Pak. j. life soc. Sci. (2024), 22(2): 1760-1772 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.2.00123

RESEARCH ARTICLE

The Crucial Significance of Cyber Threat Intelligence in Mitigating Cyber Attacks

Omer Eltayeb Omer Eltayeb*

Alliance Manchester Business School, The University of Manchester, United Kingdom

University of Science & Technology, Sudan

ARTICLE INFO

Received: May 16, 2024

Accepted: Jul 22, 2024

Keywords

Cyber threat intelligence
Cybersecurity
Threat actors
Information sharing and analysis centres
Threat intelligence integration

***Corresponding Author:**

omer.eltayeb@ieee.org

ABSTRACT

Cyber Threat Intelligence (CTI) has risen to prominence in the constantly evolving cybersecurity landscape, playing a pivotal role in the protection of digital systems. Through a thorough examination of intelligence's many aspects and origins, an understanding of this field emerges. Information sharing and analysis centres serve as beacons of collaboration, exemplifying the collective vigilance required to combat such evolving threats. As we know, a threat actor may launch an attack against the system and spread malware. The ultimate objective of this particular cyber security breach is to manipulate, alter, or switch delivery mechanisms. Therefore, CTI must be integrated into existing cybersecurity practices in order to detect and comprehend the intentions and motivations of threat actors against the backdrop of persistent cyber threats. As businesses navigate the complexities of the digital landscape, the prudence of adopting an integrated approach to threat intelligence becomes glaringly apparent. Thus, this in-depth analysis tries to provide a potent instrument for organisations devising robust, adaptable cybersecurity strategies and bolsters knowledge of the defences that protect digital assets from an ever-changing sea of cyber threats.

INTRODUCTION

Cyber risks emerge larger and more alarming than ever before in an era dominated by the rapid digitization of information and services. According to the study conducted by (Clark & Hakim 2017), a cyber-attack can be defined as the denial of service, theft or manipulation of data, and damage to infrastructure caused by a cyber-based attack that may result in significant losses and have repercussions national security, the economy, or the protection of citizens (Clark & Hakim, 2017). Therefore, the escalating sophistication and frequency of these digital hazards have heightened the need for a robust cyber-defense mechanism (Albahri & AlAmoodi, 2023).

In today's rapidly advancing digital age, cyber threats have attained an unprecedented level of complexity. This increase in complexity is predominantly attributable to the proliferation of advanced attack vectors. Utilizing malware deployment, phishing schemes, ransomware attacks, and intricate social engineering strategies, cyber adversaries have refined their techniques to exploit vulnerabilities across a spectrum of

targets (Rains, 2020). Not only do these methods exhibit technical expertise, but they are also meticulously designed to exploit human weaknesses, making them exceptionally effective (Rains, 2020).

Generally, advanced persistent threats (APT) are an advanced and highly targeted form of cyber-attack. APT represents the most sophisticated types of attacks against modern networks, which have proven to be exceedingly difficult to combat. Attackers utilize sophisticated attack techniques to remotely control infected machines and infiltrate sensitive data from organizations and governments. Because of the dynamic nature of the APT attack process, enterprise networks deploying security products based on traditional defenses frequently fail to detect APT infections. (Zimba et al., 2020)

Furthermore, cyber warfare funded by the states and the prevalence and increase in organized cybercrime syndicates prove to be added difficulties in the digital world. In the case of the ever-evolving terrain of cyber threats, new emerging digital technologies such as the Internet of Things and artificial intelligence seem to ignite new competition and dimensions to the cyber threat (Iqbal et al., 2020). As a result, defending against cyber threats has become an increasingly difficult endeavor, necessitating a multidimensional and flexible cybersecurity strategy (Iqbal et al., 2020).

Cyber Threat Intelligence (CTI) entails multiple phases, each of which plays a crucial role in bolstering digital defenses against evolving threats. In the first phase, known as direction, threat intelligence objectives are established. This entails identifying the potential repercussions of interrupting processes, such as shutting down drug markets or terrorist propaganda blogs (Cascavilla et al., 2021). Priorities are established in order to determine what requires protection, such as prioritizing efforts to curtail arms trafficking in order to protect civilian lives. In addition, this phase includes the identification of information assets and business processes that require protection. The subsequent phase, collection, is devoted to information gathering. This entails a variety of techniques, including open-source scanning (e.g., monitoring news, blogs, and markets), crawling and scraping relevant websites and forums, and, in some cases, infiltration of closed sources such as dark web forums. The objective is to collect vital information to inform cybercrime-fighting decisions, particularly within law enforcement agencies (Cascavilla et al., 2021). Processing and analysis, the concluding phases, are interdependent and crucial for transforming raw data into actionable intelligence. In processing, collected data is formatted, filtered for precision, and cleansed of redundancies, thereby making it usable for the organization. This may entail activities such as extracting IP addresses and organizing report files. In the subsequent analysis phase, human-driven processes decode processed data to generate intelligence. This intelligence informs crucial decisions, which could lead to further investigation of a threat, action to prevent an attack, heightened security measures, or even investments. The dissemination phase ensures that the completed intelligence output is communicated to the appropriate stakeholders (Cascavilla et al., 2021). Various categories of threat information are managed throughout this procedure, including indicators, security alerts, threat intelligence reports, and tool configuration data. These accommodate various levels of management and executives, from strategic to technical, to meet their individual needs. Lastly, Feedback is crucial for refining and perfecting the complete CTI procedure. It enables a comprehension of intelligence priorities, guiding data collection, processing, and intelligent analysis. This feedback cycle ensures that the intelligence-gathering process remains adaptable and efficient in the face of evolving cyber threats (Cascavilla et al., 2021).

