Vokasi Unesa Bulletin of Engineering, Technology and Applied Science (VUBETA)
https://journal.unesa.ac.id/index.php/vubeta
Vol. 2, No. 2, 2025, pp. 227~242 DOI: 10.26740/vubeta.v2i2.36031
ISSN: 3064-0768

A Survey on Categorization of Threat Intelligence and Trust-Based Sharing Strategies on Cyber Attack

Nureni Ayofe Azeez[1*], Tajudeen Abdulquadri Opeyemi[2]
[1,2]Department of Computer Sciences, Faculty of Science, University of Lagos, Nigeria

Article Info

Article history:

Received November 17, 2024
Revised January 09, 2025
Accepted May 15, 2025

Keywords:

Threat Intelligence
Cybersecurity
Trust-based Sharing
Classification
Vulnerability

ABSTRACT

Threat Intelligence (TI) refers to knowledge derived from analyzing current and potential cyber threats, including their context, mechanisms, and indicators of compromise. By understanding adversaries ' tactics, techniques, and procedures, TI empowers organizations to proactively detect, prevent, and counter cyber threats. Given cyberattacks' increasing frequency and sophistication, stratifying and categorizing TI remains challenging, particularly in building trust for secure information sharing among organizations. This research addresses these challenges through a survey on TI categorization and trust-based sharing mechanisms. The study is expository research that employs quantitative research methodology. The study incorporates a systematic literature review to explore TI classification, methodologies, and its effectiveness in mitigating cybersecurity vulnerabilities. Findings reveal that organizations leveraging advanced TI methods, such as machine learning and behavioral analytics, achieve up to a 60% reduction in threat detection and response times. Furthermore, trust-based sharing initiatives such as Information Sharing and Analysis Centers (ISACs) and standardized frameworks like Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) enhance collaborative defense capabilities by 65%. The study concludes that integrating standardized sharing protocols, advanced analytics, and machine learning can significantly bolster cybersecurity defenses. It recommends global standardization of TI practices, incentivizing participation in information-sharing communities, and investing in workforce training to optimize TI deployment. These findings allow practitioners, policymakers, and researchers to strengthen cybersecurity frameworks.

1. INTRODUCTION

Threat intelligence is the knowledge mined from evidence of current or potential cyber threats that can help take defensive measures. It is based on context, mechanisms, indicators of compromise, the possible impact, and an effective recommendation on counteracting. It means threat intelligence makes your organization understand more about "who, what, why, and how" somebody is attacking, or it may attack your digital assets so that you could defend yourself proactively against them [1]. The concept of threat intelligence has evolved significantly with time. Today, threat intelligence, threat actor profiling, malware analysis, and continuous monitoring of the cyber threat landscape also come under it. This means an increase in the complexity of the cyber threat and the vital role threat intelligence plays in any modern cybersecurity strategy.

With the growth of internet-connected devices and the increasing sophistication of cyber attackers, safeguarding digital assets for today's organizations from a myriad of sophisticated cyber threats that evolve in a rapidly changing cybersecurity landscape is an unprecedented challenge. Traditional security measures

*Corresponding Author
Email: nurayhn1@gmail.com

are not enough to effectively protect against such modern cyber threats. According to Galinec et al [2], modern cyber threats are grave challenges to individuals, organizations, and nations all over the globe; their ever-changing nature creates excellent challenges. With growing frequency, sophistication, and increasingly dire impact, cyber-attacks put practical threat intelligence and sharing strategies at a growing premium [3]. Threat intelligence has become a valuable element of present-day cybersecurity strategies that offer knowledge to organizations about emerging threats and enable them to enhance their systems of defense against threats evolving in the cyber world. Therefore, proper knowledge is crucial about adversaries' tactics, techniques, and procedures so that defenders can quickly identify, mitigate, and respond to any potential attack by taking proactive measures.

Trust is the most important aspect of an organization that wants to share threat intelligence. Within cybersecurity, trust is more than information accuracy and reliability; it also implies the honest and benign intentions of the exchanging parties [4]. Finding common ground among multiple security stakeholders, government offices, private companies, and cybersecurity researchers is an essential step towards standardizing the exchange of information between organizations. Nevertheless, trust is not easily earned, especially in today's world, which is surrounded by uncertainty, competition, and adversarial relationships. That is why effective and secure share-based relations are based on technical, organizational, legal, and social factors. Consequently, comprehending the dynamics of trust in threat intelligence sharing is crucial in increasing the resilience of cybersecurity systems in absolute and collective terms. In essence, when trust relationships as well as sharing of such threat intelligence is done securely and in confidence, organizations can improve their collective defense postures against cyber threats [5].

The justification of this survey lies in its potential to give more understanding of threat intelligence categorization and trust-based sharing strategies in the context of cyberattacks. As cyber threats evolve in complexity and scale, there is a pressing need for effective mechanisms to promptly identify, assess, and respond to these threats. The essential aspect of examining how organizations categorize and prioritize different types of threat intelligence aims to provide insights into best practices for optimizing resource allocation and decision-making processes in cybersecurity operations. Furthermore, by investigating the role of trust in facilitating information sharing among stakeholders, this survey seeks to identify strategies for overcoming barriers to collaboration and fostering a culture of collective defense. The findings of this research have practical implications for cybersecurity practitioners, policymakers, and researchers alike, offering actionable recommendations for enhancing threat intelligence capabilities and strengthening cyber resilience across diverse sectors and domains. Ultimately, this study contributes to the broader goal of safeguarding digital assets, preserving trust in online interactions, and promoting a more secure and resilient cyber ecosystem.

1.1. Problem Statement

Despite the growing recognition of the importance of threat intelligence and information sharing in cybersecurity, there remains a lack of comprehensive understanding regarding the categorization of threat intelligence and the effectiveness of trust-based sharing strategies in mitigating cyberattacks. Organizations face significant challenges in identifying relevant threat intelligence sources amidst the vast evolving cyber threat [6]. Moreover, the reluctance to share sensitive information due to concerns about trust, privacy, and competitive advantage hampers collective efforts to combat cyber threats effectively [7]. As a result, there is a critical need to examine how organizations categorize and prioritize different types of threat intelligence and to explore the factors that influence trust-based sharing initiatives in cybersecurity. It is essential to address this gap to develop evidence-based strategies and policies to enhance cyber resilience and promote collaboration among stakeholders in the fight against cybercrime. Thus, this survey investigates the categorization of threat intelligence and trust-based sharing strategies and their implications for cybersecurity resilience.

1.2. The Articles' Aim and Objectives

This research will survey the categorization of threat intelligence (TI) and trust-based sharing strategies against cyberattacks. This survey seeks to explore the various dimensions of TI, including types, sources, and characteristics. The objectives are as follows:

- To classify and categorize different types of threat intelligence (TI).
- Examine the methodologies and practices associated with Threat intelligence (TI), including data collection, analysis, and dissemination.
- Evaluate the effectiveness of TI in enabling proactive threat detection, incident response, and risk mitigation strategies.

- Identify challenges and barriers hindering the adoption of trust-based sharing strategies in organizational contexts.
- Propose recommendations and strategies for enhancing the utilization and effectiveness of TI in bolstering cybersecurity defences.

2. Literature Review

Threat intelligence is key in strengthening organizational capabilities for proactive detection and response to cyber threats. It therefore allows them to understand what emerging threats look like and the direction attacks appear to take. With threat intelligence, an organization can tell which systems it runs open windows through which attackers can get into its system network, even before it happens [8]. Threat intelligence has considerably shifted in response to the ever-changing nature of cyber threats and the increasing intricacy of the cybersecurity landscape. In earlier times, internal sources such as security logs and incident reports were the primary threat intelligence sources. Nevertheless, with networks becoming more interconnected and digital ecosystems taking shape, organizations have increasingly looked outwards for threat intelligence.

These external sources of information include commercial providers of threat intelligence, open-source intelligence (OSINT) feeds, and information-sharing communities [9]. Additionally, technological advancements like artificial intelligence (AI) and machine learning (ML) have brought an evolution in how people understand threat intelligence by automating the collection, analytics, and sharing of it among different organizations [10]. As a result, these technologies enable organizations to process vast amounts of data within seconds or minutes to track down patterns that may signal danger or departures from normality, which can be converted into helpful real-time advice [11]. This allows organizations to enhance their cyber defense capabilities while avoiding being caught flat-footed by cyber adversaries.

