Pak. j. life soc. Sci. (2024), 22(2): 1883-1904 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-2024-22.2.00132

RESEARCH ARTICLE

Cyber Defense Using Cyber Threat Intelligence to Anticipate and Avoid Future Cyber Attacks

Omer Eltayeb Omer Eltayeb*

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

University of Science & Technology, Sudan

ARTICLE INFO

Received: Apr 30, 2024

Accepted: Aug 10, 2024

Keywords

Cyber attacks

Cyber security

Cyber threat intelligence

Threat intelligence

***Corresponding Author:**

omer.eltayeb@ieee.org

ABSTRACT

This study evaluates the efficiency of cyber threat intelligence (CTI) for predicting and mitigating cyber threats, which is important in business today. Organisations endure cyber assaults and fight cyber crimes, which threaten commercial exposure. CTI is a proactive approach to these risks since it gives the finest methods and relevant information on potential cyber crimes. This review article analyses the literature in the context to find gaps and include ethical research practices. This systematic study may determine how threat intelligence improves cyber security knowledge and eliminates cyber threats by examining assessable information. It may guide the development of new threat intelligence-influencing methods and frameworks. Through a qualitative approach based on the systematic review, the study goals were evaluated, analysed, and explained. PRISMA chart was also used to describe exclusion and inclusion study criteria to ensure correct data gathering. The results were presented in a thematic analysis while examining article dependability, quality, and validity. The author used inductive research to reach the primary study conclusions. Using observations or data, inductive inquiry creates hypotheses or generalisations. Threat intelligence may considerably increase an organisation's ability to anticipate and prevent cyber threats. The literature emphasised that threat information improves incident response, identifies new threats, and strengthens cyber security. Organisations should continually train and educate cyber security personnel to increase threat intelligence utilisation. Instruct incident response, threat intelligence analysis, and emerging threat trends.CTI helps a company grow smoothly and achieve its goals.

INTRODUCTION

In the modern era, cyber attacks have become more sophisticated, frequent, and effective, posing a serious threat to businesses and other organisations and entities to exploit computer system weaknesses, disrupt operations, compromise data and information, and cause financial and reputational harm. To tackle these ever-changing cyber threats, firms invest in cyber threat intelligence (CTI) to anticipate and prevent cyber assaults. The procedure of assembling, analysing and interpreting the information and data concerning the stable and potential cyber threats is called CTI. CTI regulates a group and investigation of information and data from numerous resources, with open-source intelligence, dark web monitoring, threat feeds and mutual distributive platforms. With another capability of CTI to harness, many business organisations search for actionable approaches for promising threats, cyber attacker approaches, and Indicators of Compromise (IoCs) to increase their cyber defensive capabilities for the organisation's reputation (Samtani et al., 2020).

Despite the modern growth in CTI implementation, assessing the intensity of how well it can work in mitigating or avoiding cyber threats is essential. For organisations and business entities looking to expand strong and protective cyber security postures, considering the pros and cons of CTI is crucial. A logical and objective literature review is provided by a systematic review, which also synthesises the consequences of various studies to offer insights on the effectiveness of CTI as a cyber defence approach.

This systematic review evaluates how well cyber threat intelligence prevents and detects online attacks. We intend to determine the present state of knowledge and resolve knowledge gaps on the role and impact of CTI in cyber security by thoroughly analysing recent peer-reviewed literature. The consequences of this evaluation will be helpful for business entities and researchers concerning the pros and cons and finest practices of incorporating CTI through their cyber defensive plans. The research focuses on the PRISMA standards; only the publications of journals between 2021 and 2023 are used in the research paper to evaluate and investigate the efficacy of CTI for anticipating and avoiding cyber attacks. The following portions of this work will involve an in-depth examination of the literature, methodology and a discussion of the results. We search to add to the pool of knowledge, enhance decisions based on evidence, and help organisations in their efforts to improve their cyber defence capabilities through the tactical execution of CTI by carrying out this systematic review.