Moreover, the establishment of collaborations between corporate and governmental institutions is frequently regarded as a fundamental strategy for tackling various cybersecurity governance issues. Such private and public partnerships (PPPs) provide an organizational framework that facilitates enhanced adaptability and cooperation (Christensen & Petersen, 2017). In order to share hazards, a large number of public and private sector actors must be included. Still, some critics, such as Dunn-Cavelty and Suter (2009), claim that PPPs may be perceived as a potential means of delegating responsibility for national security to the private sector (Dunn-Cavelty & Suter, 2009).

On the other hand, CTI is made more effective by specialized platforms and data inputs. These repositories function as receptacles for structured intelligence data, thereby facilitating its incorporation into existing security frameworks. The landscape for acquiring CTI is enriched by various entities, such as commercial

threat intelligence providers, open-source intelligence (OSINT) platforms, and government-sponsored initiatives such as Information Sharing and Analysis Centres (ISACs), thereby providing organizations with multiple routes for acquiring CTI (Nash, 2021).

Critical to CTI is the practice of creating threat actor profiles (Tang et al., 2022). By employing a categorization framework that evaluates adversaries based on expertise, affiliations, and geopolitical goals, organizations can significantly improve the efficacy of their defensive measures. This comprehension facilitates both the prediction of prospective attacks and the attribution procedure.

CTI plays an indispensable function in the realm of incident attribution and analysis. CTI specialists have the capability to identify and attribute cyberattacks to specific threat actors or groups by means of a thorough examination of digital signatures, methodologies, and contextual information (Sun et al., 2023). The acquisition of this knowledge is of great significance in understanding the broader scope of potential threats and formulating targeted tactics for effective response.

CTI plays a key role in combating cyber-attacks, particularly in light of the rapid evolution of the digital ecosystem. The primary objective of this literature study is to conduct a comprehensive analysis of CTI, encompassing its core principles and pragmatic implementations aimed at bolstering cybersecurity defences. By acquiring a deeper understanding of the intricate nature of CTI, companies can proficiently safeguard themselves against current dangers while simultaneously taking proactive measures to counter the strategies employed by forthcoming cyber adversaries.

LITERATURE REVIEW

Defining Cyber Threat Intelligence

The term CTI can be delineated as the systematic undertaking of gathering, scrutinising, and disseminating data pertaining to prospective cyber dangers, with the objective of augmenting an entity's capacity to identify, forestall, and address such threats. The domain of CTI encompasses a thorough investigation and implementation of several fields, encompassing the collection, analysis, and dissemination of information pertaining to potential cyber threats. It functions as the essential foundation of modern cybersecurity strategies, empowering companies to adopt proactive steps in protecting against diverse digital adversaries. In recent times, a multitude of highly secure institutions have been subjected to a series of cyberattacks (Gao et al., 2021). The fundamental concept of CTI centres on the consolidation and integration of data derived from various origins, encompassing network traffic, malware analyses, and open-source intelligence. The compilation of data presented here forms the fundamental basis for deriving practical insights pertaining to potential cyber dangers.

Goal and Scope of Cyber Threat Intelligence

In the studies conducted by (Yeboah-Ofori et al., 2021), the goal of CTI is to provide information about technical indicators, context, motivation, and actionable recommendations pertaining to existing and emerging threats (Yeboah-Ofori et al., 2021). The scope of CTI refers to the extent and range of activities and knowledge involved in identifying, analysing, and mitigating cyber threats. The scope of CTI extends beyond the mere collection of data. The scope of this endeavour encompasses a diverse range of tasks, spanning from the detection and analysis of indicators of compromise (IoCs) to the comprehensive characterisation of threat actors. The utilisation of a diverse strategy allows organisations to get a comprehensive comprehension of the threat landscape in which they are situated. Through a complete analysis of potential vulnerabilities, vigilant monitoring of harmful actions, and the discernment of evolving attack routes, CTI enables organisations to fortify themselves against a wide array of cyber-attacks proactively.