Figure 1 illustrates the possible magnitude of the global threat intelligence market, estimated to be USD 3.02 billion in 2016. The rising importance of intelligence among organizations to effectively predict threats based on available information might propel demand trends over the analysis period. Threat intelligence is integral to contemporary cybersecurity practices, empowering organizations with visibility and depth to efficiently identify, react to, and prevent cyber threats. This will be beneficial for organizations to define and understand what threat intelligence is and why it is so vital in today's cybersecurity landscape. It will be used to develop and implement strong threat intelligence programs for their digital assets and protection against cyber threats [12].

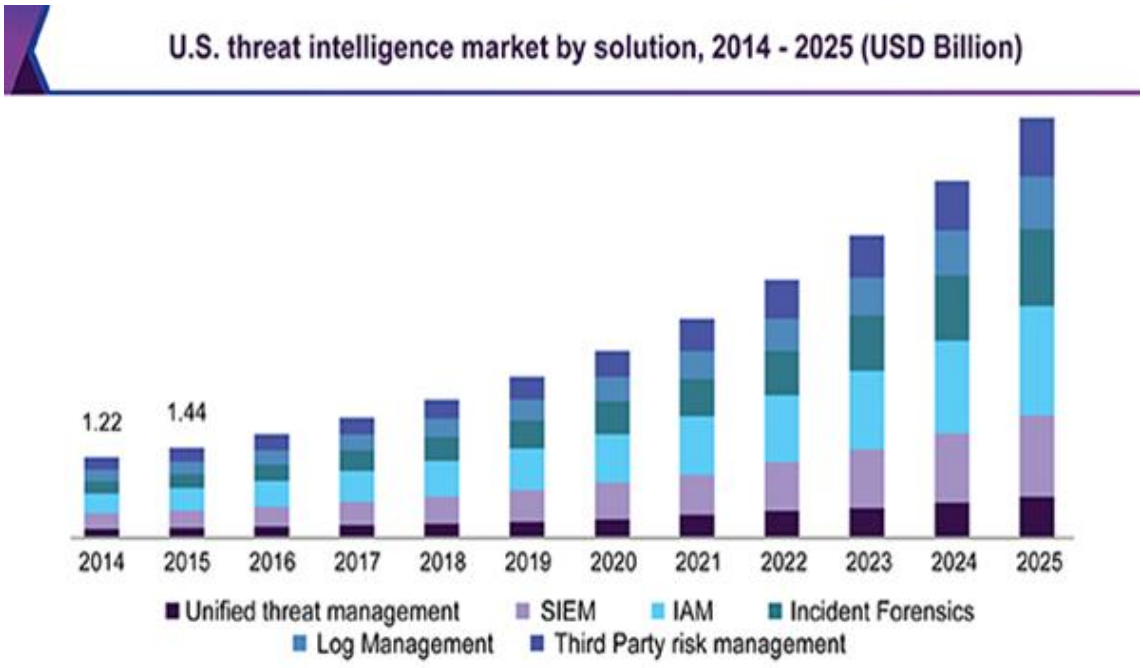

Figure 1. US Threat Intelligence Market by Solution (Report, 2023/24)

Figure 2 shows the simplified Threat Intelligence graph. In this model, the trigger point is employees using tools to detect and report cyber incidents. There is a focus on phishing attacks, but other security

incidents can also be represented. The potential phishing emails from the incidents raised can be identified. Parts of an incident are looked into to determine whether it is a potential attack or a phishing incident. The most important feature of the graph predicts this using the domains from which these emails are sent.

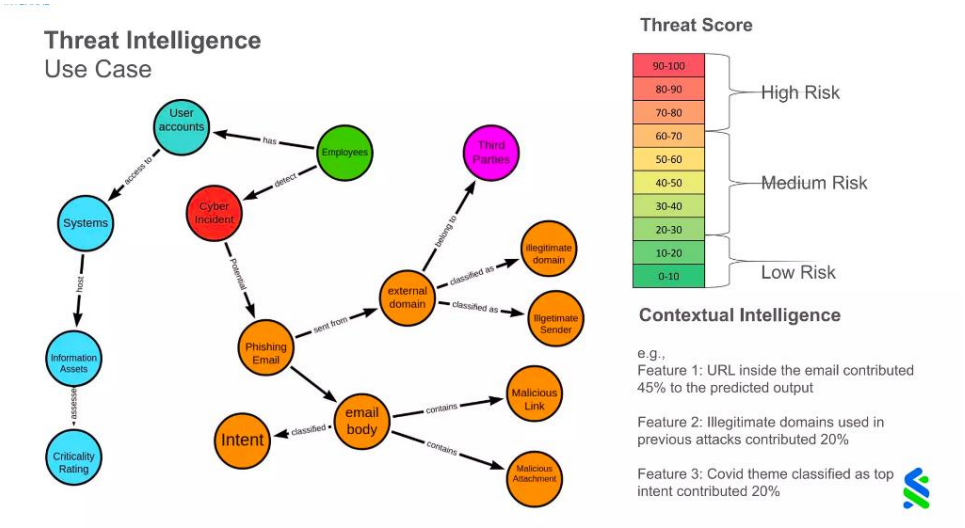

Figure 2. Threat Intelligence Graph by Standard Chartered [13]

2.1. Types and Categories of Threat Intelligence

Cybersecurity has threat intelligence as its foundation in combating adversaries and cyberattacks. Thus, organizations must get abreast of the various types and land categories of threat intelligence to ensure proper identification, assessment, and response to threats. One of the categories of technical threat intelligence is the Indicators of Compromise. Indicators of Compromise, or IOCs, are anything seen on a network or system that could indicate malicious activity or artifacts observed on a host or network. IOCs could be an IP, a domain name, a file hash, a registry key, and so forth [14].

Organizations can reduce their exposure to potential cyber threats and enhance their overall security posture. The issue is that staying informed regarding emerging vulnerabilities and respective risks will likely minimize organizations' exposure to potential cyber threats and improve their general security posture. TTPs are the last category considered here within this section of the literature review. TTPs refer to the methods used by threat actors to conduct cyberattacks. They include but are not limited to reconnaissance, initial access, lateral movement, and data exfiltration. Therefore, an organization must appreciate the TTPs employed by a given adversary for any detection and disruption of operations. This is to assist in developing the detection rules and signatures meant to aid in spotting any malicious activity within their networks. TTP also gives insight into the capabilities and intentions of the threat actors. Therefore, organizations can develop a better defense against future attacks [15]. Figure 3 shows categories of technical threats, as discussed in this section.

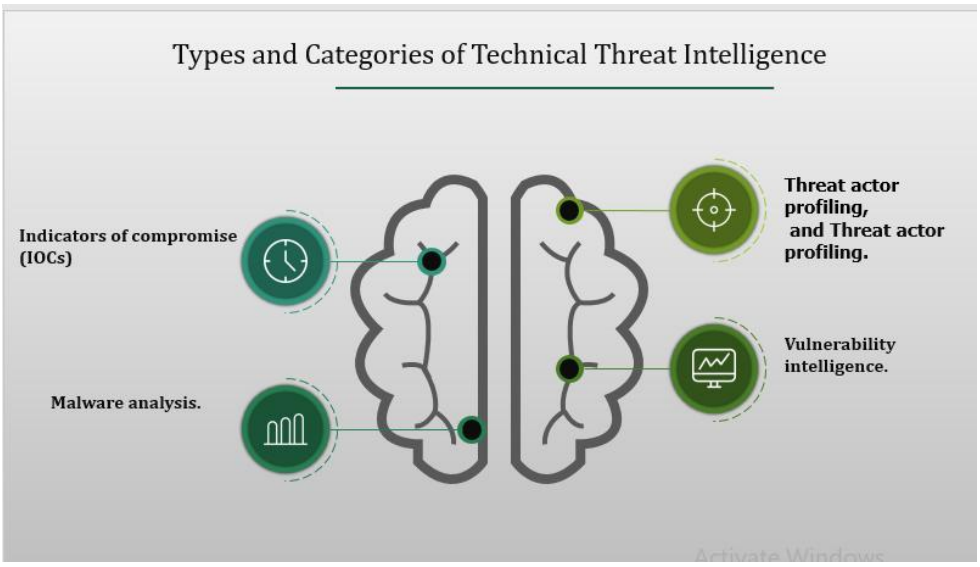

Figure 3. Categories of Technical Threats [16]

2.2. Sources of Threat Intelligence

In the modern dynamic cybersecurity setting, availability and reliability provide their full utility in identifying, developing mitigation steps, and responding to cyber threats. Figure 4 shows the graph of the open-source intelligence market. Open-source intelligence is the product of collecting and processing publicly available information to create intelligence that can be used to inform decisions. Open-source intelligence is applied to provide understanding concerning the operating environment of a company or organization, comprising its competitors, customers, suppliers, and risks of an actual or potential threat. It is a technique for gathering intelligence that uses data sources that are easily accessible and widely available, such as the Internet, print media, broadcast media, television, and radio.

