: rufusmuchiri@gmail.com

Abstract

The importance of CTI is underscored by its ability to provide structured and actionable insights into threat landscapes, helping organizations anticipate and neutralize cyber-attacks before they manifest. This study surveys the landscape of CTI sharing and explores the various mechanisms and strategies employed to enhance CTI information sharing. The paper explores the fundamentals, benefits, and challenges of CTI sharing and reviews current proposals addressing these issues. Additionally, we examine the use of machine learning in CTI sharing, which improves intelligence by incorporating advanced analytics for more refined data and predictive analytics to anticipate attack patterns, thereby enabling proactive measures. The study also explores the role of trust in collaborative CTI sharing, especially in automated environments, and the use of sector specific CTI sharing mechanisms to mitigate the issues of trust concerns in CTI sharing. Through this review, this study contributes to the ongoing discourse on CTI sharing to improve cyber defense mechanisms in an increasingly interconnected and vulnerable digital world.

Keywords: Cyber Threat Intelligence (CTI), CTI Sharing Framework, Cyberattacks, Cybersecurity, Trust
DOI: 10.7176/JIEA/15-2-08
Publication date: September 28th 2025

1. Introduction

The rise and complexity of cyber threats in the current digital era have led to a pressing need for effective countermeasures [1,2]. Cyber threat intelligence (CTI) has become a critical aspect in addressing these risks. Gartner defines Threat intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard" [3]. CTI encompasses the collection, analysis, and distribution of information concerning existing and emerging threats in order to assist organizations in devising strategies to safeguard their infrastructure and in identifying the threats that present the highest level of risk. The contemporary escalation in cyberattacks has generated an extensive repository of data pertaining to these incidents, effectively creating a detailed repository of information about such threats. In order to adequately protect computer systems and IT infrastructure, organizations must possess a thorough understanding of system vulnerabilities, weaknesses, and the methods employed by malicious actors. [4]. Comprehending the behaviours of threat actors enables organizations to more effectively safeguard against potential threat. CTI allows organizations to adopt a proactive stance in their security measures, rather than merely responding to threats as they arise [5,6]. According to [7], for a CTI to garner trust, it must be rooted in substantiated evidence. Moreover, to effectively address and mitigate threats, the knowledge derived from CTI must be actionable. The fundamental purpose of CTI is to counteract the escalating complexity, variety, agility, and frequently ingenious tactics of threat actors with equivalent capabilities.

CTI plays a pivotal role in identifying, understanding, and combating cyber threats by reducing information asymmetries between attackers and defenders, thus enabling more informed and timely responses to potential threats [6]. The primary rationale behind CTI is the necessity to counteract the escalating complexity, variety, agility, and frequently ingenious tactics of threat actors with equivalent capabilities. The objective of CTI is to enhance organizations' awareness of the dynamic threat landscape, enabling them to detect and mitigate potential threats before they impact their systems [8]. By utilizing threat intelligence data, organizations can improve their decision-making processes when confronted with imminent threats posed by threat actors, thereby protecting the organization's interests. CTI has the capability to guide cyber-response efforts by offering a specific defence strategy designed to counteract the tactics and techniques employed by cyber-threat actors. CTI is essential in assisting cyber defenders to develop strategies that support in detecting, preventing, or ideally predicting cyber-attacks, thereby enabling informed decision-making [9].

Our paper provides three main contributions. First, we examine how machine learning can enhance CTI sharing by refining intelligence and predicting attack patterns, thereby enabling proactive measure. Second, we highlight the critical function of trust in collaborative CTI sharing environments and emphasize how sector-specific sharing frameworks can address trust concerns. Lastly, this review contributes to the ongoing discourse on CTI sharing to improve cyber defense mechanisms in an increasingly interconnected and vulnerable digital world.

2. CTI Life Cycle

In order to achieve a comprehensive understanding of cyber threat intelligence, it is imperative to incorporate relevant threat data that undergoes a series of sequential stages including acquisition, examination, and refinement. These stages ultimately lead to the generation of actionable intelligence, enabling informed decision-making, all within a timely manner. The CTI lifecycle is a systematic structured process that aims to improve the acquisition, processing, analysis, and dissemination of CTI information, with the ultimate goal of aiding in the detection, prevention, and response to cyber threats [9-12].

The initial phase of the CTI life cycle entails data collection, which consists of gathering information from various sources, such as human intelligence (HUMINT), open-source intelligence (OSINT), signals intelligence (SIGINT), and imagery intelligence (IMINT) [9-10]. CTI data sources can be categorized into internal, external, and community sources. Internal sources include sources such as network logs and Security Information and Event Management (SIEM) systems, while external sources may include open or commercial threat intelligence feeds. Community sources include data from CTI sharing arrangements such Information Sharing and Analysis Centres (ISACs) and others that may be National, Industry, or sector specific in nature and could be regulated or not [13-16]. These sources provide comprehensive coverage of potential threats, ensuring that organizations have access to a wide array of data points.

Once data is collected from various sources, it is analysed by trained professionals or through automated analysis to identify patterns, correlate data points, and understand the context of the threats to identify specific threats aimed at targets. This analysis stage involves processing and storing of the intelligence in standardized formats such as the Structured Threat Information Expression (STIX) to allow for consistent and machine-readable representation of threat information. This standardization facilitates efficient sharing and refinement of the information [4, 9-10, 17]. After CTI has successfully undergone the analysis process, it becomes essential to promptly deliver this intelligence to the appropriate recipients to make informed decisions.

The final stages of the CTI lifecycle involve implementing preventive or mitigation actions based on the analysed intelligence. Automated systems can respond to threats in real-time, guided by predefined courses of action, and continuous feedback from these actions helps in refining the intelligence and updating the lifecycle, thereby improving the overall cybersecurity posture of the organization.

3. CTI Sharing

CTI sharing is the process of exchanging information about cybersecurity threats and vulnerabilities among various entities, including security teams, business partners, vendors, clients, regulatory bodies, and industry organizations [18]. This is critical because organizations must collaborate to strengthen their cybersecurity posture. According to [19], CTI sharing serves two essential functions. First, it facilitates a proactive response to threats, ensuring timely protection of information systems. By sharing CTI through dedicated platforms, businesses can quickly access crucial information, bypass time-consuming threat analysis processes, and promptly apply them to enhance their security measures. Second, the motivation for CTI sharing arises from the recognition of limited analytical capabilities within individual organizations. Organizations that are part of a CTI sharing community have the opportunity to utilize the combined knowledge, experience, and capabilities of the community members in order to develop a comprehensive understanding of the potential threats that their organization may encounter.

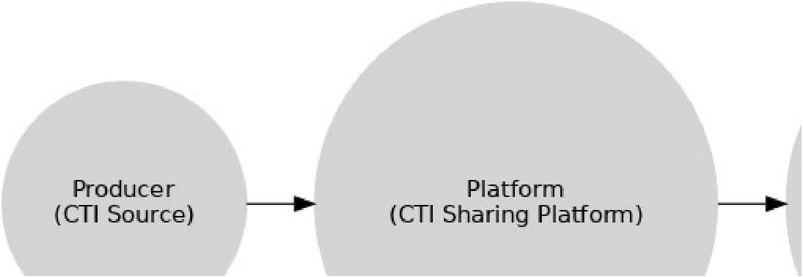

Fig. 1. This figure shows the main components of CTI sharing. [19].

The theoretical idea of CTI sharing involves three main components: CTI producers, CTI consumers, and platform operators. CTI consumers subscribe to CTI feeds to promptly receive the most up-to-date threat intelligence. Conversely, CTI producers release new CTI derived from threat analysis. The platform serves as an intermediary to facilitate the exchange and storage of CTI. Participants in CTI sharing have the capability to simultaneously hold multiple roles. Consequently, the diverse sharing mechanisms for CTI encompass both a hub-and-spoke model and a publish-subscribe model with distinct roles [19].