1.1 Problem Statement

Cyber attacks are becoming more frequent and advanced, threatening companies and people's security and balance in today's linked society. To tackle these dangers, CTI provides timely and relevant information to anticipate and mitigate cyberattacks. Despite CTI's growing use, it's necessary to assess its efficacy in predicting and mitigating cyber assaults. This study seeks to fill this information gap by rigorously and methodically evaluating the literature to determine if CTI provides actionable insight that helps prevent and mitigate cyberattacks. The aims and objectives of the research:

The foremost aims or objectives of this research paper are given as follows.

- To identify the key components of CTI
- To identify CTI's contribution in anticipating and avoiding cyber attacks
- To find out the efficacy of CTI in identifying and responding to emerging cyber threats in real-time
- To determine the best practices for implementing a CTI program within an organisation for maximum effectiveness.
- To provide measures for a comprehensive approach to cyber defence with the help of existing security measures.
- To identify gaps, suggest future research, and outline limitations for improved cyber protection using CTI. This will provide a clear direction for future researchers.

1.2 Research Relevance

This research aims to assess the efficacy of CTI in anticipating and mitigating cyber assaults that have significant relevance in the contemporary corporate landscape. Organisations encounter cyber assaults, with personnel often at the forefront of combating these cyber crimes, which persistently pose a danger to the exposure of the organisation's business. CTI is an effective strategy for combating such threats since it offers optimal methodologies and practical information about potential cybercriminal activities. The assessment of the efficacy of CTI has emerged as a crucial consideration for corporate organisations due to many factors. Furthermore, assessing this systematic study has significant benefits for informing policy decisions inside a specific company focused on cyber security. It enables experts in this field to identify and implement effective solutions to mitigate cyber risks. Organisations may consider investing in cyber security to enhance the firm's operational efficiency and overall well-being.

1.3 Research Significance

This review paper provides a broad and structured inspection of the current literature of the provided context, enabling the researcher to find the gaps and input the righteous practice for research purposes. As a result of analysing the assessable information, this systematic review can obtain informative approaches to the efficacy of threat intelligence in increasing the knowledge of cyber security and eliminating the possibility of cyber attacks. It can be helpful for future consideration and guidance for expanding new methodologies and frameworks for influencing threat intelligence. For various reasons, the viewpoint of CTI efficacy has become crucial for corporate organisations. In addition, a particular organisation's policy-making process can benefit from evaluating this systematic study, as cyber security experts can use it to determine the best methods for reducing cyber dangers.

2. LITERATURE REVIEW

The literature review involves a detailed review of the topic that demonstrates in the shape of academic research a domain is selected for writing research for a specific context to enhance the knowledge and understanding of a certain area. This article examines threat intelligence's ability to predict and prevent cyberattacks. Thus, literature evaluations on the potential of threat intelligence solutions in businesses and other entities have emerged to uncover the most important results to safely and securely retrieve study data. In this segment, the systematic review presents literature evidence that may be obscure as a compound aspect of the study to wrap up the primary goals from 2021 to 2023 peer-reviewed journals. The literature review format includes important component explanations and contextual reviews.

2.1. The Components of the Research Topic

a. Cyber attack

Cyber–attacks are wicked activities or unethical frameworks that officially target computer software, networks any digital roads that are related to the privacy of any person or business organisation with the immoral intention to get access to a particular computer or network to disrupt the operations, steal the information or important data that can cause harm and the security is compromised. These cyber-attacks take advantage of susceptibility in the computer's software or maybe human behaviour, for they sacrifice the privacy and integrity of the available online assets. Hackers scatter many cyber attacks, including phishing attacks, data breaches, etc. The main reason behind these attacks is the financial gain of a certain organisation or any other body.

b. CTI

CTI gathers, analyses, and transmits cyber threat information. It involves collecting and analysing data from security feeds and threat intelligence platforms to understand the CTI background's aim and methods.