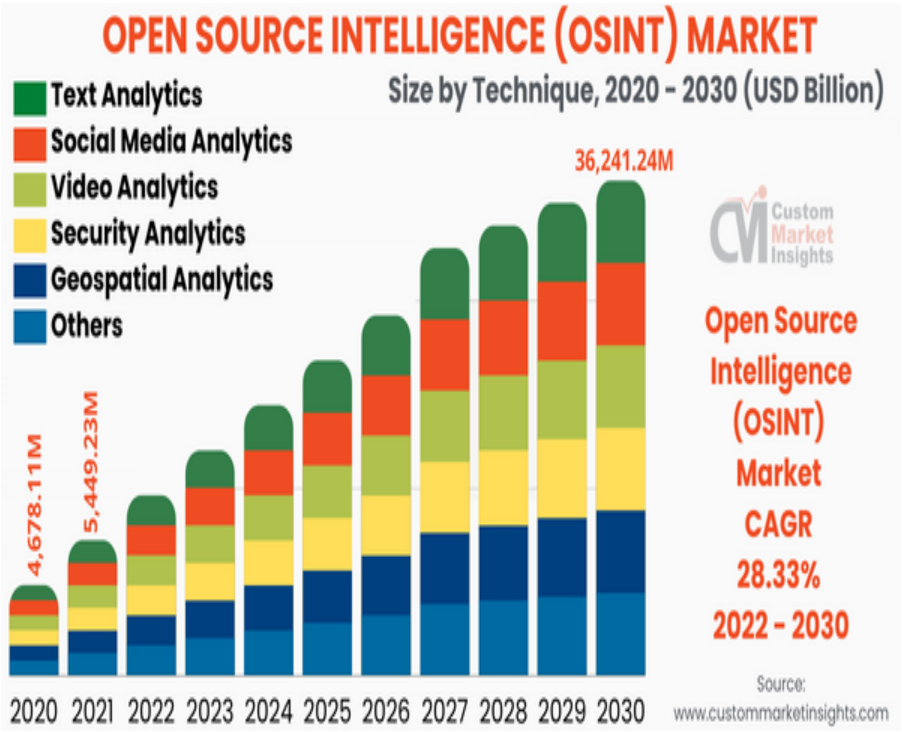

Figure 4. Open Source market [17]

Open-source intelligence, or OSINT, is data gathered from freely available sources. These sources might include websites, social media sites, discussion forums, and online blogs [18]. Some of the significant techniques that analysts use in collecting, processing, and analyzing vast amounts of information from a

wide range of online sources include web scraping, data mining, and social network analysis. However, it should be realized how OSINT may be filled with conflicting pieces of information; significant variations in reliability and accuracy should be expected; and, for OSINT to have actual worth in threat intelligence operations, a lot shall be required to validate and verify the information [19].

On the other hand, closed-source intelligence is the type of proprietary data that is created based on information obtained from internal databases, proprietary software, and closed communities [20]. Contrasted and quite different from OSINT, CSINTs offered exclusive access to sometimes restricted information made available by target organizations or expert intelligence providers. Some of the sources to be used in CSINT include security vendors, threat intelligence platforms, and industry-specific information-sharing groups, which are tailored to provide insights on specific threats and vulnerabilities that would interest an identified sector or even organization [21]. Information-sharing communities and platforms foster collaboration among different stakeholders to exchange threat information among government agencies, private enterprises, cybersecurity vendors, and academic institutions to help protect one another

2.3. Methodologies and Practices in Threat Intelligence

Threat intelligence is built on analytic techniques honed by government and military agencies over several decades. Figure 5 on the next page shows the traditional intelligence, which focuses on six distinct phases of the "intelligence cycle": direction, collection, processing, analysis, dissemination, and feedback.

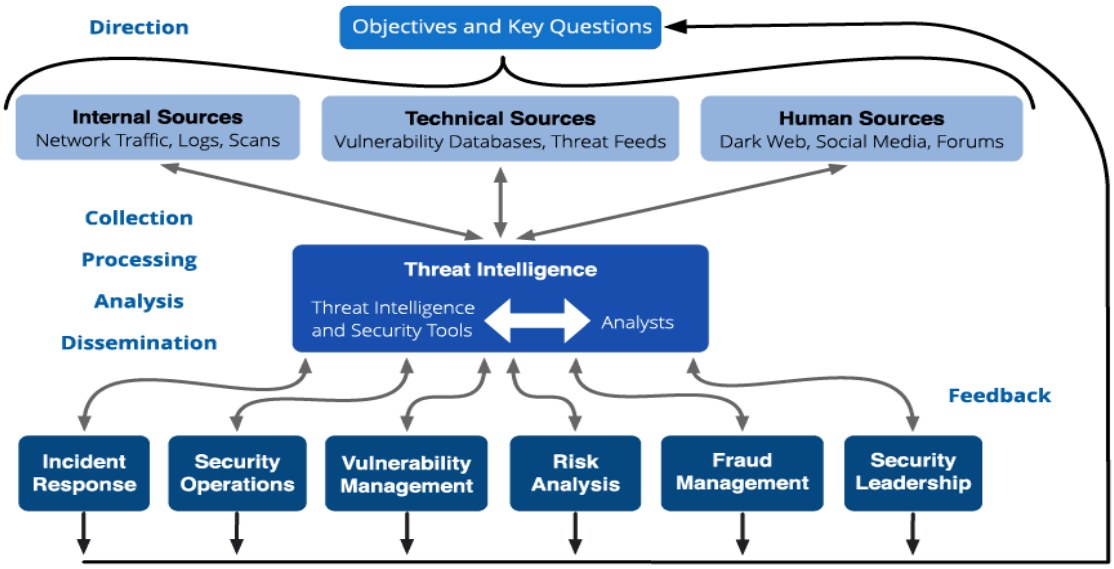

Figure 5. Threat intelligence and the six phases of the intelligence lifecycle [22]

Threat intelligence is the process by which information about threats is gathered, analyzed, and disseminated. This practice enables organizations to be better positioned to predict, detect, and respond to new threats and even defend themselves proactively [23]. The acquisition process of information relevant to particular sources forms the basis of threat intelligence through data collection. Among the commonly applied methods of data collection is passive DNS monitoring. This involves the analysis of Domain Name System or DNS traffic to spot suspicious or malicious domains and infrastructure [24]. Through passive monitoring of DNS queries and responses, organizations detect Indicators of Compromise associated with malware infection, Command and Control communications, and other malicious activities. Figure 5 shows the cyber threat intelligence that includes obtaining, treating, and visualizing Indicators of Compromise and any other relevant data to identify and mitigate cyber threats.

On the other hand, behavioral analysis monitors suspicious or anomalous behavior that reflects the possibility of a threat. Behavior analysis techniques monitor the actions and exchange of users, applications, and entities in the network to find deviations in typical behavior patterns [25]. This technique works well for previously unknown or zero-day threat identification that cannot be located using signature-based detection mechanisms. Effective dissemination and sharing are vital to collective defense enhancement against cyber threats and building outreach resilience. Intelligence dissemination delivers actionable intelligence to pertinent consumers of a specific organization or within a particular community. Sharing protocols guide

the exchange of intelligence between different entities, which include organizational entities like private firms, government agencies, and information-sharing communities. Some commonly used sharing protocols include STIX or TAXII, which provide standard formats and protocols for encoding, transmitting, and sharing threat intelligence, allowing interoperability amongst security tools or even different platforms [26].

2.4. Effectiveness of Threat Intelligence

Hackers can exploit security weaknesses to compromise vulnerable devices and conduct cyberattacks. After all, it is precisely threat modeling that can help get out of the situation when reliable data on cyber risks is lacking. Figure 6 shows the security maturity level of some developed countries. That gives the cybersecurity maturity level of some developed countries with their respective overall cybersecurity risk and the maturity level in the cybersecurity context of the readiness of an organization or a country to counter cyberattacks. It is instead an updated report. The higher the maturity, the better the defense against cyberattacks, such as having a sound plan, better training of employees, and the most recent software updates. The y-axis shows the percentage of countries that have high and upper maturity levels, and the x-axis shows total cybersecurity risk [27]. It thus shows a trend line that indicates that the higher the level of maturity, the lower the overall risk of cybersecurity.