Researchers [13,17] pinpointed three prevalent models for CTI sharing, namely peer-to-peer, which facilitates direct CTI sharing, peer-repository (hub-spoke), which enables peers to subscribe to published events, and hybrid sharing, which fuses the aforementioned models. [16], identified similar basic sharing models namely; Hub-and-Spoke, Post to all, and hybrid Models. According to [2], the current CTI sharing market landscape is characterized by three primary types of entities; (a) Professional and for-profit CTI firms: These commercially motivated entities operate as business enterprises, driven by the pursuit of financial gain. They prioritize the protection of their proprietary information (PI) and restrict access to their services exclusively to paying members. (b)Sector-specific, invitation-only networks: These exclusive communities, such as those in the banking domain, operate on an invitation-only basis, emphasizing the notion of exclusivity within specific industries. This exclusivity facilitates the exchange of specialized knowledge and expertise among trusted peers, and (c) Government-funded, national, semi-closed platforms: These platforms, such as the United Kingdom's CiSP and the United States' CISCP, are established and funded by governments. They operate on a national scale and maintain a semi-closed structure, granting access only to authorized users. This semi-closed approach enables the sharing of sensitive information while maintaining controlled access and ensuring data security [1]. This segmentation of the CTI market reflects the diverse needs and priorities of its stakeholders.

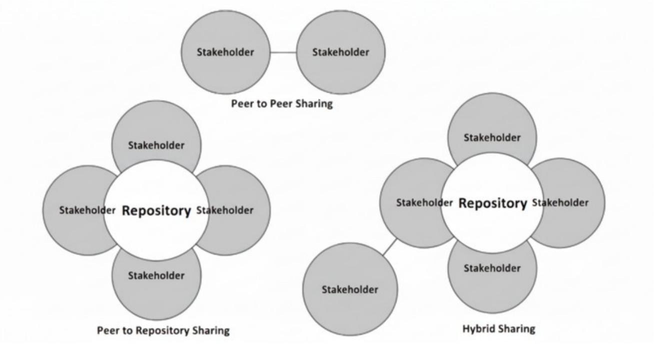

Fig. 2. This figure shows the 3 common models in CTI sharing. [13]

3.1 Types of Threat Intelligence

According to [17, 20], CTI can be divided into four main categories, namely strategic, operational, tactical, and technical. [21] also identified more or less similar categorization of CTI namely; tactical, operational and strategic levels. At each of the different levels, different kind of CTI information is used to serve the different purposes ranging from the more technical atomic or discrete indicators of compromise (IoCs) data to the computed IoCs, and behavioural IoCs, to Tactics, Techniques and Procedures (TTPs)[10]. Ultimately these different levels of CTI help in augmenting cyber defensive capabilities through situational awareness, prediction, and automated course of action. At the low or the more technical levels CTI is more about getting information about an attacker's assets, attack vectors employed, Command and Control domains used, and types of vulnerabilities exploited. The goal is to expedite early detection of malicious behaviour, preferably before a malicious actor gains a foothold in the network [21].

At the operational and tactical levels, CTI helps organizations transition from reactive to proactive responses to cyber threats by providing information about the nature and motivations of potential upcoming attacks. This information can be used to develop targeted prevention strategies. At the tactical level, Technical Tactics and Procedures (TTPs) and Indicators of Compromise (IoCs) can be employed to identify specific attack vectors and vulnerabilities. These can then be used to proactively update signature-based defenses against known threats [20]. According to [22], utilizing tactical threat intelligence, which encompasses tactics, techniques, and procedures (TTPs), is highly beneficial in attempting to detect and prevent future attacks. This area is currently receiving the most attention in research and development within CTI, particularly in relation to Advanced Persistent Threats [23].

At the higher levels, CTI assumes a strategic role by empowering decision-makers with the ability to comprehend and interpret the relevant threat landscape, thereby enabling them to make well-informed choices [21]. At a strategic level, CTI is typically conveyed in plain language and aims to enhance situational awareness while presenting business risks. Its target audience is comprised of senior, non-technical decision-makers within an organization [20].

3.2 Benefits and Risks of CTI Sharing

CTI Sharing improves early threat detection, accelerates response times, and fortifies defence strategies through collaboration and data exchange. It offers cost-effective security measures, enhances regulatory compliance, and fosters community engagement. Ultimately, CTI sharing greatly enhances situational awareness and proactive defence capabilities [6,13,24].

3.3 Challenges and Barriers of CTI Sharing

Although the advantages associated with CTI sharing are significant, its implementation across diverse industries and sectors remains limited [25]. Several obstacles, including both technical and non-technical factors, hinder organizations from adopting CTI sharing. For instance, barriers such as initial setup, learning curve, organizational compatibility, and comprehension of cyber threat language can impede the adoption of standards like STIX and TAXI [13,26]. Other challenges and barriers to CTI sharing are outlined below

3.3.1 Limited know-how

Most organizations especially commercial ones often lack the knowledge and expertise on how to adopt and integrate CTI into their cybersecurity practices. The utilization of threat intelligence often entails a military mindset that is not typically found within the business culture prevalent in many organizations [27]. There is a gap between understanding and adopting CTI sharing practices [11] points out that organizations and vendors often lack a complete understanding of what constitutes CTI, indicating a need for further research to define CTI clearly. Although there are vendor-supplied CTI services and general industry guidelines on best practices in cybersecurity, there is a scarcity of precise guidance on integrating CTI into regular organizational practices [27]. Developing user-centric sharing platforms and clarifying CTI concepts can enhance the know-how among organization in CTI sharing [11]. There are challenges faced by users of CTI platforms, particularly from a user experience (UX) perspective, which are not well explored. This suggests that there may be a disconnect between the development of CTI sharing tools and the practical needs and know-how of their users [28]. Additionally implementing CTI sharing mechanisms have economic costs that organization must be willing to spend and stakeholders may have varying resources in terms of how much they can spend on detection and defence [12,16, 20]. Establishing and sustaining a comprehensive CTI capability can prove to be a costly endeavour, especially for smaller entities that possess restricted resources.

3.3.2 CTI sharing Automation

The traditional CTI sharing approaches are mainly manual and are therefore labor intensive, for example emails, telephone call etc. The lack automation limits their scalability and effectiveness. Lack of automation in CTI sharing results in inefficiencies, delays, and are prone to errors in processing and distributing threat information. Automation is the key to effective CTI sharing [17]. It is required to manage the influx of internal alerts and externally received vulnerability information. In the recent past, the formation of communities for the semi-automated exchange of Cyber Threat Intelligence (CTI) has gained momentum. The SANS institute's 2021 survey indicates that automated CTI sharing platforms have experienced a 3% upsurge in usage compared to the previous year, while traditional sharing mechanisms have witnessed a 7.8% decline [29]. The primary objective of automated CTI exchange is to streamline and expedite the process of sharing, documenting, evaluating, and remedying security-related information [13].

3.3.3 Legal and Regulatory challenges

CTI Sharing can be hindered by legal, regulatory, and even political constraints mainly due to potential liability and national security concerns. The regulations governing the disclosure of personal information vary across nations, with privacy protection laws determining the extent to which data may be shared and the necessity of anonymity [13]. Sharing may also subject nondisclosure agreements and product-based contracts to liability. For instance, it might expose a product vulnerability that is safeguarded by the vendor through disclosure restrictions or disclose indications that a breach has occurred within the organization, potentially resulting in regulatory penalties [30]. Compliance with legal and regulatory requirements, such as data protection and privacy laws, can limit the sharing of threat intelligence. Organizations may hesitate to report cyber threat incidents due to uncertainty about the types of information that can be disclosed without raising legal questions regarding data and privacy protection. Additionally, there may be penalties for failing to inform the authorities and affected individuals of security breaches [13]. Due to the significant disparities in legal and regulatory structures across different countries and jurisdiction, it is imperative for CTI sharing environments to be flexible in order to fulfill the varying duties imposed by different legal and regulatory obligations [20]. Legal protection may be required to shield sharing organizations from liability. For example, in the USA where the Cybersecurity Act of 2015 provides protections for organizations that share threat information [31].

3.3.4 Cultural, organizational and language barriers

Organizational cultures and structures can impact information exchange. Siloed approaches, lack of communication channels, and internal barriers within organizations can impede the flow of information between different teams or departments. Lack of standardized processes and formats for sharing threat intelligence, may make organizations face difficulties in understanding, interpreting, and utilizing the shared information. Standardization can enhance interoperability and facilitate effective information exchange [16].

The global nature of CTI exchange can give rise to cultural and linguistic obstacles among stakeholders. It is imperative to establish a consensus regarding the adoption of a universally recognized language, such as English, for effective communication. The utilization of a common language facilitates the exchange of knowledge among individuals, thereby expediting the knowledge-sharing process. In the event that a stakeholder lacks comprehension of the language being used, it becomes necessary to allocate significant time and effort towards the process of translation. According to [13] the quality and usefulness of the CTI may be compromised if certain crucial features are not accurately conveyed during the process of translation.