Here are some aims or objectives of the threat intelligence:

- Identifying and gathering the data and information. Includes the threat performers, which motivates them and how they access their capabilities.
- Analysing the collected for estimating the potential display of the wicked activities.
- Contextualising the relevant data and considering the threat's background, including potential assaults and targeted segments.
- Prioritising the resources and accessing the intensity of the cyber threats.
- Defending the threats before they cause harm to the organisation facilitates the organisation in mitigating and anticipating the cyber attack.

c. Cyber security

Cyber security is defending computer systems from cyber-attacks and defeating the disclosure of confidential information from organisations. It refers to implementing security measures to control cyber threats by implementing several strategies and maintaining decorum for the organisational information.

Here are some points of cyber security

- It is important for the organisation or any business entity to access the responsive information to the lawful person or body and protect it from the unauthorised entity.
- Maintaining the important information's correctness and consistency in the organisation and avoiding unofficial modifications.
- Identifying the potential risk is another subject, and there should be vulnerable measures to avoid them.
- The timely detection of cybercrime can diminish the risk of damage, and there can be room for the investigation process.
- A security awareness program is helpful for the employees of the organisation to help them educate about cyber assaults and how these assaults can be anticipated and avoided. (Kotsias et al., 2023).

2.2. Introduction to Threat Intelligence and Cybersecurity

According to (Goel, 2022), cyber threat intelligence is information a company or an organization uses to consider and understand the threats and diminish their effects. The information of CTI is used for identifying and avoiding cyber threats to obtain benefits from the susceptible information. It can only be recognized with an experience-based understanding and data concerning the cyber threats, assessments of the threats, and performers. There are numerous definitions of intelligence in the previous papers. The CTI provides investigated and organised data about the current situation. It indicates future threats and also records the data from past incidents. Those recordings are committed to being stored in a memory by the CTI, which can identify the future directions of the threats affecting the organisational goals. The CTI always provides in-depth knowledge. Ultimately, the potential can be obtained by cyber threat intelligence. Apart from research implementations on CTI, government employees and other entity bodies use CTI execution and accomplishment as a routine activity because it directly impacts the growth of their business organisations and also because they recognise the importance of cyber security. Developing in this linked world necessitates businesses to conduct cyber security operations and set up staff employees to benefit their business entities.

It is significant for business entities or organisations to learn about the risks of cyber threats, such as these kinds of assaults are zero-day assaults, for instance, the exploits, bonnets and viruses that can be used as a measure reason for hacking. The CTI and the activities can detect many visible threats and then be shown to diverse organisations for introducing the methods and safety cautions they can take. As a result, this can provide knowledge for the defence in the cyber battle, as these assaults can cause real damage to organisations or even institutions. It is the gratitude of Cyber threat intelligence since the wide-ranging and profound analysis is done to help the organisations from the attacks mentioned above.

According to (Van Haastrecht et al., 2021), discussed about the new technology about cyber security of the SME(Small Medium Enterprises) groups advancement from the slightest established start-ups to the most established digital enablers, the SME s are matured enough and has become advanced enough that we might anticipate digital marketers to get such built-in and computerised cyber precautions measures where they are starting to identify and be recognised by the relevance of cyber security, there is always a call for of CTI because till now in this digital era of the world, the digital enablers are constantly little doubtful since due to new technologies, the digital enablers have to follow the up-to-dated rules and the previous obsolete technologies, CTI plays a crucial role in the management of cyber security by tracking and evaluating the continuous internal security information, the new group has been added called “Large enterprises” to mixed up with the other strategies which does not fit with SME assembly.

A potential of CTI is that it makes it possible to inform us about cyber attacks and stores data backup for security measures; it also modifies its performance as a prompt response to the response before cyber attacks on the battlefield against the performance of cyber threats. Actionable CTI has numerous characteristics such as prioritise, accuracy, just-in-time, efficient response and applicability. There are three strategic phases of the actionable CTI: strategic, tactical, and operational intelligence.