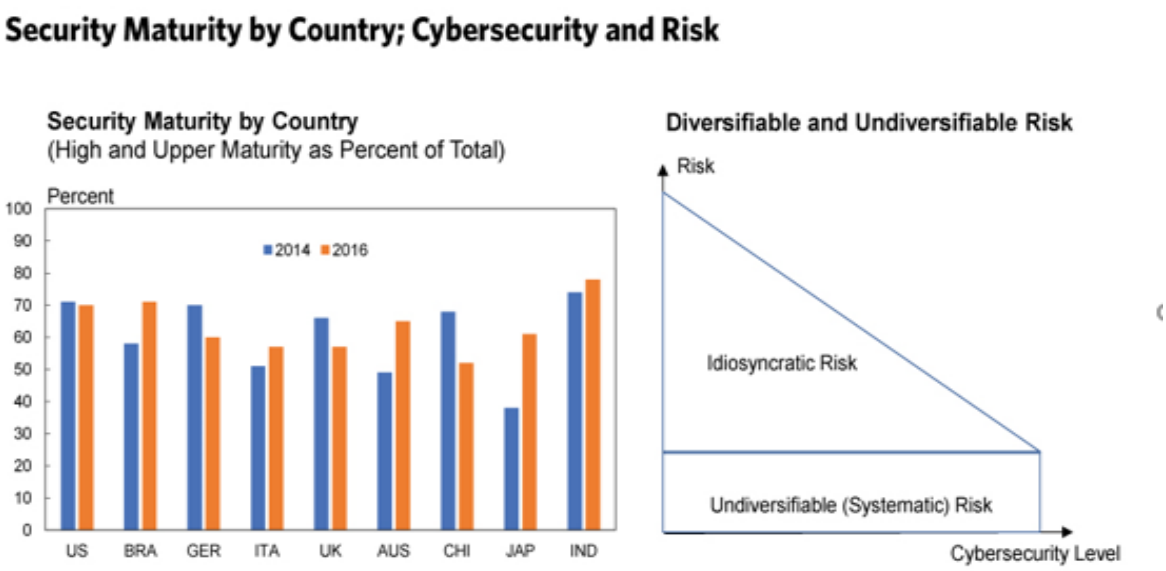

Figure 6. Cybersecurity Risk by Countries [28]

Proactive threat detection identifies and mitigates the potential threat before it becomes a full-scale attack. Continuous monitoring of varied sources for IOCs, malware signatures, and anomalous network behavior allows organizations to anticipate cyber threats through TI to prevent them [29]. In addition, advanced threat detection technologies such as machine learning and behavioral analytics detect sophisticated threats that evade traditional security measures. TI also facilitates the identification of new threats that are emerging along with trends of attacks, so that organizations can update their defenses accordingly. For example, in a study undertaken by Nassar et al [30], it was reflected that the functionality of TI could be very useful in the real-time environment of network traffic analysis and malicious domain registrations for detecting and mitigating botnet-based attacks.

Case studies of organizations that have benefited from using TI to enhance their cybersecurity posture and reduce the impact of cyber threats are well-documented. For instance, one of the most significant ransomware attacks ever seen, the 2017 outbreak that spread to hundreds of thousands of computers worldwide, has brought home the need for early threat detection and response using TI [31]. Those organizations with timely access to streams of threat intelligence feeds were thus able to patch and apply mitigations to forestall WannaCry infections and, hence, arrest the spread of the ransomware malware. Whereas Michelson acknowledges that this was so, he also brings to light the salient role of threat intelligence in incident response and recovery efforts from the 2017 NotPetya ransomware attacks [32]. Those already with good TI capabilities promptly isolated the infected systems, restored their data from backup, and resumed regular business in minimal time.

2.5. Trust-Based Sharing Strategies

Trust is the basis for any successful cybersecurity information sharing. If organizations feel that the recipients of that sensitive threat intelligence will protect the information and give something back in return, they are much more willing to share information [33] (Figure 7).

According to Raheema [33], trust forms the basis for developing collaboration and cooperation between different actors in the cybersecurity space. In sharing threat intelligence, the foundation of this trust would be the assurance that they would not be taken advantage of by sharing such sensitive information. Despite its importance, trust-based sharing has faced several challenges and barriers that hamper effective collaboration among various stakeholders. A significant challenge is the absence of transparency and accountability in the information-sharing approach [35]. Most organizations will be very reluctant to share threat intelligence if they are unsure how it will be used or if there is a perceived lack of reciprocity on the part of their potential customers. Secondly, issues related to legal and regulatory compliance, data privacy as well as protection of intellectual property rights, can further deter sharing initiatives premised on trust folklore [36]. Finally, minor cultural differences, rival interests, and asymmetries of organizational power play can work against stakeholder trust or even cooperation.

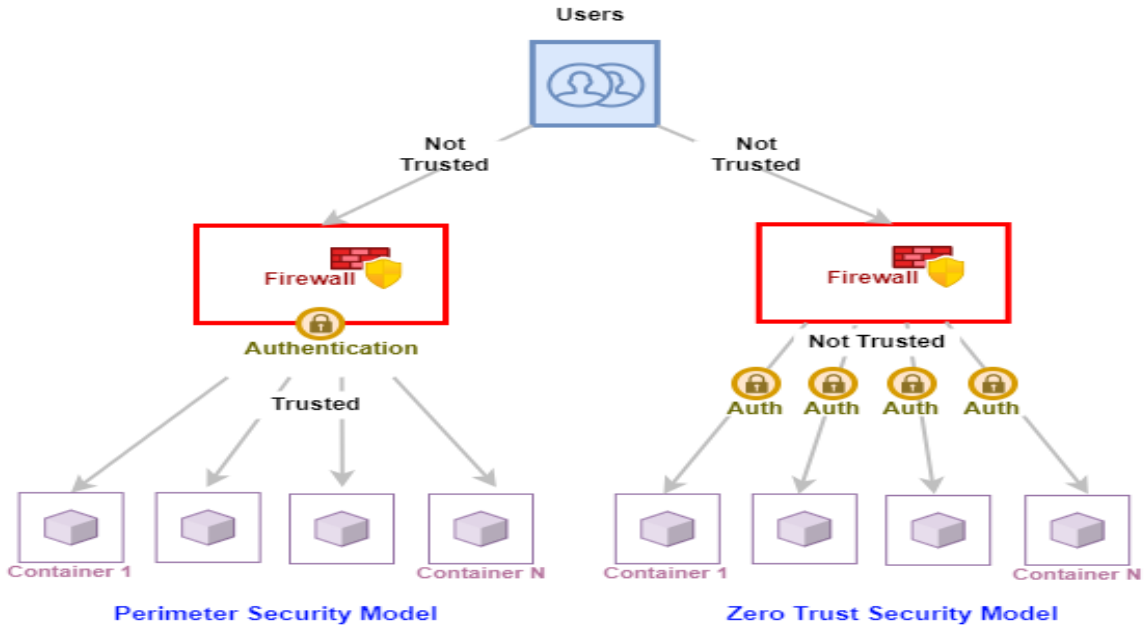

Figure 7. Comparison between the perimeter security model and the zero-trust model [34]

Several mechanisms and strategies can be used to overcome sharing based on trust challenges. First, trust must be built and sustained between the stakeholders. According to Barrane et al [37], transparency in communication and articulation of the policy and procedure for information sharing does build trust. Personal relationships and mutual understanding play a significant role in creating shared purpose and commitment toward collective defense. Moreover, formal agreements of the ISAs or MOU type can provide some legal framework for trust-based sharing, thereby defining the rights and duties of participating entities. Industry consortia and government agencies are, for instance, trusted intermediaries that offer neutral means for information exchange and dispute resolution and, hence, are another means for effecting trust-based sharing [38].

Many case studies apply to successful trust-based sharing initiatives that reveal the real essence of collaboration and cooperation regarding cyber threats. Case in point, the Cyber Threat Alliance was formed in 2014 as a consortium of cybersecurity vendors working together by way of sharing threat intelligence and coordinating responses to cyberattacks [39]. Pooling resources and expertise, CTA members analyze and attribute cyber threats, develop countermeasures, and disseminate actionable intelligence to customers and partners. The FS-ISAC and H-ISAC are among several ISACs providing sector-based trust-based sharing for likewise [40]. These ISACs have developed this trusted environment for sharing threat intelligence, a coordinated incident response effort, best practices, and guidance unique to that industry. This shows the world how trust, collaboration, and information sharing lead to cyber resiliency and minimize the significance of cyber threats.