A5TRR

Numerous classifications of CTI are recognised within this discipline. These classifications comprise various intelligence types that are gathered and analysed to identify and mitigate cyber threats. There are three primary categories of CTI: tactical, operational, and strategic intelligence, **Figure 1** (Kure & Islam, 2019).

Figure 1: Types of cyber threat intelligence (Correa)

a) Tactical Intelligence:

Technical CTI is distinguished by its specific concentration on IoCs and technical data associated with cyber threats. This level of granularity enables organisations to identify threats precisely (Montasari et al., 2021). Therefore, it facilitates efficient and targeted mitigation efforts. By utilising technical CTI, organisations are able to fine-tune their security measures and implement protective strategies with laser-like accuracy. This level of accuracy strengthens a company's overall cybersecurity posture, assuring a robust defence against potential threats (Montasari et al., 2021).

b) Operational Intelligence:

Operational CTI facilitates a more comprehensive comprehension of cyber risks through an examination of the tactics, techniques, and procedures (TTPs) utilised by malicious actors (Sun et al., 2023). This thorough analysis surpasses the scope of technical indicators, providing a more expansive framework for understanding the panorama of threats. By comprehending the modus operandi of adversaries, organisations can proactively adjust their defensive strategies, hence increasing the difficulty for attackers to achieve their objectives. The implementation of operational CTI enables organisations to anticipate and mitigate emerging threats proactively, hence strengthening their ability to withstand and adapt to a constantly evolving threat environment.

c) Strategic Intelligence:

The concept of strategic intelligence crucially enlightens the field of cyber security and threat intelligence. It is the process of collecting, analysing, and interpreting data in support of strategic decision-making. Geopolitical, economic, and sociological factors are all taken into account in the thorough analysis of the cyber threat scenario provided by Strategic intelligence (Kure & Islam, 2019). The analysis takes into account worldwide events, geopolitical conflicts, and emerging patterns in the cyber threat landscape. This form of intelligence holds significant importance in the context of long-term planning and policy development, as it allows firms to synchronise their cybersecurity endeavours with overarching strategic objectives effectively. The utilisation of strategic intelligence empowers firms to proactively anticipate and make necessary preparations for the ever-evolving landscape of cyber threats. Organisations can adapt their cybersecurity strategies to mitigate potential risks if they comprehend the geopolitical and socio-political dynamics that may influence cyber-attacks. In addition, strategic intelligence supports resource allocation, regulatory compliance, and risk management decision-making processes. (Nova, 2022).

For a comprehensive and proactive cybersecurity strategy, the effective integration of these three categories of CTI is an essential tenet. Collectively, technical, operational, and strategic intelligence empowers organisations to identify, respond to, and mitigate cyber threats, thereby improving their overall cybersecurity posture.

Sources of Information for Cyber Threat Intelligence

CTI gathers information about potential cyber hazards from a variety of data sources. Structured and unstructured data from numerous platforms and channels are included in these sources. Understanding the CTI data types is essential for the development of a comprehensive and efficient threat intelligence program.

Structured Data Sources

a) Indicators of Compromise:
These are indicators of a possible security incident. They include attributes associated with malicious activities, such as IP addresses, domain names, file hashes, and URLs (Firefly, 2023).
b) Indicators of Attack:
Indicators of Attack (IoAs) reveal the TTPs of threat actors. This includes information about assault patterns, behaviours, and techniques (Anashkin & Zhukova, 2022).
c) Signatures of Malware:
These are distinct identifiers for each variant of malware. They are derived from the analysis of malicious code and used to identify and prevent malware infections (Dugyala et al., 2022).
d) Vulnerability data:
Information regarding known software vulnerabilities and their associated exploits is crucial for identifying potential attack vectors.

Unstructured Sources of Data

a) Open-Source Intelligence:

This is the unstructured source that includes information that is accessible to the general public from a variety of sources, such as news articles, social media, forums, and blogs. (Yadav et al., 2023) OSINT offers valuable context concerning emerging threats, threat actors, and their respective tactics.

b) Dark Web and Underground Forums:
Monitoring illicit online communities can reveal forthcoming cyber threats, planned attacks, and the distribution of hacking tools and services (Schäfer et al., 2019).
c) Incident Reports and Case Studies:
Analysing historical incidents and case studies provides valuable lessons learned and patterns of assault behaviour, aiding in the identification of similar threats in the future.
d) Threat Feeds and Intelligence Sharing Platforms:
Commercial and open-source threat intelligence feeds to aggregate and disseminate real-time threat data, providing organisations with proper information regarding current threats and vulnerabilities.
e) Human Intelligence:
(Maras 2021) claim that the information gathered through direct interactions with experts, security researchers, and dependable industry contacts can provide unique insights into emergent threats and attack techniques (Maras, 2021).
f) Sources for Technical Data:
Analysing network traffic patterns and anomalies can disclose indications of ongoing or impending cyber-attacks. This data source is indispensable for identifying suspicious network activity.
g) Endpoint Logs:
Information from endpoint devices, including antivirus alerts, logs, and system events, can provide crucial indicators of compromise and proof of malicious activities (Divya et al., 2022).
h) Firewall and intrusion detection system (IDS) Logs:
These documents contain details about attempted and successful network intrusions, as well as blocked connections, which may indicate the presence of a threat actor.(Pulyala et al., 2023)
i) Email Headers and Logs:

Email-related data sources provide information about phishing campaigns, malicious attachments, and the origin of suspicious emails.