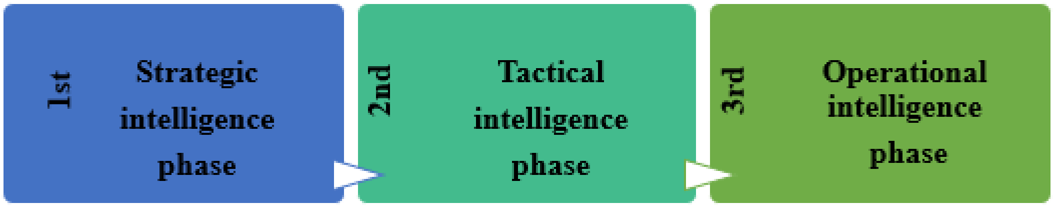
1st
Strategic intelligence phase
2nd
Tactical intelligence phase
3rd
Operational intelligence phase

Figure 1: shows the phase of actionable CTI

The first phase deals with the non-procedures and expresses the purpose behind the threats or cyber-attacks. It seeks for the individual to recognise a certain individual for the cyber attacks and their actual or obvious aims. The second phase produces the reports as evidence or indicators and obtains consultation for the reported threat. The third and last phase deals with how the cyber attack breaks the chain, which means signifying the threat performer by TTPs (Tactics, technique and procedures), which assist in recognising the particular in-sequence information about the cyber attack. Actionable CTI also categorises the intensity of the threat and incident responses to avoid the threats by using machine-understandable data, which refers to IOC such as URLs, IP addresses and hashes. The operational intelligence phase also focuses on the time and nature of the cyber attack. It can use personal or public resources such as the dark web and chats for research or investigate the communication ways of the cyber attacks to mitigate and avoid future cyber attacks.

The Artificial Intelligence applications at various stages of CTI, for example, operational and tactical intelligence, enlighten that tactical threat intelligence is more suitable for the multi-agent structure than operational threat intelligence is suitable for the recurrent neural network. Artificial intelligence is the amalgamation of machine learning, and cyber threat intelligence allows accurate cyber threat deception with lesser computation.

A newly made machine learning-based model is used with a Naïve Bays classifies to detect the exact prospective threat intelligence by the structured data resource and which can predict threats with 96% level of accurate data. Using AI and ML, the research explains the architectural model of CTI with the components of data collection, data processing, and model generation demonstrated in the research (Dutta & Kant, 2020).

The accurate stakeholders obtain operational, tactical and strategic phases of threat intelligence by the threat intelligence team, providing a consistent and trustworthy routine feed. In the first phase, the threat intelligence workforce actively controls the warning landscape by feeding actionable threat intelligence towards SOC forecaster (for example, blocking IP addresses, disturbance in security levels and others.), In the second phase of Threat Intelligence, the workforce of threat intelligence depicts the threat action and confirms in opposition to the observation to the next level. In the last phase, the workforce of Threat Intelligence recognises new threat performers and tactics, TTPs applied by them to classify and address gaps in the organisation's cyber threat defence, which can be shown. (Kotsias et al., 2023)

2.3. CTI Approach and Its Role in Anticipating Cyber Attacks

Within the previous few years, artificial intelligence procedures or techniques have successfully detected many problems in various application domains. In this new digital era, applications like robots, cyber security, and social media are introduced worldwide. There are various potential AI real-world applications in different fields, and also that are under the provision of AI potential techniques such as machine learning, deep learning and reasoning of natural languages, expert system modules, knowledge discovery and many others. The conception behind this threat intelligence is sharing the information and permitting proactive cover over cyber attacks, which is the key factor of CTI. When there is enough information for communication, CTI can detect the characteristics of risks and respond to them with suitability accordingly when the resources are recognised. After the expectations are positioned and the threats are clear, threat intelligence is undoubtedly an effective tool for these attacks. There should be an audit plan incorporated as a part of it. The objective for execution of the plan is already stated in the strategy, with what should be integrated or protected. This also defines what spots are most likely to be assaulted. CTI is used at the difficult stages where thwarting cruel activities is used to indicate threats, which specifies performing patch management in which it is explained to organise the event in such a way as to maintain the level of response and reactions also suggestions.(Zhiqun, 2023)