3.3.5 Scalability

The capacity of a system to maintain its enhanced performance levels even as workloads change is known as scalability. Scalability is a significant challenge in the sharing of CTI [17, 32, 33]. The integration of blockchain technology and federated learning mechanisms have the potential to address some of the technical challenges of scalability of CTI sharing [33]. For example, federated learning mechanisms can enable distributed training of machine learning models across a network of devices, without the need for centralized data storage. The integration of these two technologies can potentially lead to the development of highly efficient and dependable systems capable of managing extensive data processing and machine learning tasks while simultaneously preserving data privacy and security [6]. Despite being mainly, a technical problem in CTI sharing [17], scalability it is intertwined with various other technical and non-technical factors that may also need to be addressed to achieve effective and scalable CTI sharing [13, 34]. On major challenge related to scalability in the context of CTI sharing is information overload . Information overload can lead to difficulties in identifying relevant threats, resource constraints, and challenges in prioritization and decision-making. Achieving scalability is of paramount importance as CTI deals with substantial volumes of data pertaining to threats. To tackle this issue, organizations may explore avenues such as automation and machine learning, data filtering and aggregation, collaboration and information sharing, and visualization and reporting [35].

Table 1. Summary of Challenges of CTI Sharing

No.	Challenges	Explanation
1	CTI sharing Automation	Automation in CTI sharing involves using automated tools and processes to collect, analyze, and disseminate threat intelligence data. These tools enhance threat detection and facilitate the sharing of relevant intelligence among organizations, thus reducing the time and effort needed for cybersecurity management.
2	Scalability	Scalability in CTI sharing pertains to the ability of CTI systems to manage growing data volumes and participants without losing performance, ensuring efficiency as more organizations join and share data.
3	Privacy	In CTI sharing, privacy entails protecting sensitive information about an organization's security posture, vulnerabilities, and incidents. Techniques like data anonymization, encryption, and access controls prevent unauthorized disclosure of such information.
4	Information Overload	Information overload in CTI sharing refers to challenges in processing and prioritizing vast amounts of threat intelligence data, making it difficult to identify the most relevant threats and respond promptly.
5	Interoperability/ standardization	Interoperability and standardization in CTI sharing require adopting common standards and protocols for seamless communication and data exchange between various CTI platforms and organizations. Examples include; STIX and TAXII
6	Cultural, organizational	Cultural and organizational factors in CTI sharing involve attitudes, policies, and practices that affect organizations' willingness and ability to share threat intelligence.
7	Legal and Regulatory	Legal and regulatory considerations in CTI sharing require compliance with data sharing and privacy laws. Organizations must navigate multiple legal requirements to share threat intelligence without breaching regulation
8	Lack of trust	Lack of trust in CTI sharing arises from concerns about data misuse, competitive disadvantage, or revealing vulnerabilities. Establishing trust through transparency, clear agreements, and demonstrated benefits is crucial

3.4 Blockchain based CTI sharing models

The conventional methods of CTI sharing suffer from challenges of free riding, accountability, validity, and auditability within the CTI sharing processes, as well as lack of incentives of sharing [36, 37]. The term "free riding" is often used to describe individuals who derive benefits from collective intelligence without contributing any knowledge of their own, which can, in turn, undermine the collaborative nature of CTI sharing and lead to a decreased willingness among participants to provide useful information.

Blockchain technology is being employed to address the predominant challenges of the conventional sharing methods. CTI sharing using blockchain technology exhibits notable diversity. Within this landscape, various models make use of distinct attributes of blockchain and cryptographic elements in diverse manners to enable effective sharing. In regard to the problem of producer-consumer imbalance (free riding), various blockchain sharing models have been proposed [20]. These are based on incentived sharing by either applying concessions or discounts to the CTI sharing subscription fees to reward CTI producers for their contributions. Another approach used to address the issue of free riding in CTI sharing is through the implementation of consumption fees. Unlike subscription concessions, consumption fees require consumers to pay producers for access to the CTI they have shared [38, 39]. Essentially, consumption fees aim to create a marketplace where CTI can be traded between organizations for currency [39]. Proposed models include a blockchain-based CTI sharing platform, DEALER (Decentralized Incentives for Threat Intelligence Reporting and Exchange), which utilizes a user-defined consumption fee to incentivize CTI sharing. Most incentive-based blockchain CTI sharing models aim to create a blockchain-based CTI marketplace where producers who actively share valuable CTI can profit significantly from doing so. The use of blockchain is particularly advantageous in this case due to its trustless properties, which enable CTI exchange between two organizations without the need for pre-established trust or a third party [20].

Another significant challenge that blockchain addresses in the realm of conventional CTI sharing pertains to the validity and quality of the shared CTI. This concern is tackled through the utilization of blockchain's inherent immutability features, which facilitate auditing of users' actions within the sharing platforms. The main idea is to be able to identify and punish users who participate in false sharing. This can be done through imposing financial penalties. [40] proposed one such framework named BLOICS. In the context of blockchain-based CTI sharing platforms, conditionally refundable deposits are implemented to impose financial penalties on CTI producers who engage in deceptive practices. A major criticism of these deposit-based mechanisms revolves around the methodology employed to validate the credibility of shared CTI. Due to the current challenge of definitively classifying CTI as false, this could affect the success of deposit-oriented approaches. Ultimately, this situation might deter honest users from engaging in the sharing process.

Blockchain-based solutions can also employ reputational systems to combat false sharing. These systems differ from deposit systems in that they do not levy monetary penalties on malicious users. Instead, they assign each user a reputation score, such as between 1 and 100, which represents their perceived trustworthiness. These reputation scores can be leveraged to directly influence a user's capacity to both access and disseminate intelligence within a group, or to communicate to others their degree of confidence in the sharing platform. Similar to deposit mechanisms, the efficacy of these reputation-based systems hinges on the methodology adopted to validate the veracity of the shared CTI- an ongoing challenge, as previously mentioned [37].

3.5 Types of CTI Sharing Frameworks

CTI Sharing Frameworks can be categorized in various types depending on their areas or geographical regions, or nations, and sectors of applicability or depending on their developers or proprietary.

3.5.1 Regional CTI Frameworks

Regional CTI sharing frameworks are systems that support the exchange of CTI among businesses operating within a specific geographic region. These frameworks can be advantageous for companies that have a global or multi-regional presence. Some of the most prominent frameworks include the European Union Agency for Cybersecurity (ENISA), which provides resources for CTI sharing, such as a platform for sharing cyber threats among EU member states; the Asia-Pacific Regional Cyber Threat Intelligence Sharing Platform (APTISP), which facilitates CTI sharing among countries in the Asia-Pacific region; the Organization of American States (OAS), which has initiatives aimed at promoting CTI sharing in the Americas; and the African Union Cyber Security Expert Group (AUCSEG), which works towards enhancing cooperation and information sharing among African countries in the field of cybersecurity.

CTI production and sharing at the regional level can play an important role in fostering regional collaboration among states. In the instance of the European Union, ENISA developed a Joint Cyber Unit in 2019 with the goal of real-time information exchange across nation-states [41]. CTI sharing is regarded as crucial for preventing zero-day attacks.

3.5.2 Industry-Specific CTI Frameworks

In recent times, there has been a growing trend towards a proactive approach in addressing the increasing cyber risks faced by different sectors. This has resulted in the establishment of Information Sharing and Analysis Centres (ISACs) that cater to certain industries. ISACs are organizations that facilitate the sharing of CTI among members of a specific industry or sector. ‘’ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency’’ [42]. According to [43] most of the challenges with ISACs sharing revolves around lack of trust and incentives for sharing especially in the competitive financial sector environment, which could lead to ‘free riding behaviour’, where organizations fail to participate in CTI sharing. ISACs function as collaborative platforms where firms within a specific industry convene to exchange crucial cybersecurity threat intelligence. The recognition of this paradigm change involves an understanding of the unique characteristics and weaknesses within different sectors, which necessitate customized strategies for protecting essential infrastructure. The Financial sector has one of the earliest and more mature sharing frameworks especially in the United States and Europe through frameworks like the NIST (National Institute of Standards) and European Financial Services (FS-ISAC) [25]. Other notable industries or sectors with ISACs include Health, automobile, and the Electricity Subsector. This phenomenon serves as a demonstration of a deliberate shift towards a cybersecurity partnership that is focused on certain sectors, so validating the idea that customized frameworks for sharing information are crucial elements in strengthening the ability of industries to withstand ever-changing cyber-attacks.