By combining structured and unstructured data from multiple sources, organisations can develop a comprehensive understanding of the threat landscape. This ultimately strengthens their cybersecurity posture by allowing them to identify, analyse, and respond to potential cyber threats in a proactive manner.

Techniques and Strategies for Gathering Intelligence On Cyber Threats

CTI gathering is a proactive method for assisting organisations in collecting, analysing, and disseminating intelligence; CTI could assist in determining if an imminent attack is likely (Koloveas et al., 2021). For instance, if an organisation experiences 40% of spear phishing or malware attacks according to a threat analysis report, we can assume that the frequency of attacks will increase in the future. CTI requirements could be utilised to assess the system's susceptibility to Known-known, Unknown-unknown, and Known-known attacks (Yeboah-Ofori & Islam, 2019). The following techniques are brought into consideration while gathering intelligence on cyber security breaches.

a) Threat Intelligence Platforms and Feeds:

The utilisation of specialised platforms and feeds is considered a fundamental strategy in the field of CTI. These resources function as repositories for systematically organised intelligence data, facilitating smooth integration into pre-existing security infrastructures. Commercial threat intelligence providers, OSINT platforms, Open threat partner exchange (Open TPX), Your Everyday Threat Intelligence (YETI) and government-sponsored programs such as ISACs are essential sources for obtaining a wide range of timely CTI (Chantzios et al., 2019).

b) Information Gathering and Aggregation:

The process of intelligence acquisition entails the systematic compilation of information from a diverse array of sources. This encompasses organised information, such as IoCs, such as malicious IP addresses and domain names, together with unorganised information obtained from open-source intelligence, dark web forums, and cybersecurity networks. The extensive methodology employed for data collecting serves as the fundamental basis for the efficacy of CTI.

c) The Examination and Correlation of Data:

After the collection of data, it is subjected to a thorough process of analysis and correlation. In order to discover significant patterns and abnormalities, automated methods are utilised in conjunction with human experience to sift through a vast amount of information. This essential procedure functions as a mechanism for linking raw data with actionable insights, requiring the application of advanced analytical methods and specialised expertise in a certain domain.

d) Threat Actor Profiling:

Gaining insight into the attributes and driving forces of threat actors is essential for formulating efficacious defence tactics. This particular element entails the classification of threat actors according to several qualities, including their level of expertise, affiliations, and geopolitical goals (Wood, 2021). By developing an in-depth understanding of the capabilities and intentions of adversaries, organisations can effectively augment their capacity to foresee and effectively plan for potential attacks.

e) Incident Attribution and Analysis:

CTI assumes a crucial role in the process of attributing cyber-attacks to distinct threat actors or groups. The process entails analysing digital fingerprints, strategies, and contextual data in order to ascertain the identity of the offender. The process of attributing incidents is of utmost importance as it offers valuable insights into the wider scope of threats and aids in the development of focused response plans.

f) Intelligence-driven vulnerability management approaches:

CTI enhances vulnerability management by offering valuable insights regarding documented vulnerabilities and associated exploits. This allows organisations to strategically prioritise their patching efforts and efficiently spend resources in order to strengthen their systems against prospective assaults (Samtani et al., 2022). Organisations can increase their overall security posture by allocating resources toward addressing the most significant vulnerabilities.

g) The Implementation of Proactive Measures to Mitigate Threats:

Through the utilisation of CTI, organisations can proactively detect and mitigate possible threats prior to their actualisation. The implementation of defensive measures, such as the establishment of firewall rules, deployment of intrusion detection systems, and utilisation of endpoint protection, may be necessary in this context (Sood, 2023). The implementation of proactive threat mitigation strategies substantially decreases the probability of successful attacks.

h) Incident response guided by intelligence:

By leveraging their knowledge of prospective dangers, organisations can optimise their incident response plans. CTI empowers organisations to cultivate resilient incident response methods, guaranteeing a prompt and synchronised response to cyber occurrences. The adoption of a proactive approach serves to mitigate the impact of assaults and streamline the recovery process.

i) Constant Threat Reporting and Monitoring:

CTI encourages ongoing danger landscape monitoring. The continuous vigilance exhibited by organisations enables them to remain updated on evolving threats and adjust their defensive strategies accordingly (Kayode-Ajala, 2023). Furthermore, CTI facilitates the production of extensive threat assessments, offering stakeholders significant insights into the risk exposure and security stance of the organisation.