2.6. Legal and Ethical Considerations in Threat Intelligence Sharing

In many cases, sharing threat intelligence involves exchanging sensitive information, including personally identifiable information and other confidential data. Therefore, the privacy and data protection regulations rank among the most critical considerations that govern the collection, use, and sharing of such information. The Nigerian Data Protection Commission shall apply high standards while processing and transferring personal data. This commission charges the necessary obligations on organizations to lawfully and transparently process personal data [41]. Similarly, different United States legislations, such as the Health Insurance Portability and Accountability Act, California Consumer Privacy Act, etc., have limitations on releasing personal data and demand proper measures from the organization for safeguarding the entitled privacy of individuals. As stated by Mulgund et al [42], the requirements of these regulations need to be complied with; otherwise, legal liabilities will create problems and shake stakeholder trust regarding threat intelligence-sharing projects [43].

Sharing threat intelligence is pretty much a complex business from the point of view of intellectual property rights and ownership of the information to be shared. Often, organizations invest too much in terms of the collection, analysis, and curation of data towards threat intelligence; hence, reasonably and naturally, concern will be expressed about protecting proprietary information and trade secrets [44]. Because of this, sharing agreements define terms and conditions under which intelligence will be shared among participating entities. These contracts and agreements often explain the rights and duties of parties involved and may contain clauses regarding data ownership, usage limitations, and liability. Organizations can also use such technologies as anonymization and encryption of data to be shared in collaboration to ensure that information sharing is guaranteed. Nonetheless, threat intelligence sharing ecosystems constantly face the challenge of balancing safeguarding intellectual property rights and encouraging collaborative sharing practices.

As sensitive information is shared, particularly where cybersecurity matters might have consequences that spread far and wide upon disclosure of vulnerabilities and threats, it does not shy away from ethical considerations. Ethical guidelines like the Menlo Report and ACM Code of Ethics emphasize honesty and integrity with respect for privacy in cybersecurity research and practice. Ethical dilemmas related to responsible disclosure of vulnerabilities include balancing transparency and risk that might compromise the integrity of the system and its users' privacy. According to Wang et al [45], Security researchers and ethical hackers are exposed to many moral dilemmas when responsibly disclosing a particular vulnerability. The proportionality principle is the second, whereby such sensitive information is held to be shared only after weighing its adverse effects. That is earnest consideration of the injury, which is likely caused by an action to the affected person or organization [46].

2.7. Integration with Cybersecurity Frameworks

Cybersecurity frameworks are, therefore, organized processes in which organizations can manage and mitigate cybersecurity risks. There have been two significant frameworks widely adopted across the industry: The National Institute of Standards and Technology (NIST) Cybersecurity Framework and the MITRE ATT&CK Framework [47]. Numerous private and public sector entities have implemented the NIST CSF; it has thus become part of a common vocabulary to which many cybersecurity practitioners, policymakers, and other stakeholders refer [48]. The CSF is "a guidance document, not a set of regulations" that allows organizations to manage their cybersecurity risk appropriately to their specific needs and circumstances. The critical framework of NIST is depicted in Figure 8 below.

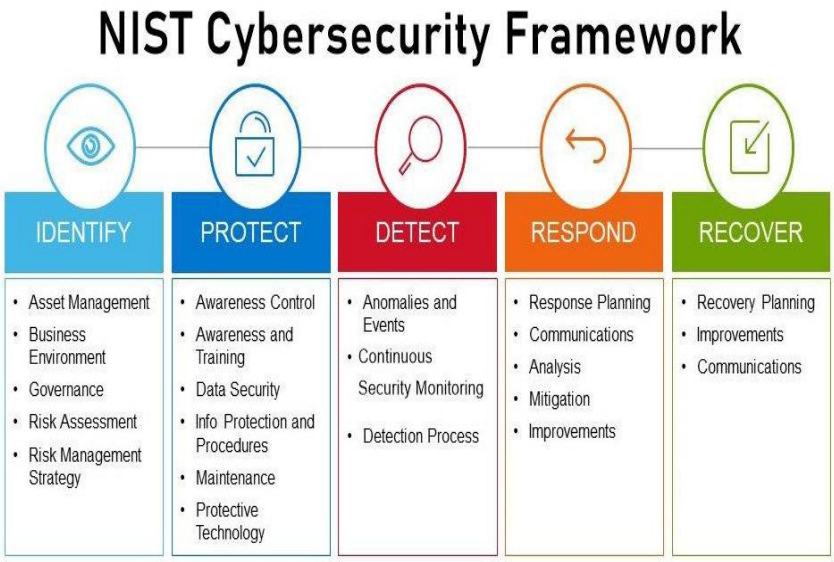

Figure 8. Key steps in the cybersecurity risk management process [49]

Figure 8 shows significant steps in a Cybersecurity Risk Management Process. The framework aims to lead organizations to confront cybersecurity risks comprehensively and systematically. With threat intelligence incorporated into the frameworks, an organization will be more capable of detecting, responding to, and recovering from cyber threats. Additionally, NIST CSF is a broad and widely used framework. Different guidelines in this framework help organizations effectively manage and improve their cybersecurity posture [50]. It provides an elaborate matrix of adversary tactics, techniques, and procedures from actual sightings. Organizations now have an eye for adversarial behavior and tactics; hence, anticipatory and countermeasures have become easy. They could get results from threat intelligence analysis, where specific TTPs would be given that are being used by the threat actor for targeting an organization. Security teams can now develop their defense according to those specifications [51].

3. Classification of Threat Intelligence (TI)

This section presents the results and validation of the experiments along with a detailed discussion. Tables and figures are explained in paragraphs. The author needs to add a more detailed analysis. Authors need to adjust the use of equations based on the journal The classification of Threat intelligence holds diverse types and categories that fulfill different purposes in enhancing organizational cybersecurity resilience [24]. Extensive literature surveys and case studies led to the following classifications:

- Indicator-based Intelligence: This refers to indicators of compromise or IOCs. These encompass but are not limited to IP addresses, domain names, file hashes, and signatures [20]. It is the most actionable form of intelligence in detecting and mitigating cyber threats.
- Tactical Intelligence: Tactical intelligence helps to establish an adversary's tactics, techniques, and procedures that will, in turn, lead an organization to identify the behavior of the threat actor, thus being able to predict the likely attack vectors.
- Strategic Intelligence: Focused on the more significant threat trends, emerging threats, and geopolitical factors that influence the organizational security posture in the long term. It includes threat assessment, trend analysis, and geopolitical intelligence.

3.1. Methodologies and Practices Associated with TI

The practices and methodologies of Threat intelligence or TI ranged from collection and dissemination to application. Some of the prime findings associated with it are stated below.

- Data Collection: Sources used for collecting threat intelligence by organizations include OSINT, commercial threat feeds, incident reports, and internal telemetry data [26]. Automated collection mechanisms and threat intelligence platforms take their turn in gathering varied sources and normalizing this data.
- Techniques of Analysis: The analysis techniques are applied to threat intelligence by machine learning algorithms, data analytics, and human judgment for finding patterns, linkages, and anomalies that would suggest an impending cyber-attack. Behavioral analytics and anomaly detection techniques are rising for advanced and proactive threat detection.

- Dissemination and Utilization: Sharing meaningful and actionable threat intelligence with the appropriate stakeholders has to happen promptly. Commonly seen standards for distributing threat intelligence data are TAXII or STIX. Additionally, organizations use threat intelligence platforms or SIEMs to operationalize threat intelligence, automating response workflows.

3.2. Effectiveness of TI in Enhancing Cybersecurity Resilience

The results showed that TI is quite effective in strengthening an organization's cybersecurity resiliency in various ways, such as proactive threat detection, incident response, and risk mitigation strategies. The following are some key findings:

- Proactive Threat Detection: TI allows organizations to detect and mitigate cyber threats proactively with timely insight into the emergence of cyber threats, vulnerabilities, and attack vectors [29]. This is because of indicator-based intelligence and behavioral analytics that allow the security team to detect and respond to threats as they are building, before becoming full-bore incidents.
- Incident Response: Responding to incidents is another active role for TI, supplying security teams with valuable event context, attribution information about associated actors or groups, and remediation guidance. With the benefit of TI, organizations are better positioned to contain and mitigate security incidents, hence decreasing their impact on operations and dwell time.
- Risk mitigation strategies: Organizations can get clear priority investment and resource allocation with the TI. They shall then adopt targeted risk mitigation strategies.