The information is delivered in a structured format along consistent methods with clear and actionable stages. An organisation must complete the entire plan before appropriately executing the threat intelligence.

a. Community-based approach

According to (Zhiqun, 2023), the community-based approach included parts of the intelligence community validating threat information to ensure the quality before spreading it among the members of the community-based approach. There are some requirements, for instance, the threat information expression (STIX) in a structured form. This language is a standard language-based structured-based demonstration of threat intelligence. The STIX language is produced by MITRE, which is used to record, specify, classify and communicate information. This approach uses language, adaptable, accessible, and human-readable. The flexibility of STIX makes it more approachable for wide-ranging applications. The collection of proven threat information involving measurements, identifications, incidents, exploitation of the targets, and threat performers is defined as an expression of CTI.

b. The risk-based approach

This approach is a structure of the threats that have already been faced before and is an amalgamation of vulnerability, effects and threats. So, this approach is an understanding of the previous threats. Plenty of nations in the world have made their frameworks to protect themselves from cyber threats and deal with the definite industries and threats they have faced. Usually, in many countries, red team practices are carried out with the help of self-governing contributors associated with government institutions. The proactive attacks are pretended in real-world life to indicate or predict future attacks and how to depict them with the help of CTI. (Joel,2021)

For the United Kingdom's financial business world, the Bank of England created CBEST in 1974, as defined by CREST, to assess financial institutions' risks. They discovered a technique: CBEST is a technique for possible risk threats. The stakeholders carried out the inspired testing. The threat intelligence-based Ethical Red team (TIBER-NL) is a group that conducts operations in the Netherlands. Other sectors in the UK include CBEST for government organisations and are best for the telecommunication industry.

c. Narrative-based approach

This approach involves detailed information that portrays incidents related to the organisation's intrusion or events.

According to (Samtani et al., 2022), different academic studies have been inspired to build understandable Artificial Intelligence (XAI) methodologies by systematic methods involving AI. First and foremost, there are two forms of XAI: post-hoc and intrinsic techniques and reasoning paths, masks, and graphs in others, incorporated by using the models of intrinsic XAI strategies. XAI techniques are in action right after the model of intrinsic is being trained and ready to use. Post-hoc techniques are visualisation, surrogate models, significance of concepts and others. These examples of this approach are often perceived as model-agnostic approaches to be clear about the different parts of a model after it has converged. Despite the establishment of XAI, many AI-enabled CTI applications are still independent of the outdated methodologies of the black box.

2.4. Tools and Techniques of CTI

A rising number of organisations or business entities are implementing Artificial Intelligence in their daily course of business life with (AI)-)-enabled methods for enhancing or improving present CTI practices. AI-enabled analytics have been subjected to modification or shown in their studies about extracting meaningful models and patterns from a large amount of information and data from cyber security automatically. There are many other presently used AI-enabled analytics techniques that, for the most part, have built on deep learning (DL) are over and over again the black boxes that fail to clarify how the model reached its final consequences.

There is a lack of understanding in the context of CTI, which can cause severe damage to AI acceptance, trust, model tweaking and model performance with the other considerations. (Samtani et al., 2022) An advanced persistent threat (APT) is a disguised threat performer that gets unofficial computer system usage and avoids detection for an extended period. These kinds of threats are frequent nationwide states and associated with the government of a particular country. APT represents unknown cyber attacks in cyberspace, which is spreading worldwide and exhibit a sequence of complex competition and game playing scenario between the nations. To protect from such cyber-attacks, security researchers have recommended CTI, and IOCs send a word of warning before the threats when the computer system meets up with unknown or suspicious threats. In 2014, essential information concerning a previous or ongoing cyber attack or security incident response was verified by security researchers as CTI.