Facilitating Collective Defense: The Significance of Information Sharing and Collaboration in Cybersecurity

The practice of CTI sharing exemplifies a collective defence strategy, wherein entities amalgamate their resources, insights, and expertise to combat cyber threats more efficiently. This section endeavours to delve into the substantial significance of information sharing, spotlighting key initiatives such as ISACs, which serve as pivotal facilitators of collaborative efforts.

In the swiftly evolving field of cybersecurity, effective information sharing and collaborative efforts among organisations have become of the utmost significance. The practice of CTI sharing exemplifies a collective defence strategy, wherein entities amalgamate their resources, insights, and expertise to combat cyber threats more efficiently. This section endeavours to delve into the substantial significance of information sharing, spotlighting key initiatives such as ISACs, which serve as pivotal facilitators of collaborative efforts.

This collaborative approach's capacity to expedite threat detection and response is a key component. By sharing CTI, organisations gain access to timely alerts about emergent threats, IoCs, and evolving attack methodologies. This accelerated information flow results in quicker detection and response times, effectively reducing the window of opportunity for cybercriminals. (Chantzios et al., 2019)

In addition, information sharing provides organisations with a more comprehensive view of the threat landscape as a whole. It equips them with knowledge of attacks aimed at comparable industries or sectors, even if they have not been directly targeted. This collective intelligence fosters the ability to anticipate potential threats, thereby fortifying defences proactively.

Collaboration also increases the defensive capabilities of an organisation. Entities are able to develop more comprehensive strategies for the detection and mitigation of threats by leveraging the collective knowledge and experience of a community (Sukhabogi, 2021). This collaborative synergy contributes substantially to the overall threat landscape adaptability of organisations.

The cost-effectiveness of security measures generated by shared intelligence is another advantage. Armed with a thorough comprehension of prevalent attack vectors and vulnerabilities, organisations can allocate their resources prudently (Saeed et al., 2023). This targeted allocation optimises resource utilisation by directing investments in security measures to areas where they are most likely to have the greatest impact.

In addition, the practice of information sharing aligns organisations with regulatory and compliance standards, especially in industries where regulating bodies advocate or mandate such collaborative efforts to strengthen cybersecurity. By actively participating in these collaborative efforts, organisations not only improve their security posture but also demonstrate their commitment to upholding regulatory and compliance requirements.

The integration of information exchange and collaborative initiatives, as exemplified by initiatives such as ISACs, is an indispensable component of modern cybersecurity strategies (Trocoso-Pastoriza et al., 2022). It exemplifies a proactive and unified approach to safeguarding digital assets and infrastructure, empowering organisations to bolster their collective resilience against an ever-evolving threat landscape.

Initiatives Promoting Collaborative Cybersecurity: A Focus on Isacs and Beyond

ISACs play a crucial role in the collective efforts aimed at enhancing cybersecurity. Industry-specific organisations play a pivotal role in allowing the exchange of vital CTI, best practices, and mitigation methods among members belonging to a particular industry.

The Financial Services Information Sharing and Analysis Centre (FS-ISAC) serves as an exemplary illustration. The conference emphasises the financial sector and provides a platform for financial institutions to share insights regarding emerging internet threats. The FS-ISAC provides a secure platform for its members to share intelligence, empowering them to defend against cyber threats targeting the financial sector proactively (Trocoso-Pastoriza et al., 2022).

The Health Information Sharing and Analysis Centre (H-ISAC) plays a crucial role in the healthcare industry. National Health ISAC, which was later renamed the H-ISAC to reflect its worldwide membership, is a global forum for stakeholders in the health industry to share information about potential physical and cyber hazards to sensitive data. The platform provides a space for healthcare enterprises to engage in communication and collaboration around optimal cybersecurity protocols. H-ISAC is essential in protecting the healthcare sector from increasing cyber threats since patient data is so sensitive (Hlávka, 2020).

The establishment of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) represents a significant supplementary endeavour in the field. The emphasis is placed on key sectors that are vital to the development of infrastructure, such as water, energy and transportation. Industrial control systems (ICS) play a vital role in facilitating the operation of critical sectors by serving as a central platform for the interchange of valuable information (Knapp & Samani, 2013). The Multi-State Information Sharing and Analysis Centre (MS-ISAC) is an additional exemplary initiative. It is designed exclusively for state, local, tribal, and territorial (SLTT) administrations. According to (Pescatore 2019), MS-ISAC provides a centralised platform for SLTT entities to collaborate on cybersecurity and share threat intelligence, thereby augmenting the cyber resiliency of these governments as a whole (Pescatore, 2019).

(Daniel and Kenway, 2020) state that the Cyber Threat Alliance (CTA) is a global initiative that unites cybersecurity vendors and organisations. CTA concentrates on sharing threat intelligence pertaining to sophisticated cyber threats (Daniel & Kenway, 2020). By combining their resources and intelligence, CTA members are better able to defend themselves against sophisticated cyber adversaries.