3.5.3 Proprietary CTI Frameworks

Proprietary CTI frameworks, developed and owned by individual organizations or vendors, are typically closed-source platforms designed for commercial purposes. Examples of such proprietary frameworks include ThreatConnect, Defense Intelligence Platform, Palo Alto Networks Cortex XDR, IBM X-Force Threat Intelligence, and Cisco Talos Intelligence. Additionally, open-source proprietary CTI frameworks such as MISP (Malware Information Sharing Platform) and OpenCTI also exist in this category. These proprietary CTI frameworks often incorporate Threat Intelligence Platforms (TIPs), which are specialized software systems designed to facilitate the collection, processing, analysis, production, deployment, and integration of internal and external threat intelligence. Despite the existence of various platforms, finding a comprehensive solution for defense based on threat intelligence remains a challenge due to the divergent focuses of these platforms. As a result, no "one size fits all" platform exists, and organizations must tailor their approach based on their specific requirements [45].

3.6 CTI Sharing Formats

The dissemination of intelligence varies based on the nature of the information and its level of urgency [29]. Currently CTI sharing among organizations is mainly being performed through informal procedures such as email or social media, and reports [46, 29]. While this can still serve as exchange mechanisms, there is a shift towards formal, structured and platform-centered approaches to CTI sharing. This is because the structured CTI formats limit ambiguity and support automation. CTI formats further contain favourable characteristics such as serialization rules [47]. According to [48] CTI formats and languages can be categorized into four primary groups: firstly, standards that are explicitly created for CTI representation; secondly, formats designed for specific CTI applications or vendors; thirdly, widely adopted standards not originally intended for CTI representation; and finally, outdated legacy formats often referenced in literature but no longer supported or utilized. Standardizing the formats for sharing CTI reduces the likelihood of degrading the quality of threat data, thereby enabling more effective automated analytics on CTI data [16].

The United States Government and MITRE Corporation have established the most promising and popular protocols. These include the Trusted Automated eXchange of Indicator Information (TAXII) and the Structured Threat Information Expression (STIX) [13]. The STIX Project is described as "a language and serialization format used for exchanging CTI, enabling consistent and machine-readable sharing of CTI among organizations"[49]. STIX defines both the scope of information to be included and how the threat information should be structured. It is a standardized language using JSON (STIX 2.x) to represent structured CTI. The standard aims to provide a comprehensive range of potential CTI applications. It strives to be both expressive and flexible while also being extensible, automatable, and easily readable by humans. Its primary objective is to establish guidelines for information representation rather than prescribing specific sharing methods. STIX is designed to enhance various capabilities, including collaborative threat analysis, automated threat exchange, and automated detection and response. STIX 2.1 defines 18 STIX Domain Objects (SDOs) including Attack Pattern (a type of TTP), Campaign, Course of Action, Grouping, Identity among other and two STIX Relationship Objects (SROs) - relationship and sighting [50]. TAXII "is an application layer protocol for the communication of cyber threat information in a simple and scalable manner"[49]. It was created to specify how the CTI information should be shared. TAXII main objective is to define how the CTI information represented in STIX format can be exchanged over HTTPS [51].

Other well-established languages comprise VERIS, IODEF, OpenIOC, MISP internal format, and IDEA. These languages predominantly utilize JSON, a lightweight data interchange format that is both easily comprehensible to humans and parse-able by machines. VERIS, in particular, offers a standardized format for recording and sharing security-related events. It primarily focuses on the monitoring and detection of internal incident and less on the detection of unanticipated dangers [52]. The Incident Object Description Exchange Format (IODEF) was created by the Internet Engineering Task Force (IETF), which is the primary standardization body for the Internet. This format was introduced in 2007 and is now in its second version. The purpose of its development was to facilitate the automation of communication between Computer Security and Incident Response Centres (CSIRTs). Additionally, it was designed as a language that network components, particularly Intrusion Detection Systems (IDS), could comprehend by using the intermediate format known as IDMEF [53]. OpenIOC is a well-established standard created by Mandiant in the early 2010s and it primarily emphasizes the exchange of actionable IOCs like malware signatures or configuration entries like those found in Microsoft Windows' registry [54].

4. CTI Sharing and Artificial Intelligence Machine Learning

Artificial intelligence (AI) and machine learning (ML) constitute two closely related domains that have witnessed considerable progress in cutting-edge technology. AI pertains to the development of computer systems that exhibit human-like cognitive capabilities, such as the aptitude for learning, reasoning, and problem solving [55]. Conversely, machine learning entails imparting computers with the ability to discern and analyze patterns in data, thereby empowering them to make predictions and derive valuable information without the need for explicit programming [56]. The application of artificial intelligence and machine learning in the analysis of vast amounts of data has demonstrated its effectiveness as a powerful resource, facilitating the efficient processing and synthesis of threat intelligence information, and the generation of actionable insights [57-58]. Machine learning algorithms can automate data acquisition and processing, gather information from multiple sources, and provide context for the activities of malicious actors. These technologies are also facilitating innovative approaches for the efficient distribution and sharing of information related to the analysis of cyber incidents and malware [59].

4.1 Intelligent Intelligence

As previously stated, CTI can be classified into four distinct categories: strategic, operational, tactical, and technical. At each of these levels, CTI serves a distinct purpose. The role of AI/ML in the enhancement of sharing CTI at the different levels of CTI for better decision making has been identified in literature [20,25,60]. The majority of CTI sharing is primarily focused on the sharing of technical data and information at a low-level. This is due to its ease of standardization and its practicality in implementation, as it may be readily utilized by firewalls, gateways, or other appliances of diverse nature that possess indicators of compromise (IOC). The challenge is being able to interpret this into higher-level intelligence, analogous to finding a needle in haystack [20, 61].

Intelligent CTI, which can also be referred to as refined intelligence, is a type of CTI that involves analysed and processed data. This information offers actionable insights to decision-makers, allowing organizations to proactively identify potential threats and vulnerabilities and take measures to mitigate risks and safeguard their assets [62]. By incorporating refined intelligence into CTI, organizations can improve the efficiency and accuracy of their threat detection, reduce false-positive alerts, and make more informed decisions about how to share CTI with relevant parties. According to [17] intelligent CTI means CTI that is meaningful and actionable, so it can be easily understood by both human analysts and machines. [63] urge that intelligent or refined intelligence need to be relevant, actionable, and valuable. In order to improve sharing of more intelligent intelligence in CTI, the use of AI/ML has been proposed. The main aim is to find ways of utilizing AI/ML techniques for more intelligent intelligence sharing.

The context in which intelligence is generated is crucial, as it guarantees that the intelligence is pertinent to the specific organization. One of the significant challenges in intelligent CTI is accurately categorizing and prioritizing potential threats based on their level of severity and probability of occurrence. [64] proposed a system called TriCTI that aims to automatically discover actionable cyber threat intelligence from cybersecurity reports using natural language processing and trigger-enhanced classification models. TriCTI utilizes natural language processing techniques to classify CTI based on campaign stages and incorporates trigger vectors and IOC features to improve performance. The work of [8] presents TIminer, a solution designed to address the difficulties in recognizing unknown IOCs and producing CTI with domain tags for enhanced CTI sharing. The domain recognizer in TIminer is built upon a convolutional neural network (CNN). When implementing CTI sharing, it is important to consider how specific the intelligence is to a particular organization's needs. The following are some of crucial aspects of refined intelligence in CTI [63].

Table 2. Summary of Attributes of intelligent or refined intelligence

No.	Attribute	Meaning
1	Accurate and valuable	Enhancing cybersecurity measures requires focusing on obtaining reliable and accurate information from various data sources, including indicators of compromise (IOCs), vulnerability exploits, and malware deployment techniques.
2	Actionable	Refined intelligence converts raw data into actionable insights, offering clear guidance for decision-making or specific actions to mitigate or respond to threats.
3	Timely	Timely and relevant information enables them to anticipate and counter emerging threats effectively. It facilitates prompt responses, ensuring successful protection against potential risks
4	Contextualization	Contextualizing intelligence is essential for understanding a threat's broader

		implications. This involves linking the threat to known adversaries, common attack techniques, and potential organizational impacts

The table below highlights some of the significant and noteworthy contributions made in the field of intelligent intelligence in CTI research.