3.3. Challenges and Barriers to Trust-Based Sharing Strategies

Although trust-based sharing strategies are helpful, several barriers and challenges come with adopting and implementing them in organizational contexts. The significant findings in this regard are outlined below:

- Lack of Trust: It is still a significant constraint to information sharing across organizations, especially given the concerns about data privacy, competitive advantage, and legal implications. Transparency of communication, reciprocity, and assurance about confidentiality and data integrity help build trust [52].
- Resource Constraints: Progressive SMEs might not have the resources and skills to contribute to information sharing initiatives effectively. Unequal participation and collaboration reflect threat intelligence-sharing ecosystems due to disparity in organizational capability, resources, and risk appetite.
- Legal and Regulatory Challenges: Privacy regulations, data protection laws, intellectual property rights, etc., make any information-sharing system vulnerable to legal and regulatory problems.

4. CONCLUSION AND LIMITATION

4.1. Recommendations for Enhancing TI Utilization and Effectiveness

Therefore, to help deal with the challenges and improve the utilization as well as the effectiveness of threat intelligence in enhancing cybersecurity defenses, the following recommendations are made:

- Promote Standardization. Since threat intelligence is to be shared across entities, standardized formats and protocols of sharing, such as TAXII and STIX, will ensure interoperability, hence seamless information exchange [53].
- Build Trust and Collaboration: Establishing trust, transparency, and collaboration between all the stakeholders will lead to a culture where clear communication channels are established, best practices are shared, and proper incentives for participation in information-sharing initiatives exist.
- Invest in Education and Training: Workforce development and training programs are to be made available to workers and other types of skilled workers for maximum exploitation of threat intelligence. This includes training on threat intelligence analysis procedures, incident response procedures, and information-sharing protocols.
- Advocate for Policy Enhancements: Advocate for exact and uniform regulatory frameworks that encourage information sharing and maintain privacy and security. Governments and regulatory bodies should concentrate on formulating policies allowing incentives based on collaboration, collective defence, and sharing information regarding cyber threats. Figure 9 shows the existing architecture for a threat intelligence system.

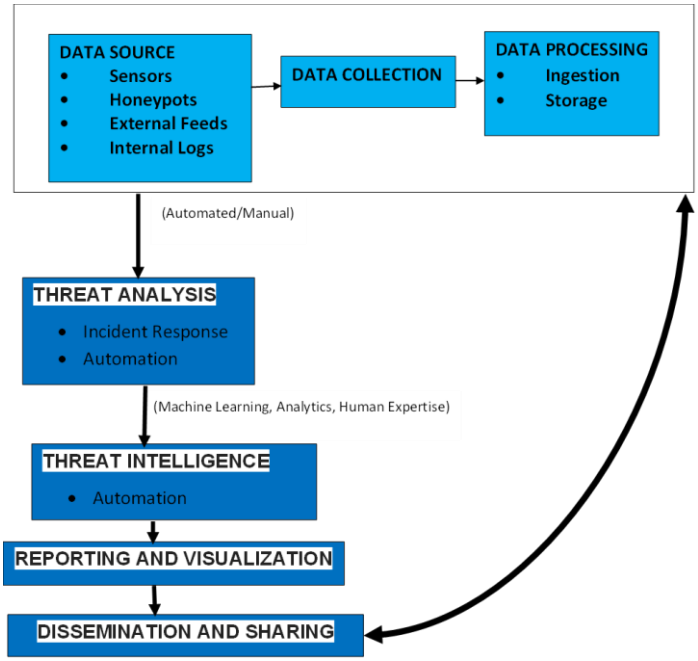

Figure 9. Existing Architecture of Threat Intelligence System

Figure 10 shows that the enhanced architecture reflects the addition of the recommended components. The architecture highlights how these components improve threat intelligence utilization and effectiveness.

The initial threat intelligence architecture revolves around collecting data from various sources, storing it centrally, and then processing and analyzing it to identify threats. This analysis is then transformed into reports and visualizations for internal teams. Finally, actionable intelligence can be disseminated and shared with relevant parties. An enhanced architecture incorporates several recommendations to improve threat intelligence utilization and effectiveness [54]. Firstly, a standardization layer ensures that collected data from diverse sources adheres to standard formats, allowing seamless exchange and analysis. Secondly, training and education empower personnel with the skills to leverage threat intelligence effectively. Automation tools streamline data processing and analysis, freeing up analysts for higher-level tasks. A secure threat intelligence sharing platform facilitates collaboration and information exchange with trusted partners. Finally, policy management ensures data privacy regulations and intellectual property protection. These enhancements work together to strengthen the organization's threat intelligence posture, enabling a more proactive and collaborative defense against cyber threats.

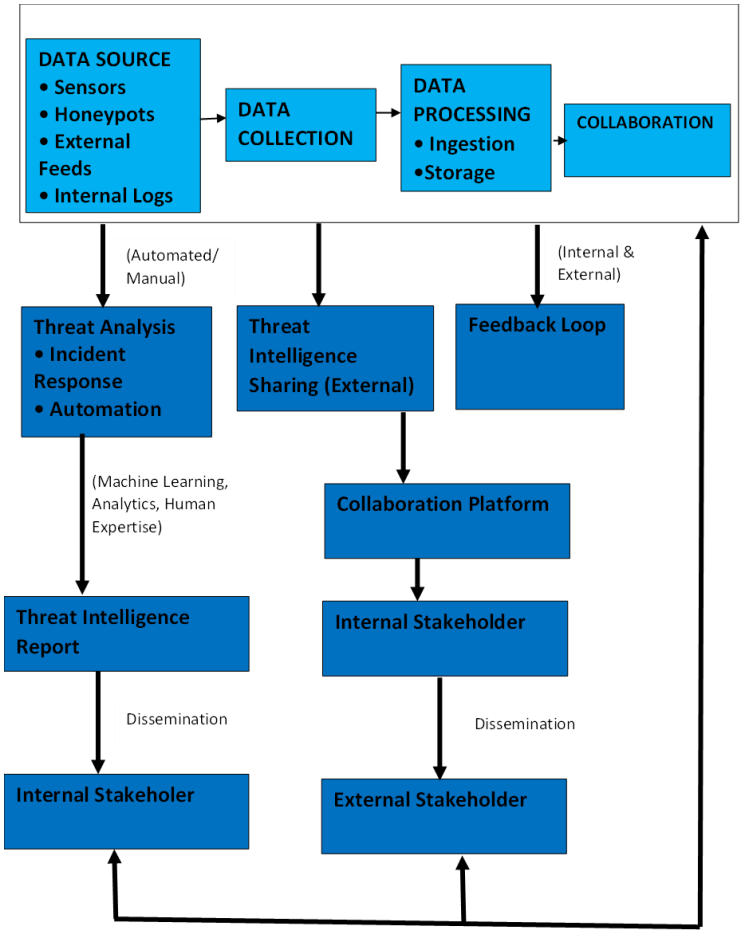

Figure 10. Enhanced Architecture of Threat Intelligence System

4.2. Discussion of Findings

Classifying threat intelligence into different categories reflects a nuanced understanding of its role in cybersecurity. The literature review reveals that threat intelligence can be categorized into several key dimensions: indicator-based intelligence, tactical intelligence, strategic intelligence, and attribution intelligence. These classifications provide a comprehensive framework for understanding the multifaceted nature of cyber threats. Narayan et al [53] highlights the critical role of indicator-based intelligence, such as Indicators of Compromise (IOCs), in strengthening cybersecurity defenses. This type of intelligence enables proactive threat detection, thus allowing for swift incident response. Similarly, tactical intelligence, as discussed by Wang [51], underscores the importance of understanding adversary tactics, techniques, and procedures (TTPs). Therefore, categorizing threat intelligence in this manner enables organizations to tailor their defenses to specific threats.

Reviewing methodologies and practices related to threat intelligence collection, analysis, and dissemination identifies best practices that significantly impact the effectiveness of threat intelligence operations. A primary finding from the literature is the importance of collecting data from diverse sources, such as Open Source Intelligence (OSINT), proprietary threat feeds, and internal telemetry [55]. According to Alfawareh, gathering intelligence from various sources is crucial for comprehensively understanding emerging threats. By aggregating data from different channels, organizations can enhance their threat intelligence datasets, improving their ability to effectively detect and respond to cyber threats.

Findings also emphasize the effectiveness of trust-based sharing mechanisms in fostering collaborative defense against cyber threats. Various practices, such as Information Sharing and Analysis Centers (ISACs), threat intelligence sharing platforms, and inter-organizational partnerships, enhanced collective cybersecurity efforts. This aligns with Nagahawattan et al [56], who argues that ISACs and similar platforms effectively share actionable threat intelligence within industry-specific communities. Although the intelligence shared through these mechanisms is often unfiltered, organizations benefit from the sheer volume and variety of information, enabling them to detect and respond to a broader spectrum of cyber threats in a more proactive manner.