In addition, the Financial Services Sector Coordinating Council (FSSCC) is a noteworthy initiative led by the private sector in the financial industry. It collaborates with government agencies to strengthen the stability and security of the financial sector. FSSCC functions as a forum for dialogue between the public and private sectors on matters pertaining to cybersecurity.

These initiatives, among others, illustrate the diversity of industry-specific and cross-sectoral initiatives to promote information exchange and collaborative cybersecurity measures. These organisations

considerably contribute to the collective defence against cyber threats by fostering trusted communities and providing platforms for intelligence exchange.

Threat Intelligence Integration: Strengthening Cybersecurity Posture

Threat intelligence integration pertains to the seamless integration of up-to-date and comprehensive threat information into an organisation's pre-existing security architecture. This integration enables the organisation to proactively predict, identify, and successfully respond to new cyber threats. The procedure mentioned above entails the incorporation of threat feeds into crucial security elements such as Security Information and Event Management (SIEM) systems, endpoint protection platforms, and firewalls, hence facilitating a proactive and all-encompassing approach to the field of cybersecurity.

Security Information and Event Management Systems

These are advanced technological tools utilised in the field of cybersecurity. These systems are designed to collect, analyse, and manage security-related information and events within an organisation's network infrastructure. SIEM systems are of paramount importance in the detection and mitigation of potential security threats while also aiding in adherence to regulatory compliance requirements. SIEM systems play a vital role in the consolidation and analysis of security-related data across an organisation's network. Incorporating CTI into SIEM systems entails the incorporation of threat intelligence feeds, which include IoCs and IoAs. The approach mentioned above improves the capabilities of SIEM systems by facilitating the establishment of connections between threat data and pre-existing logs and events (Ackermann et al., 2023). Consequently, this enables the acquisition of a comprehensive and contextual comprehension of potential dangers.

Furthermore, through the utilisation of the sophisticated analytical functionalities offered by SIEM systems, organisations can detect trends and deviations that may suggest the presence of possible hazards. The adoption of this proactive approach empowers security personnel to address issues, hence minimising any potential harm immediately.

Endpoint protection platforms

Endpoints are a notable area of vulnerability inside an organisational network. The integration of CTI into endpoint protection technologies represents a notable progression in strategic implementation. This procedure entails enhancing conventional detection methods based on signatures with intelligence-driven indications, enabling the system to detect previously unknown hazards by carefully analysing their behavioural characteristics. This integration extends its functionality by facilitating automatic responses at the individual endpoint level. In the case of detecting a recognised threat, the endpoint security platform promptly responds by segregating the compromised device (El-Kosairy et al., 2023). This proactive strategy serves the purpose of both restricting lateral movement and reducing the possible harm that the attack could cause.

Firewalls and Intrusion Detection/Prevention Systems

Firewalls and Intrusion Detection and Prevention Systems (IDPS) serve as the primary means of safeguarding against external threats. The process of incorporating CTI into these components entails enhancing their rule sets by integrating threat intelligence data. This enables these systems to decide on network flow with more knowledge, enabling them to recognise and stop possibly adversarial behaviour. In addition, organisations can proactively mitigate emerging attack strategies and tactics deployed by threat actors by consistently upgrading their firewall and IDPS rules with the most up-to-date threat intelligence (Möller, 2020).

Security Orchestration, Automation, and Response Systems

It refers to a set of integrated technologies and processes that aim to enhance the efficiency and effectiveness of security operations. These systems enable organisations to streamline their security incident response activities by automating repetitive tasks, orchestrating the many security tools and technologies in use, and facilitating the Security Orchestration, Automation, and Response (SOAR) technologies enable the coordination and mechanisation of security procedures (Lee et al., 2022). Through

the integration of CTI, organisations can develop playbooks that automate response activities according to predetermined triggers (Varma et al., 2023). For example, upon the identification of a particular danger signal, the SOAR system can autonomously isolate impacted systems, commence forensic examinations, and promptly inform the appropriate stakeholders.

DISCUSSION

The extensive investigation conducted in this literature review has shed light on multiple crucial aspects of CTI. Through an in-depth examination of the differentiating factors among technical, operational, and strategic intelligence, this study has contributed to a thorough comprehension of the intricate characteristics of intelligence within the realm of cyberspace. A thorough understanding of this fundamental idea is essential in the development of efficient solutions to mitigate cyber dangers. Moreover, the distinction between structured and unstructured sources of CTI highlights the intricate nature of the data that is accessible. This finding emphasises the significance of using cutting-edge analytical techniques to extract useful insights from the abundance of information sources accessible. The purpose of this study is to deepen comprehension of CTI and underscore the need to uphold scientific rigour in the field of intelligence analysis.