Table 3. Significant and noteworthy contributions made in the field of intelligent intelligence in CTI research

Authors	Proposed model/ Framework for CTI Sharing	Summary
64	TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network.	TriCTI, a discovery system, employs trigger-enhanced neural networks to extract actionable cyber threat intelligence (CTI) from unstructured cybersecurity reports, identifying indicators of compromise (IOCs) and mapping them to cyber-attack campaign stages. Utilizing natural language processing (NLP) to detect "campaign triggers," the framework efficiently handles large datasets while maintaining IOC contextual relevance, enabling security professionals to prioritize and mitigate threats with detailed, actionable intelligence.
8	TIminer	TIMiner is a robust framework for automatically extracting and analyzing CTI from social media. Utilizing a convolutional neural network (CNN) based domain recognizer, TIMiner classifies CTIs into domains such as finance, government, education, IoT, and industrial control systems. Additionally, TIMiner employs a hierarchical IOC extraction method, leveraging word embeddings and syntactic dependencies to identify both known and novel IOCs. This approach yields domain-specific CTIs that are more pertinent and actionable for organizations, enhancing CTI sharing effectiveness and enabling personalized threat intelligence dissemination.
75	InTIME: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence	An open-source, integrated framework aids security analysts in identifying, collecting, analyzing, extracting, integrating, and sharing CTI from various online sources, including the clear, deep, and dark web, social networks, and trusted security databases. It automates data acquisition, ranks content based on intelligence potential, uses natural language understanding for entity extraction, and supports CTI management and sharing through standards and intuitive tools. The framework supports the entire threat lifecycle, emphasizing the importance of actionable intelligence in pre-empting cyber threats and enhancing security measures.

4.2 CTI Predictive Analytics

The idea of predictive analytic in CTI sharing has not been adequately explored in earlier surveys. Many surveys have acknowledged the role of ML in providing CTI analysis to discover unknown to known threats using various properties like threat actor skills, motivations, Tactics, Techniques, and Procedures (TTP), and Indicators of Compromise (IoC) [55]. However, CTI predictive analytics especially in the sharing aspect of CTI has not been adequately examined in most CTI sharing surveys. For example, [13, 65] do not directly address predictive analytics but imply its importance in the context of automating CTI processes and generating actionable intelligence, respectively. Predictive analytics, which entails the utilization of historical data and statistical algorithms to anticipate future outcomes, can be a highly beneficial resource in the realm of CTI sharing. Predictive analytics can aid in recognizing potential attack vectors, predicting attacker behaviour, and determining the most effective security measures. Through analysis of huge amounts of data from internal networks as well as external sources, predictive analytics can identify patterns that may suggest a looming cyber-attack. This information can be used proactively to prepare for and possibly prevent such attacks [66].

[13] highlighted the importance of integrating intelligent techniques to automate the detection and prediction of cyberattacks, thereby enhancing the capability of organizations to anticipate and respond to threats. Abel Yeboah-Ofori et.al [67] in their study show that Cyber Supply Chain (CSC) systems can leverage CTI and ML techniques to predict cyber threats and improve overall CSC security, which is crucial for maintaining business continuity and protecting critical assets. The study found that integrating CTI with ML techniques can

effectively predict cyberattacks and identify vulnerabilities in CSC systems. Their experiments revealed that spyware/ransomware and spear phishing are the most predictable threats. The ML models achieved a total accuracy of 85% in threat prediction, with LR and SVM producing the highest accuracy.

Saeed et al. [45] emphasize the significance of CTI in enhancing organizational defenses by processing, assessing, and disseminating information about potential cyber risks and opportunities. They underline the utilization of machine learning techniques to analyze CTI data, forecast threats, and improve cybersecurity. For instance, they showcase the application of logistic regression, support vector machines, random forests, and decision trees to forecast malware attacks. Furthermore, they illustrate how CTI can be employed to configure intrusion detection systems (IDS) based on established attack patterns and the behaviours of threat actors.

5. CTI Sharing & Trust

To foster sharing and consuming, a CTI sharing environment must effectively balance the interplay between privacy, trust, and accountability. Privacy can be defined as the ability or inability of a recipient to associate certain shared information with the true identity of the individual or entity that shared it. Revealing intelligence in an identifiable manner can lead to the risk of reputational damage, which is a significant barrier that hinders organizations from participating in CTI sharing. Consequently, ensuring anonymity during sharing becomes an essential consideration [20].

Trust can be defined as the ability of a consumer to have confidence in the information that they receive. This phenomenon fosters a sense of trust and reliance between producers and users of CTI within sharing networks. Trust is widely regarded as the most challenging element in the CTI sharing environment. In contrast to concerns about privacy, the criteria used to establish a trust relationship between producers and customers typically require a linkage to the authentic identity of the producer [68]. Building trust can be hastened through ongoing communication via scheduled in-person meetings, phone calls, or social media [18]. Before sharing their own CTI, most organizations face the challenge of determining how to use the CTI information themselves, i.e., comprehending the information and implementing its remedy [13]. Many organizations remain reluctant to share their data, primarily due to the absence of incentives. However, they expect to receive knowledge from data shared by other peers in their community. Building trust can be helpful in encouraging sharing. According to [2] the exact meaning of trust is not clear, suggesting that it is not an absolute requirement, but is fostered by factors like quality and confidentiality of the shared CTI. Fair sharing practices and avoiding adversarial usage of CTI, like utilizing information against the provider or generating fake CTI to sow confusion will positively impact trust among sharing partners.

5.1 Trust Models in Digital Environments

Trust is an essential aspect of the digital world, and various models and mechanisms are utilized to establish and maintain it. These models have been developed to address different challenges and are tailored to specific contexts, based on analytical and theoretical approaches that consider factors such as beliefs, experience, and authenticity [69]. Literature has identified several trust models, including reputation-based models, trust management systems, contextual trust models, Public Key Infrastructure (PKI)-based trust models, and Blockchain-Based Trust Models. Reputation-based trust models are designed to evaluate the reliability of entities by examining their past behavior and feedback from other participants. For example, the model proposed by [70] adjusts trust levels dynamically as entities continue to interact, making it effective in large-scale, distributed networks where direct trust relationships are impractical. Trust management systems provide a structured approach to trust evaluation and decision-making in distributed environments. The TRUST framework, developed by [71], exemplifies this by offering a systematic method for defining and enforcing trust policies across an organization. This is crucial where consistent and transparent trust management is needed to ensure secure information exchange.

In contrast, contextual trust models emphasize the importance of situational factors in trust decisions. These models assess trust based on the specific context of the interaction, recognizing that trust is not static but varies according to the nature of the information, the roles of the participants, and the environment in which the interaction takes place [72]. Public key infrastructure (PKI)-based models rely on digital certificates and a hierarchical trust structure to authenticate participants and safeguard the information exchange. By utilizing trusted certificate authorities, PKI offers a robust framework for ensuring that only authorized entities can access sensitive information [73]. Blockchain-based models leverage the decentralized and immutable nature of blockchain technology to guarantee the integrity and authenticity of shared intelligence. The transparency provided by blockchain makes it particularly effective for maintaining trust in distributed networks [74].

5.2 Accountability in CTI Sharing

Accountability refers to the ability of a sharing environment to build robust governance mechanisms for the effective management of shared CTI, encompassing the capability to hold accountable those users who engage in deceptive sharing. This, consequently safeguards the integrity of the disseminated intelligence. Much like trust, accountability relies on the disclosure of the genuine identity of a contributor, particularly those who have made a harmful contribution [75]. It can be inferred from the aforementioned that privacy, trust, and accountability exist in a paradoxical relationship. Producers of intelligence typically desire anonymity when disseminating information, while consumers necessitate verifiable evidence that the intelligence they obtain originates from a reliable source.