In line with these findings, the study also underscores the importance of trust in the success of information-sharing initiatives. Yulianto et al [57] stress the need for establishing trust and clear communication channels among organizations involved in threat intelligence sharing. Such trust allows organizations to confidently share sensitive intelligence, knowing that it will be used responsibly and reciprocated with valuable insights. Furthermore, Nkoom [15] highlight the role of regulatory incentives and industry certifications in encouraging participation in information-sharing initiatives. Policymakers suggest that implementing regulatory protections and liability safeguards can foster greater collaboration by incentivizing organizations to share intelligence and strengthen collective defense capabilities.

4.3. Conclusion and Future Work

This review has explored threat intelligence (TI) and trust-based sharing strategies within the cybersecurity framework. The findings highlight the multifaceted nature of TI, categorizing it into distinct types, including indicator-based, tactical, and strategic intelligence. The review underscores integrating diverse threat intelligence sources and advanced analytics to enhance threat detection and response capabilities. The study reveals that effective threat intelligence management requires organizations to adopt a comprehensive approach, drawing on multiple data sources, fostering collaboration, and ensuring timely threat identification and mitigation communication. Trust-based sharing mechanisms, such as industry collaborations and information-sharing platforms, are crucial in improving collective defense efforts.

Additionally, the review emphasizes the role of regulatory frameworks in encouraging information sharing and ensuring the responsible use of sensitive intelligence. The findings suggest that organizations must continuously improve their threat intelligence practices through collaboration, advanced analytics, and proactive risk mitigation strategies to stay ahead of evolving cyber threats. Future work can explore integrating emerging technologies, such as AI and machine learning, to enhance threat intelligence analysis and predictive capabilities and the impact of regulatory changes on the effectiveness of collaborative defense strategies.

REFERENCES

[1] R. Montasari et al.,"Application Of Artificial Intelligence And Machine Learning In Producing Actionable Cyber Threat Intelligence," *Advanced Sciences and Technologies for Security Applications*, pp. 47–64, 2021. https://doi.org/10.1007/978-3-030-60425-7_3.

[2] D. Galinec, D. Možnik, and B. Guberina, "Cybersecurity And Cyber Defence: National Level Strategic Approach," *Automatika*, vol. 58, no. 3, pp. 273–286, 2017. https://doi.org/10.1080/00051144.2017.1407022.

[3] Y. Wang et al., "A Dataset For Cyber Threat Intelligence Modeling of Connected Autonomous Vehicles," *Scientific Data*, vol. 12, no. 1, 2025. https://doi.org/10.1038/s41597-025-04439-5.

[4] M. Karjalainen, A.-L. Ojala, M. Vatanen, and J. Lötjönen, "Learn To Train Like You Fight," I*nternational Journal of Adult Education and Technology*, vol. 14, no. 1, pp. 1–20, 2023. https://doi.org/10.4018/IJAET.322085.

[5] M. Frydenberg and B. Lorenz, "Lizards in the Street! Introducing Cybersecurity Awareness in a Digital Literacy Context.," *Information Systems Education Journal*, vol. 18, no. 4, pp. 33–45, 2020. http://ISEDJ.org/2020-4.

[6] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," *Sensors*, vol. 23, no. 16, p. 7273, 2023. https://doi.org/10.3390/s23167273.

[7] A. S. Alzakari et al., " An Intelligent Ransomware Based Cyberthreat Detection Model Using Multi Head Attention-Based Recurrent Neural Networks with Optimization Algorithm in IoT Environment", S*cientific Reports*, vol. 15, no. 1, 2025. https://doi.org/10.1038/s41598-025-92711-4.

[8] B. W. Weaver, A. M. Braly, and D. M. Lane, "Training Users To Identify Phishing Emails," *Journal of Educational Computing Research*, vol. 59, no. 6, pp. 1169–1183, 2021. https://doi.org/10.1177/0735633121992516.

[9] J. Zhang et al., " When Llms Meet Cybersecurity: A Systematic Literature Review", *Cybersecurity*, vol. 8, no. 1, 2025. https://doi.org/10.1186/s42400-025-00361-w.

[10] P. Nuangchalerm and V. Prachagool, "AI-Driven Learning Analytics in STEM Education," *International Journal on Research in STEM Education*, vol. 5, no. 2, pp. 77–84, 2023. https://doi.org/10.33830/ijrse.v5i2.1596.

[11] T. Pham, T. B. Nguyen, S. Ha, and N. T. N. Ngoc, "Digital Transformation in Engineering Education: Exploring The Potential of AI-Assisted Learning," *Australasian Journal of Educational Technology*, vol. 39, no. 5, pp. 1–19, 2023. https://doi.org/10.14742/ajet.8825.

[12] Y. Renu, and V. Saveshwaran, " A Review of Cyber Security Challenges and Solutions in Unmanned Aerial Vehicles (UAVs)" *Inteligencia Artificial*, vol. 28, no. 75, pp. 199-219, 2025. https://doi.org/10.4114/intartif.vol28iss75pp199-219.

[13] H. Prabakaran, "Standard Chartered: Threat Intelligence Using Knowledge Graphs. This presentation was given by Hemanth Prabakaran at a GraphSummit.," 2023.

[14] U. Kant and V. Kumar, "A Systematic Review Paper on Attack Detection Systems in Internet of Things Environment", *Lecture Notes in Networks and Systems*, vol. 1139, pp. 427-443. https://doi.org/10.1007/978-981-