One significant addition to this study involves the examination of various methodologies and approaches employed in the acquisition of intelligence pertaining to cyber threats. This study presents an overview of different methodologies, namely OSINT, human intelligence, and SIGINT, with the aim of improving readers' understanding of the process of acquiring intelligence. Furthermore, it emphasises the significance of implementing a comprehensive and multifaceted strategy in the field of cybersecurity. This insight carries substantial significance within the context of emerging cyber dangers that manifest in diverse forms and vectors.

Organisations can enhance their preparedness in responding to the dynamic tactics employed by threat actors by recognising and appreciating the diverse range of intelligence-gathering methodologies.

The primary emphasis of this review centres on the necessity of collective defence mechanisms, which are accomplished through the exchange of information and collaborative endeavours. The discussion highlights the crucial significance of efforts such as ISACs in promoting a community-oriented approach to cybersecurity. By utilising collaborative platforms, organisations can overcome traditional barriers and enhance their collective ability to withstand and respond to cyber threats. The significance placed on the cultivation of shared situational awareness and coordinated reactions serves as a poignant reminder of the inherent interconnectedness of the digital world.

This literature review's support for the incorporation of threat intelligence into cybersecurity frameworks is arguably its most significant addition. The discourse clearly elucidates the benefits of this methodology, encompassing heightened awareness of potential risks and the ability to take preemptive measures for defence. Organisations may enhance their security measures against an ever-changing threat landscape by integrating intelligence-driven insights into their security postures. The integration plays a crucial role in establishing a strong cybersecurity framework that can effectively respond to evolving attack vectors. Overall, this thorough evaluation of the literature contributes to the advancement of our knowledge of CTI in numerous ways. It not only illuminates the intricacies of intelligence gathering and analysis but also underscores the critical significance of collaborative defence mechanisms in defence integration strategies. By conducting a thorough analysis of these elements, this review establishes a strong basis for organisations aiming to navigate the intricate landscape of cybersecurity with increased resilience and effectiveness.

CONCLUSION

Within the ever-evolving landscape of contemporary cybersecurity, the scholarly field of CTI has emerged as a prominent area of strategic importance. It serves as a crucial element in strengthening our digital defences. By engaging in a methodical examination of the various manifestations and sources of intelligence, a comprehensive perspective of this discipline emerges. The journey not only unveils the

craftsmanship in the methods of obtaining intelligence but also emphasises the importance of taking proactive security measures.

ISACs serve as a booming chorus in this symphony of cyber defence, illustrating the teamwork needed to counter emerging threats. In light of the intricate nature of the digital environment, organisations are increasingly recognising the importance of adopting a comprehensive strategy for threat intelligence. This comprehensive analysis serves as a powerful tool for organisations to develop strong and flexible cybersecurity strategies, enhancing the defences that protect our digital assets in the face of constantly evolving cyber threats.

DECLARATIONS AND STATEMENTS

Funding: No funding sources are reported

Ethical Approval: Not applicable

Conflict of interest: The author does not have any conflict of interest.

Author Biography

Omer Eltayeb, a dedicated researcher, and former Cloud Solution Architect at Microsoft, focuses on cutting-edge cybersecurity issues. His research interest showcases his commitment to addressing pressing challenges in digital security. Omer's is currently affiliation with the University of Science & Technology underscores his dedication to higher education and scholarly pursuits. Through his work, he aspires to contribute valuable insights that enhance cybersecurity strategies and foster a safer digital landscape. Omer Eltayeb is also an active IEEE member (Membership: #100379961) under the affiliation of Europe, Middle East, and Africa Region (Region R8) acting as section Co-Lead and focuses on Technology Research and Devolopement.

BIBLIOGRAPHY

Ackermann, T., Karch, M., & Kippe, J. (2023). Integration of Cyber Threat Intelligence into Security Onion and Malcolm for the use case of industrial networks. *at-Automatisierungstechnik*, *71*(9), 802-815.

Albahri, O., & AlAmoodi, A. (2023). Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database. *Mesopotamian Journal of CyberSecurity*, *2023*, 158-169.

Anashkin, Y., & Zhukova, M. (2022). Implementation of Behavioral Indicators in Threat Detection and User Behavior Analysis. CEUR Workshop Proceedings,

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W.-J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258.

Chantzios, T., Koloveas, P., Skiadopoulos, S., Kolokotronis, N., Tryfonopoulos, C., Bilali, V.-G., & Kavallieros, D. (2019). The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform. DATA,

Christensen, K. K., & Petersen, K. L. (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affairs*, *93*(6), 1435-1452.

Clark, R. M., & Hakim, S. (2017). Protecting critical infrastructure at the state, provincial, and local level: issues in cyber-physical security. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, 1-17.

Correa, A. *Three Types of Cyber Threat Intelligence*. Malware Patrol. Retrieved 21 december from

Daniel, M., & Kenway, J. (2020). Repairing the foundation: how cyber threat information sharing can live up to its promise and implications for NATO. *Cyber Threats and NATO*, *2030*, 178.