5.3 Elements of Trust in CTI Sharing

Trust among CTI-sharing partners is a critical factor in promoting effective sharing practices. Trust is a crucial aspect, as the success of CTI sharing depends on the confidence that the shared information is accurate, relevant, and has not been maliciously altered [32, 35, 47, 76]. Indeed, the lack of trust relationships is one of the major barriers to extensive and effective CTI threat sharing [13, 16, 18, 77]. The elements of trust in CTI-sharing have not been fully explored in many CTI-sharing research surveys [17, 34] and may require more research. The common aspects explored in relation to trust include quality, standardization, and privacy of the CTI data. [2] discussed trust urging that it is not a “true requirement” but rather a result of a combination of various factors chief among them confidentiality. Although confidentiality does play a role in preventing misuse, we urge that it is crucial to acknowledge that it is not a complete substitute for trust. Confidentiality measures may prove insufficient or be bypassed, at which point trust acts as the ultimate protection. Aspects of CTI quality include accuracy, relevance, timeliness, completeness, and indigestibility. These elements help to reduce information overload and false positives [13, 27,78].

According to [79], empirical evidence suggests that the dissemination of inaccurate information and delayed sharing of threat data can erode trust among participating entities, emphasizing the significance of data quality and timeliness in enhancing trust in the sharing of CTI. Although standardization of CTI may not directly impact trust, it is considered a facilitator of efficient CTI exchange, as it promotes interoperability for collaborative engagement especially in automated CTI sharing environments [63]. Standardization promotes timely exchange of CTI as unnecessary data transformations is be avoided [19-7]. Standardization initiatives like STIX and TAXII are acknowledged for their role in facilitating structured and machine-readable CTI exchange [13].

Trust is a critical aspect of information sharing, as exchange often involves sensitive data that could potentially harm the sharing entity if mishandled [13, 37]. In this context, ensuring data security is paramount in fostering trust in CTI sharing. To address the sensitive nature of shared information, privacy-preserving mechanisms have been implemented to minimize the risk of data exposure. [16] highlight the tension between data sharing and confidentiality, proposing a framework that utilizes privacy-enhancing technologies and federated processing to mitigate potential risks of data exposure. Privacy-preserving machine learning techniques enable the training of machine learning models on sensitive data without the need to disclose the data.

There are human factors that also contribute to enhancing trust in sharing. For example, humans may sometimes refrain from disclosing information about potential threats due to concerns about the risks associated with sharing such knowledge [13]. Familiarity between sharing parties that could be established beforehand can increase trust among the sharing parties [18]. This trust relationship building can be hastened through ongoing communication via scheduled in-person meetings, phone calls, or social media [18]. According to Pala, Ali, and Jun Zhuang [77], formal agreements or contracts can be effective in fostering trust and decreasing risks associated with information sharing. By establishing clear guidelines and assurances regarding data protection, privacy, and liability, it is possible to build trust and mitigate concerns about potential negative outcomes.

Trust is also influenced by the mechanisms in place to ensure the confidentiality and integrity of the information shared through the Threat Intelligence Platform (TIP) being used to exchange CTI [16, 28, 78]. The confidence of the sharing parties in the TIP positively influences the trust in sharing of CTI. As trust is increased the sharing of quality CTI data is increased which in turn raises the reputation of the TIP positively raising trust in the TIP and vice versa. The confidence in the TIP is heavily influenced by the data security of the TIP [81]. Data security in TIPs range from data access mechanisms to data encryption in the transmission and storage of the CTI data [12,79]. Transparent sharing practices and strong data security protocols, ensuring that shared intelligence is both useful and trustworthy [18]. Adequate training and expertise in using the TIPs platforms is necessary to interpret and share high-quality threat intelligence effectively. In their work [13] presents a new taxonomy to establish trust among stakeholders in CTI sharing environments, focusing on attributes such as sharing activity, stakeholder rating, and industry affiliation. They urge that trust can be established through internal vetting processes or manual trust-building among stakeholders. There are limitations of manual trust building, hence there is need to explore automated trust mechanisms that can complement or replace manual processes, making the system more scalable and less prone to human error. [16] highlights that organizations are often reluctant to share sensitive threat data due to concerns over negative publicity, and the potential misuse of shared information by competitors. To mitigate these issues, they proposed a solution that entails applying context-sensitive and fine-grained access control measures to safeguard the privacy and confidentiality of the data.

As mentioned earlier the application of blockchain technology has been proposed as a means to address the challenges associated with traditional CTI sharing models. This technology is particularly useful in addressing issues of privacy, trust, accountability, validity, and auditability within the CTI sharing process. To enhance trust among participants, innovative blockchain-based frameworks and consensus algorithms have been proposed, such as the "Proof-of-Reputation" (PoR) consensus algorithm introduced by [32]. This algorithm is designed to ensure credible transactions and mitigate the risk of false reporting by compromised members. Homan et al. 2019 [81] discusses the use of smart contracts and fabric channels to overcome trust barriers and privacy issues and ensure secure CTI dissemination. Chatziamanetoglou et al. 2023 [82] propose a blockchain-based system architecture that utilizes a reputation and trust-based mechanism for evaluating CTI feeds, ensuring data integrity and excluding untrustworthy evaluation peers. The system evaluates, stores, and shares CTI while assessing its quality against predefined standards. The proposed system employs a reputation- and trust-based method for selecting validators and evaluating CTI inputs.

Trust is intrinsically linked to the notion of audit, and the distributed ledger capabilities of blockchain technology facilitate the reliable and trustworthy sharing of threat intelligence while enabling the auditing of the source of the intelligence. The incorporation of blockchain technology in threat intelligence sharing can enhance trust and accountability by presenting a transparent and tamper-proof record of all transactions and interactions. By harnessing blockchain technology, organizations can confirm the integrity and authenticity of threat intelligence, as well as the accuracy of the sources providing the intelligence. This ultimately results in better decision-making and more effective threat management. [83] proposed a framework for enhancing trust in CTI sharing by addressing key challenges related to trustworthiness and reliability. The authors propose a framework that integrates distributed ledger technology (DLT) with the existing Malware Information Sharing Platform (MISP) to ensure the provenance, accountability, and auditability of shared threat intelligence. There are several blockchain technology-based CTI sharing mechanism to tackle to problem of accountability and auditability. [82] emphasized that while blockchain technology offers numerous potential benefits to the cybersecurity community through its immutability, availability, and scalability, realizing these advantages depends on factors such as the development and implementation of the blockchain platform, integration with existing systems, and stakeholder cooperation and acceptance within the CTI community.

Table 4. Attributes of Trust in CTI Sharing

No.	Attribute	Meaning
1	Quality	In cyber threat intelligence sharing, quality pertains to the accuracy, relevance, and timeliness of the information
2	Confidentiality	Confidentiality ensures that shared intelligence is accessible solely to authorized individuals and entities, thereby maintaining trust among partners by safeguarding sensitive information from unauthorized access and potential misuse.
3	Auditability	Auditability involves tracking and reviewing sharing activities to ensure adherence to standards and policies, including maintaining detailed logs of access information. It verifies appropriate information sharing, fostering trust through transparency and accountability.
4	Familiarity	Familiarity refers to the understanding and recognition among entities in the intelligence-sharing process. High familiarity can enhance trust, as parties are more likely to trust well-known partners. This trust develops through repeated interactions and established relationships over time.
5	Agreements/ Contracts/Policies	Agreements, contracts, and policies specify the formal terms for sharing cyber threat intelligence, detailing the rights, responsibilities, and expectations of all parties involved
6	Transparency	Transparency entails openly communicating the policies, procedures, and activities associated with intelligence sharing. This involves clarifying what

No.	Attribute	Meaning
		information is shared, its usage, and any monitoring practices. Transparency fosters trust by ensuring all parties are informed about and consent to the sharing practices, thereby reducing uncertainties and potential conflicts

As discussed in this survey, trust in CTI sharing especially in automated environments, is crucial for maintaining the integrity and dependability of shared intelligence, which in turn enables informed security decisions. By fostering participants confidence, trust encourages more organizations to share valuable threat data for comprehensive collective defence [24, 37]. Many different mechanisms have been proposed as discussed in this survey to foster trust, and increase CTI sharing participation. However, despite these efforts CTI sharing is not widely adopted in many sectors [25]. It is worthwhile to explore the role of sector specific sharing mechanisms in fostering trust for increased CTI sharing. Sector-specific sharing mechanisms could offer a promising solution by addressing unique sector needs, fostering collaboration, innovation, and establishing robust trust mechanisms tailored to sector-specific regulations and threat landscapes, thereby enhancing the overall efficacy of CTI sharing.