97-7603-0_36.
[15] M. Nkoom, S. G. Hounsinou, and G. V. Crosvy, "Securing the Internet of Robotic Things (IoRT) against DDoS Attacks: A Federated Learning with Differential Privacy Clustering Approach", *Computers and Security*, vol 155, 2025. https://doi.org/10.1016/j.cose.2025.104493.
[16] M. A. Almaiah, A. Al-Zahrani, O. Almomani, and A. K. Alhwaitat, "Classification of Cyber Security Threats On Mobile Devices and Applications,"*Artificial Intelligence and Blockchain for future Cybersecurity Applications*, pp. 107–123, 2021. https://doi.org/10.1007/978-3-030-74575-2_6.
[17] NRich, "Open-Source Intelligence forecast to 2030," 2020.
[18] T. Ivanjko and T. Dokman, "Open Source Intelligence (OSINT): Issues and Trends," *International Conference The Future of Information Sciences*, pp. 191–196, 2020. https://doi.org/10.17234/INFUTURE.2019.23.
[19] J. Loevenich, E. Adler, T. Hurten, and R.R.F. Lopes, " Design and Evaluation of an Autonomous Cyber Defence Agent using DRL and an Augmented LLM", *Computer Networks*, vol. 262, 2025. https://doi.org/10.1016/j.comnet.2025.111162.
[20] N. Alsharabi, A. Bhardwaj, A. Ayaba, and A. Jadi "Threat hunting for Adversary Impact Inhibiting System Recovery", *Computers and Security*, vol. 154, 2025. https://doi.org/10.1016/j.cose.2025.104464.
[21] T. Attema, V. Dunning, M. Everts and P. Langenkamp, " Efficient Compiler to Covert Security with Public Verifiability for Honest Majority MPC", *Lecture Notes in Computer Science*, vol. 13269, pp. 663-683, 2022. https://doi.org/10.1007/978-3-031-09234-3_33.
[22] D. Schlette, M. Caselli, and G. Pernul, "A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2525–2556, 2021. https://doi.org/10.1109/COMST.2021.3117338.
[23] C. Heath and P. Luff, "Embodied action, projection, and institutional action: The exchange of tools and implements during surgical procedures," *Discourse Processes*, vol. 58, no. 3, pp. 233–250, 2021. https://doi.org/10.1080/0163853X.2020.1854041.
[24] X. Huo, H. Huang, K. R. Davis, H.V. Poor, and M. Liu, " A Review of Scalable and Privacy-Preserving Multi-Agent Frameworks for Distributed Energy Resources", *Advances in Applied Energy*, vol. 17, 2025. https://doi.org/10.1016/j.adapen.2024.100205.
[25] P. P. Kundu, T. Truong-Huu, L. Chen, L. Zhou, and S. G. Teo, " Detection and Classification of Botnet Traffic using Deep Learning with Model Explanation", *IEEE Transactions on Dependable and Secure Computing*, pp. 1-15, 2022. https://doi.org/10.1109/TDSC.2022.3183361.
[26] C. Skandylas and M. Asplund," Automated Penetration Testing: Formalization and realization" *Computers and Security*, vol. 155, 2025. https://doi.org/10.1016/j.cose.2025.104454
[27] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the Cyber Security Readiness of Organizations and Its Influence on Performance," *Journal of Information Security and Applications*, vol. 58, p. 102726, 2021. https://doi.org/10.1016/j.jisa.2020.102726.
[28] A. Dalimi-Asl, S. Javadi, a. Ahmarinejad, and P. Rabbanifar, "Energy Management of Networked Energy Hub Considering Risk Assessment and Cyber Security: A Deep Reinforcement Learning Approach", *Computers and Electrical Engineering*, vol. 124, 2025. https://doi.org/10.1016/j.compeleceng.2025.110262.
[29] G. S Jadoun, D. P. Bhatt, V. Mathur. and A. Kaur, "The Threat of Artificial Intelligence in Cyber security: Risk and Countermeasures", *AIP Conference Proceedings*, vol. 3191, no. 1, 2025. https://doi.org/10.1063/5.0248313.
[30] A. Nassar and M. Kamal, "Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies," *Journal of Artificial Intelligence and Machine Learning in Management*, vol. 5, no. 1, pp. 51–63, 2021.
[31] A. B. Turner, M. Ikram, and A. J Uhlmann, "Classifying Ransomware-Bitcoin Nodes using Graph Embeddings", *Pacific Asia Journal of the Association for Information Systems*, vol 17, no. 1, pp. 51-81, 2025. https://doi.org/10.17705/1pais.17104.
[32] Z. Wang, H. Deng, and G. Li, "Enhancing Information Security Compliance Behavior Through Knowledge Interventions: Insights from EEG", *Information and Computer Security*, 2025. https://doi.org/10.1108/ICS-08-2024-0206.
[33] A.Q. Raheema, "Challenges and Vulnerability Assessment of Cybersecurity in IoT-enabled SC", *Wireless Networks*, vol. 30, no. 8, pp. 6887-6900, 2024. https://doi.org/10.1007/s11276-023-03493-4
[34] T. Theodoropoulos et al., "Security in Cloud-Native Services: A Survey," *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 758–793, 2023. https://doi.org/10.3390/jcp3040034.
[35] F. Mızrak, "Integrating Cybersecurity Risk Management Into Strategic Management: A Comprehensive Literature Review," *Pressacademia*, vol. 10, no. 3, pp. 98–108, 2023. https://doi.org/10.17261/Pressacademia.2023.1807
[36] F. Lekota and M. Coetzee, "Aviation Sector Computer Security Incident Response Teams: Guidelines and Best Practice," *European Conference on Cyber Warfare and Security*, pp. 507–XII, 2021. https://doi.org/10.34190/EWS.21.028.
[37] F. Z. Barrane, N. O. Ndubisi, S. Kamble, G. E. Karuranga, and D. Poulin, "Building Trust in Multi-Stakeholder Collaborations for New Product Development in The Digital Transformation Era," *Benchmarking*, vol. 28, no. 1, pp. 205–228, 2021. https://doi.org/10.1108/BIJ-04-2020-0164.
[38] A. Alanis-Ocádiz et al., "Design and Psychometric Validation of A Social Capital Questionnaire for Adults with End-Stage Chronic Kidney Disease Undergoing Dialysis or Hemodialysis", *BMC Nephrology*, vol. 26, no. 1, 2025. https://doi.org/10.1186/s12882-025-03993-9.
[39] M. Saied and S. Guirguis, "Explainable Artificial Intelligence for Botnet Detection in Internet of Things", *Scientific Reports*, vol. 15, no. 1, 2025. https://doi.org/10.1038/s41598-025-90420-6.

[40] S. Purohit et al., “Cyber Threat Intelligence Sharing For Co-Operative Defense in Multi-Domain Entities,” *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 5, pp. 4273–4290, 2022. https://doi.org/10.1109/TDSC.2022.3214423.

[41] O. Ekpo, A. Okokon, and M. Akpakpan, " Data Protection in the Digital Age: A Comparative Analysis of Nigeria's NDPA and the EU's GDPR", *International Conference on Information and Communication Technologies and Development*, pp. 48-56, 2025. https://doi.org/10.1145/3700794.3700799.

[42] P. Mulgund, B. P. Mulgund, R. Sharman, and R. Singh, “The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences,” *Health Policy and Technology*, vol. 10, no. 3, p. 100543, 2021. https://doi.org/10.1016/j.hlpt.2021.100543.

[43] S. Taylor et al., "A Framework Addressing Challenges in Cybersecurity Testing of IoT Ecosystems and Components", *International Conference on Internet of Things, Big Data and Security*, pp. 226-234, 2024. https://doi.org/10.5220/0012676300003705.

[44] M. Nankya, R. Chataut, and R. Akl, "Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies", *Sensors (Basel, Switzerland)*, vol. 12, no. 21, 2023. https://doi.org/10.3390/s23218840.

[45] S. Ali, J. Wang, and V. C. M. Leung, "AI-driven Fusion with Cybersecurity: Exploring Current Trends, Advanced Techniques, Future Directions, and Policy Implications for Evolving Paradigms– A Comprehensive Review", *Information Fusion*, vol. 118, 2025. https://doi.org/10.1016/j.inffus.2024.102922.

[46] T. Gokcimen and B. Das, "A Novel System for Strengthening Security in Large Language Models Against Hallucination and Injection Attacks with Effective Strategies", *Alexandria Engineering Journal* , vol. 123, pp. 71-90, 2025. https://doi.org/10.1016/j.aej.2025.03.030.

[47] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Assessing Mitre Att&ck Risk using A Cyber-Security Culture Framework,” *Sensors*, vol. 21, no. 9, p. 3267, 2021. https://doi.org/10.3390/s21093267.

[48] N. A. Azeez, S. Misra, D. O. Ogaraku, and A. P. Abidoye, “A Predictive Model for Benchmarking the Performance of Algorithms for Fake and Counterfeit News Classification in Global Networks,” *Sensors (Basel)*, vol. 24, no. 17, p. 5817, 2024. https://doi.org/10.3390/s24175817.

[49] Simspace, “Cyber Frameworks for the C-Suit,” 2023.

[50] S. Kanj Bonhard, P. Garcia Villalta, and O. Roses, "A Review of Tactics, Techniques, and Procedures (TTPs) of MITRE Framework for Business Email Compromise (BEC) Attacks", *IEEE Access*, vo 13, pp. 50761 - 50776, 2025. https://doi.org/10.1109/ACCESS.2025.3552523.

[51] S. Wang, " An Analytical Framework for Modeling and Synthesizing Malicious Attacks on Adaptive Cruise Control Vehicles", *Transportation Research Record*, 2025. https://doi.org/10.1177/03611981251320384.

[52] A. Yeboah-Ofori et al., “Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security,” *IEEE Access*, vol. 9, pp. 94318–94337, 2021. https://doi.org/10.1109/ACCESS.2021.3087109

[53] S. M Narayan, N. Kohli, and M. M Martin, "Addressing Contemporary Threats in Anonymised Healthcare Data Using Privacy Engineering", *npj Digital Medicine*, vol. 8, no.1, 2025. https://doi.org/10.1038/s41746-025-01520-6.

[54] A. Nhedzi and C. M Azionya, "The Digital Activism of Marginalized South African Gen Z in Higher Education", *Humanities and Social Sciences Communications*, vol. 12, no. 1, 2025. https://doi.org/10.1057/s41599-025-04535-2.

[55] P. Kumar, R. Kumar, A. Joalfaei, and N. Mohammad, " An Automated Threat Intelligence Framework for Vehicle-Road Cooperation Systems", *IEEE Internet of Things Journal*, vol. 11, no. 22, pp. 35964 - 35974, 2024. https://doi.org/10.1109/JIOT.2024.3397652.

[56] R. Nagahawattan, M. Warren, S. Salzam, and S. Lokuge, " Cyber Security in the Context of Cloud Computing: An Empirical Study of Australian SMEs", *Critical Phishing Defense Strategies and Digital Asset Protection*, pp. 271-294, 2025. https://doi.org/10.4018/979-8-3693-8784-9.ch013.

[57] S. Yulianto, B. Soewito, F. L. Gaol, and A. Kurniawan, "Enhancing Cybersecurity Resilience Through Advanced Red-Teaming Exercises and MITRE ATT&CK Framework Integration: A Paradigm Shift in Cybersecurity Assessment", *Cyber Security and Applications*, vol. 3, 2025. https://doi.org/10.1016/j.csa.2024.100077.