Divya, P., George, R. S., Madhusudhan, G., & Padmasree, S. (2022). Organization-wide IOC Monitoring and Security Compliance in Endpoints using Open Source Tools. 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT),

Dugyala, R., Reddy, N. H., Maheswari, V. U., Mohammad, G. B., Alenezi, F., & Polat, K. (2022). Analysis of malware detection and signature generation using a novel hybrid approach. *Mathematical Problems in Engineering*, *2022*, 1-13.

Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179-187.

El-Kosairy, A., Abdelbaki, N., & Aslan, H. (2023). A survey on cyber threat intelligence sharing based on Blockchain. *Advances in Computational Intelligence*, *3*(3), 10.

Firefly, B. (2023). RFC 9424 Indicators of Compromise (IoCs) and Their Role in Attack Defence. *Assessment*, *3*, 3.

Gao, P., Shao, F., Liu, X., Xiao, X., Qin, Z., Xu, F., Mittal, P., Kulkarni, S. R., & Song, D. (2021). Enabling efficient cyber threat hunting with cyber threat intelligence. 2021 IEEE 37th International Conference on Data Engineering (ICDE),

Hlávka, J. P. (2020). Security, privacy, and information-sharing aspects of healthcare artificial intelligence. In *Artificial Intelligence in Healthcare* (pp. 235-270). Elsevier.

Iqbal, F., Debbabi, M., Fung, B. C., Iqbal, F., Debbabi, M., & Fung, B. C. (2020). Cybersecurity And Cybercrime Investigation. *Machine Learning for Authorship Attribution and Cyber Forensics*, 1-21.

Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in Financial Institutions and Challenges in Its Adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21.

Knapp, E. D., & Samani, R. (2013). *Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure*. Newnes.

Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., & Tryfonopoulos, C. (2021). intime: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. *Electronics*, *10*(7), 818.

Kure, H., & Islam, S. (2019). Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *Journal of Universal Computer Science*, *25*(11), 1478-1502.

Lee, M., Jang-Jaccard, J., & Kwak, J. (2022). Novel Architecture of Security Orchestration, Automation and Response in Internet of Blended Environment. *Computers, Materials & Continua*, *73*(1).

Maras, M.-H. (2021). Industrial Control System. In *Encyclopedia of Security and Emergency Management* (pp. 441-443). Springer.

Möller, D. (2020). *Cybersecurity in digital transformation: Scope and applications*. Springer.

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

Nash, A. (2021). *Demystifying Cyber Threat Intelligence Sharing Platforms: An Evaluation of Data Quality Issues and Their Effects on Cyber Attribution* Utica College].

Nova, K. (2022). Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence. *International Journal of Information and Cybersecurity*, *6*(1), 21-42.

Pescatore, J. (2019). Sans top new attacks and threat report. *SANS Institute*.

Pulyala, R., Boorgam, S. Y., & Kakarla, G. (2023). Advanced Machine Learning Boosting Strategies for Improved Intrusion Detection Performance.

Rains, T. (2020). *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Packt Publishing Ltd.

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 7273.

Samtani, S., Chai, Y., & Chen, H. (2022). LINKING EXPLOITS FROM THE DARK WEB TO KNOWN VULNERABILITIES FOR PROACTIVE CYBER THREAT INTELLIGENCE: AN ATTENTION-BASED DEEP STRUCTURED SEMANTIC MODEL1. *MIS quarterly*, *46*(2).

Schäfer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M., & Lenders, V. (2019). BlackWidow: Monitoring the dark web for cyber security information. 2019 11th International Conference on Cyber Conflict (CyCon),

Sood, A. (2023). Defensive cyber security: continuous controls enforcement and infrastructure hygiene. *Network Security*, *2023*(8).

Sukhabogi, S. (2021). A Theoretical review on the importance of Threat Intelligence Sharing & The challenges intricated. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(3), 3950-3956.

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials*.

Tang, B., Wang, J., Yu, Z., Chen, B., Ge, W., Yu, J., & Lu, T. (2022). Advanced Persistent Threat intelligent profiling technique: A survey. *Computers and Electrical Engineering*, *103*, 108261.

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

Varma, A. J., Taleb, N., Said, R. A., Ghazal, T. M., Ahmad, M., Alzoubi, H. M., & Alshurideh, M. (2023). A Roadmap for SMEs to Adopt an AI Based Cyber Threat Intelligence. In *The Effect of Information Technology on Business and Marketing Intelligence Systems* (pp. 1903-1926). Springer.

Wood, P. (2021). Socio-technical Security: User Behaviour, Profiling and Modelling and Privacy by Design. *Challenges in the IoT and Smart Environments: A Practitioners' Guide to Security, Ethics and Criminal Threats*, 75-91.

Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. *Artificial Intelligence Review*, 1-32.

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future Internet*, *11*(3), 63.

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

Zimba, A., Chen, H., Wang, Z., & Chishimba, M. (2020). Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics. *Future Generation Computer Systems*, *106*, 501-517.