6. CONCLUSION

This literature review underscores the importance of cyber threat intelligence (CTI) sharing in building a strong cybersecurity posture and examines the obstacles associated with CTI sharing. Our review addresses three key gaps identified in previous CTI sharing research: the use of intelligent intelligence, predictive analytics, and trust-building elements in CTI sharing. We emphasize the potential of machine learning to enhance intelligence through refined data analysis and predictive analytics to anticipate attack patterns, thereby enabling proactive measures. Additionally, we explored the factors that contribute to trust in CTI sharing, demonstrating how trust can be established and maintained in CTI sharing collaborative environments and stated the need to explore how sector-specific sharing mechanisms can address trust issues.

References

[1] Machado da Silva, R., Costa Gondim, J. J., & de Oliveira Albuquerque, R. (2022, November). Methodology to Improve the Quality of Cyber Threat Intelligence Production Through Open-Source Platforms. In International Conference on Computer Science, Electronics and Industrial Engineering (CSEI) (pp. 86-98). Cham: Springer Nature Switzerland.

[2] Jesus, V., Bains, B., & Chang, V. Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence. IEEE Transactions on Engineering Management. (2023).

[3] Gartner. Definition: Threat intelligence. https://www.gartner. com/en/documents/2487216/definition-threat-intelligence. (2013).

[4] F. Rehman, S. Hashmi "Enhancing Cloud Security: A Comprehensive Framework for Real-Time Detection, Analysis and Cyber Threat Intelligence Sharing", Advances in Science, Technology and Engineering Systems Journal, vol. 8, no. 6, pp. 107-119 (2023).

[5] Althamir, M. A., Boodai, J. Z., & Rahman, M. H. (2023, February). A Mini Literature Review on Challenges and Opportunity in Threat Intelligence. In 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) (pp. 558-563). IEEE.

[6] Trocoso-Pastoriza, J. R., Mermoud, A., Bouyé, R., Marino, F., Bossuat, J. P., Lenders, V., & Hubaux, J. P. Orchestrating collaborative cybersecurity: a secure framework for distributed privacy-preserving threat intelligence sharing. arXiv preprint arXiv:2209.02676. (2022).

[7] Bromander, S., Muller, L. P., Eian, M., & Jøsang, A. Examining the" Known Truths" in Cyber Threat Intelligence–The Case of STIX. In International Conference on Cyber Warfare and Security (pp. 493-XII). Academic Conferences International Limited. (2020).

[8] Zhao, J., Yan, Q., Li, J., Shao, M., He, Z., & Li, B. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Computers & Security, 95, 101867. (2020).

[9] A reference model for cyber threat intelligence (CTI) systems G. Sakellariou, P. Fouliras, I. Mavridis and P. Sarigiannidis Electronics 2022 Vol. 11 Issue 9 Pages 1401

[10] Villalón-Huerta, A., Ripoll-Ripoll, I., & Marco-Gisbert, H. Key requirements for the detection and sharing

of behavioral indicators of compromise. Electronics, vol. 11, no. 3, 416. (2022).

[11] Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 1, pp. 371-379 (2018).

[12] Cinar, B., & Umber, J. . ‘Cyber threat intelligence: Current trends and future perspectives. J. Eng. Res. Rep, vol. 25, no. 4, pp. 91-105. (2023).

[13] Cyber threat intelligence sharing: Survey and research directions Thomas D. Wagner , Khaled Mahbub , Esther Palomar , Ali E. Abdallah

[14] Dykstra, J., Fante, M., Donahue, P., Varva, D., Wilk, L., & Johnson, A. . Lessons from Using the {I-Corps} Methodology to Understand Cyber Threat Intelligence Sharing. In 12th USENIX Workshop on Cyber Security Experimentation and Test (CSET 19). (2019).

[15] Berndt, A., & Ophoff, J. Exploring the value of a cyber threat intelligence function in an organization. In Information Security Education. Information Security in Action: 13th IFIP WG 11.8 World Conference, WISE 13, Maribor, Slovenia, September 21–23, 2020, Proceedings 13 (pp. 96-109). Springer International Publishing. (2020).

[16] Tounsi, W., & Rais, H. . A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, 72, pp. 212-233. (2018).

[17] Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., & Foo, E. . Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. Journal of Information Security and Applications, 83, 103786. (2024).

[18] Johnson, C.S., Badger, M.L., Waltermire, D.A., Snyder, J., & Skorupka, C. . Guide to Cyber Threat Information Sharing. Technical Report NIST Special Publication (SP) 800–150. National Institute (2016).

[19] Schlette, D. Cyber threat intelligence. In Encyclopedia of Cryptography, Security and Privacy (pp. 1-3). Berlin, Heidelberg: Springer Berlin Heidelberg. (2021).

[20] Dunnett, K., Pal, S., & Jadidi, Z. Challenges and Opportunities of Blockchain for Cyber Threat Intelligence Sharing. Secure and Trusted Cyber Physical Systems: Recent Approaches and Future Directions, pp. 1-24. (2022).

[21] Kris Oosthoek & Christian Doerr Cyber Threat Intelligence: A Product Without a Process? International Journal of Intelligence and CounterIntelligence, 34:2, pp. 300-315, doi: 10.1080/08850607.2020.1780062 (2021).

[22] Bromander, S., Swimmer, M., Swimmer, M., Pijnenburg Muller, L., & Borg, F. . Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange. doi: 10.1145/3458027 (2021).

[23] Parmar, M., & Domingo, A. (2019, November). On the Use of Cyber Threat Intelligence (CTI) in Support of Developing the Commander's Understanding of the Adversary. In MILCOM pp. 2019-2019 IEEE Military Communications Conference (MILCOM) (pp. 1-6). IEEE.

[24] Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. Journal of Network and Systems Management, vol. 31, no. 1, 3. (2023).

[25] Balson, D., & Dixon, W. (2020, October). Cyber information sharing: building collective security. World Economic Forum.

[26] Gong, N. Barriers to adopting interoperability standards for cyber threat intelligence sharing: an exploratory study. In Intelligent Computing: Proceedings of the 2018 Computing Conference, Volume 2 (pp. 666-684). Springer International Publishing. (2019).

[27] James Kotsias, Atif Ahmad & Rens Scheepers Adopting and integrating cyber-threat intelligence in a commercial organisation, European Journal of Information Systems, 32:1, pp. 35-51, doi: 10.1080/0960085X.2022.2088414 (2023).

[28] Stojkovski, B., Lenzini, G., Koenig, V., & Rivas, S. (2021, December). What’s in a cyber threat intelligence sharing platform? A mixed-methods user experience investigation of MISP. In Proceedings of the 37th Annual Computer Security Applications Conference (pp. 385-398).

[29] Brown, R., & Lee, R. M. 2021 sans cyber threat intelligence (cti) survey. In Tech. Rep. SANS Institute. (2021).

[30] Zibak, A., & Simpson, A. (2019, June). Towards better understanding of cyber security information sharing.

In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (pp. 1-8). IEEE.

[31] Alsmadi, I. . The NICE cyber security framework: Cyber security intelligence and analytics. Springer Nature. (2023).

[32] Zhang, X., Miao, X., & Xue, M. A Reputation-Based Approach Using Consortium Blockchain for Cyber Threat Intelligence Sharing. Security and Communication Networks, vol. 2022, no. 1, 7760509. (2022).

[33] Tongtong Jiang, Guowei Shen, Chun Guo, Yunhe Cui, Bo Xie, BFLS: Blockchain and Federated Learning for sharing threat detection models as Cyber Threat Intelligence,Computer Networks,Volume 224 2023, 109604, ISSN pp. 1389-1286.

[34] Stojkovski, B., & Lenzini, G. (2021, July). A workflow and toolchain proposal for analyzing users' perceptions in cyber threat intelligence sharing platforms. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 324-330). IEEE.

[35] Chatziamanetoglou, D., & Rantos, K. Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. Computers, vol. 13, no. 3, 60. (2024).

[36] Ma, X., Yu, D., Du, Y., Li, L., Ni, W., & Lv, H. A Blockchain-Based Incentive Mechanism for Sharing Cyber Threat Intelligence. Electronics, vol. 12, no. 11, 2454. (2023).

[37] Dunnett, K., Pal, S., Putra, G. D., Jadidi, Z., & Jurdak, R. (2022, December). A trusted, verifiable and differential cyber threat intelligence sharing framework using blockchain. In 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 1107-1114). IEEE.

[38] Riesco, R., Larriva-Novo, X., & Villagrá, V. A. Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of information. Telecommunication Systems, vol. 73, no. 2, pp. 259-288. (2020).

[39] Menges, F., Putz, B., & Pernul, G. DEALER: decentralized incentives for threat intelligence reporting and exchange. International Journal of Information Security, vol. 20, no. 5, pp. 741-761. (2021).

[40] Gong, S., & Lee, C. Blocis: blockchain-based cyber threat intelligence sharing framework for sybil-resistance. Electronics, vol. 9, no. 3, 521. (2020).

[41] Sakellariou, G., Fouliras, P., Mavridis, I., & Sarigiannidis, P. A reference model for cyber threat intelligence (CTI) systems. Electronics, vol. 11, no. 9, 1401. (2022).

[42] National Council of ISACs. . Natlcouncilofisacs. https://www.nationalisacs.org/ (2019).

[43] Kollars, N. A., & Sellers, A. Trust and information sharing: ISACs and US Policy. Journal of Cyber Policy, vol. 1, no. 2, pp. 265-277. (2016).

[44] de Melo e Silva, A., Costa Gondim, J. J., de Oliveira Albuquerque, R., & García Villalba, L. J. A methodology to evaluate standards and platforms within cyber threat intelligence. Future Internet, vol. 12, no. 6, 108 (2020).

[45] Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, vol. 23, no. 16, 7273. (2023).

[46] W. Maina, L. Nderu and T. Mwalili, "A Smart Contract Approach to Cyber Threat Intelligence Sharing in Kenya," 2022 IST-Africa Conference (IST-Africa), Ireland, 2022, pp. 1-10, doi: 10.23919/IST-Africa56635.2022.9845603

[47] Schlette, D., Caselli, M., & Pernul, G. A comparative study on cyber threat intelligence: The security incident response perspective. IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2525-2556. (2021).

[48] Ramsdale, A., Shiaeles, S., & Kolokotronis, N. A comparative analysis of cyber-threat intelligence sources, formats and languages. Electronics, vol. 9, no. 5, 824 (2020).

[49] Cyber Threat Intelligence Technical Committee. Oasis-Open.github.io. https://oasis-open.github.io/cti-documentation/ (2023).

[50] Introduction to STIX. . Github.io. https://oasis-open.github.io/cti-documentation/stix/intro (2016).

[51] Albakri, A., Boiten, E., & De Lemos, R. (2018, August). Risks of sharing cyber incident information. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-10).

[52] Vocabulary for Event Recording and Incident Sharing (VERIS), Accessed: Nov. 9, 2023. [Online]. Available: http://veriscommunity.net

[53] Danyliw, R. The incident object description exchange format version 2 (No. rfc7970). (2016).

[54] OpenIOC: Back to the Basics. . Mandiant. (2021).

[55] Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. . A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access. (2024).

[56] Gonaygunta, H. Machine learning algorithms for detection of cyber threats using logistic regression. Department of Information Technology, University of the Cumberlands. (2023).

[57] Montasari, R., Carroll, F., Macdonald, S., Jahankhani, H., Hosseinian-Far, A., & Daneshkhah, A. Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. Digital Forensic Investigation of Internet of Things (IoT) Devices, pp. 47-64. (2021).

[58] Naseer, I. . Machine Learning Applications in Cyber Threat Intelligence: A Comprehensive Review. The Asian Bulletin of Big Data Management, vol. 3, no. 2, pp. 190-200. (2023).

[59] Kanca, A. M., & SAĞIROĞLU, Ş. (2021, December). Sharing cyber threat intelligence and collaboration. In 2021 International Conference on Information Security and Cryptology (ISCTURKEY) (pp. 167-172). IEEE.

[60] Samtani, S., Abate, M., Benjamin, V., & Li, W. Cybersecurity as an industry: A cyber threat intelligence perspective. The Palgrave Handbook of International Cybercrime and Cyberdeviance, pp. 135-154. (2020).

[61] Ibrahim, A., Thiruvady, D., Schneider, J. G., & Abdelrazek. The challenges of leveraging threat intelligence to stop data breaches. Frontiers in Computer Science, 2, 36. (2020).

[62] Kant, N., & Amrita. (2023, June). Cyber Threat Intelligence (CTI): An Analysis on the Use of Artificial Intelligence and Machine Learning to Identify Cyber Hazards. In International Conference on Recent Developments in Cyber Security (pp. 449-462). Singapore: Springer Nature Singapore.

[63] Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1748-1774. (2023).

[64] Liu, J., Yan, J., Jiang, J. et al. TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network. Cybersecurity 5, 8 https://doi.org/10.1186/s42400-pp. 022-00110-3 (2022).

[65] Sauerwein, C., & Pfohl, A. Towards Automated Classification of Attackers' TTPs by combining NLP with ML Techniques. arXiv preprint arXiv:2207.08478. (2022).

[66] Hassan, M. (2023, September 7). Predictive Analytics in Cyber Security - Challenges and Threats. Research Method. https://researchmethod.net/predictive-analytics-cyber-security

[67] Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. . Cyber threat predictive analytics for improving cyber supply chain security. IEEE Access, 9, pp. 94318-94337. (2021).

[68] Schaberreiter, T., Kupfersberger, V., Rantos, K., Spyros, A., Papanikolaou, A., Ilioudis, C., & Quirchmayr, G. (2019, August). A quantitative evaluation of trust in the quality of cyber threat intelligence sources. In Proceedings of the 14th International Conference on Availability, Reliability, and Security (pp. 1-10).

[69] Pradhan, P., & Kumar, V. Trust management models for digital identities. International Journal of Virtual Communities and Social Networking (IJVCSN), vol. 8, no. 4, pp. 1-24. (2016).

[70] Yu, B., Singh, M. P., & Sycara, K. (2004, August). Developing trust in large-scale peer-to-peer systems. In IEEE First Symposium onMulti-Agent Security and Survivability, 2004 (pp. 1-10). IEEE.

[71] Blaze, M., Feigenbaum, J., & Lacy, J. (1996, May). Decentralized trust management. In Proceedings 1996 IEEE symposium on security and privacy (pp. 164-173). IEEE.

[72] Grandison, Tyrone, and Morris Sloman. "A survey of trust in internet applications." IEEE Communications Surveys & Tutorials 3, no. 4: pp. 2-16. (2000).

[73] Albarqi, A., Alzaid, E., Al Ghamdi, F., Asiri, S., & Kar, J. Public key infrastructure: A survey. Journal of

Information Security, vol. 6, no. 01, 31. (2014).

[74] Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE security and privacy workshops (pp. 180-184). IEEE.

[75] Shin, B., & Lowry, P. B. A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. Computers & Security, 92, 101761 (2020).

[76] Homan, D., Shiel, I., & Thorpe, C. (2019, June). A new network model for cyber threat intelligence sharing using blockchain technology. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-6). IEEE.

[77] Pala, A., & Zhuang, J. Information sharing in cybersecurity: A review. Decision Analysis, vol. 16, no. 3, pp. 172-196. (2019).

[78] Mavzer, K. B., Konieczna, E., Alves, H., Yucel, C., Chalkias, I., Mallis, D., ... & Sanchez, L. A. G. (2021, July). Trust and quality computation for cyber threat intelligence sharing platforms. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 360-365). IEEE.

[79] Jin, B., Kim, E., Lee, H., Bertino, E., Kim, D., & Kim, H. Sharing cyber threat intelligence: Does it really help?.

[80] Bauer, S., Fischer, D., Sauerwein, C., Latzel, S., Stelzer, D., & Breu, R. (2020, January). Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In HICSS (pp. 1-10).

[81] Homan, D., Shiel, I., & Thorpe, C. (2019, June). A new network model for cyber threat intelligence sharing using blockchain technology. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-6). IEEE.

[82] Chatziamanetoglou, D., & Rantos, K. Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus. Security and Communication Networks, vol. 2023, no. 1, 3303122. (2023).

[83] Preuveneers, D., Joosen, W., Bernal Bernabe, J., & Skarmeta, A. Distributed security framework for reliable threat intelligence sharing. Security and Communication Networks, vol. 2020, no. 1, 8833765. (2020).