An Indicator of Compromise (IoC) is a term that is used to demonstrate sample information or data prove the self-assurance of workers or security employees when they encounter network threats and describe the harmful cyber attacks or activities of the threat performer in the APT space. IPs (IP addresses), hashes, domains, emails and others are the commonly found IoCs while APT text analysis. Using IoCs to investigate APT threat intelligence content permits creating an aggregate overview to track or detect the cyber attack or any other activity with the help of a relative matrix and also increases the knowledge about how things are going in cyberspace.

The industries are presently spending on normalising CTI to maintain the adversary emulation along with various security actions. There are different forms of it, such as STIX and TAXII, but still, CTI comes up in unstructured formats such as natural language, incident reports prepared by security forecasters, and other essential texts or reports hacked by employees working inside the organisation from cyber attack groups. As a result, to enable adversary emulation with automated instruments, CTI needs to be processed into a structured format. (Orbinato et al., 2022). CTI must be recognised and identified by the machine learning approaches. The most important problems in Cyber security are spam revealing, malware and interruption due to the interruption detection systems; it enables recognition of unofficial or unauthorised entry access in cyberspace. The procedure of scrutinising the computer and files for malware is called malware detection. (RANA & PATIL, 2023)

Network security is one of several reasons to use Cyber Threat Intelligence. Malware Sharing Platforms (MISP) were created to communicate these threat intelligence data. There are many abilities of these platforms. One of them is that it generates rules for the unknown cyber attacks detected by the system. MISP is a centre and a structure that can produce various attributes to the demonstrated network actions, such as IP or MAC addresses, as described by previous research.

On the other hand, due to their volatile nature, IoCs loses their worth over time; as noted by Iklody et al., the IP name domains can be changed, can be cleaned up by themselves, and also it can be exchanged in an unsafe manner, by the cause of an infected machine. IoCs can only depict a hint of cyber threat and may change in time because of their unreliability. Traditional and deep learning approaches have been examined to boost identification accuracy.(Preuveneers & Joosen, 2021).

There is plenty of research that focuses on IoCs by assembling unstructured open-source CTI (OSCTI) to extract the indicators; the quality of OSCTI can be detected by the tactics, procedures tec, techniques and other formats that are used by them, focusing on producing CTI from network incidents for the enhancement of visualisation. Actionable CTI in the circumstance is an ability to respond while the network incidents are using the knowledge obtained by CTI. It had to be accepted by the previous studies that there is always a requirement for actionable formats of CTI of consumption of CTI while incident response and that formats will leave it with great worth. J. Liu et al. introduced an activated mechanism to build an Actionable CTI discovery system. It portrays a connection between campaign phases and IoCs for producing actionable CTI from the records of Intelligence through NLP. (Cristoffer Leite, Jerry den Hartog, Daniel Ricardo, 2023)

Deep neural networks (DNN) and Machine Learning (ML) models are the most challenging. However, they can better express and describe best what represents a cyber threat; for example, it is easier for the decision tree to describe a threat best and even demonstrate the criteria over the qualities and signals of the presence of the threat. The ML models are categorised in their own way; they might have come with built-in threats that can expand the assault surface of any security system taking on the AI strategies.(Preuveneers & Joosen, 2021)

An Internet of Things (IoT) set of connections is a mixed network of several devices using different types of protocols connected diversely. However, these kinds of varied sets of connections allow the cross-platform type of communication linking different diverse interfaces. Still, unfortunately, among so many interfaces, it allows cross-platform even though it is a diversified network. Additionally, it puts the security of the network at risk. IoT networks are very less protected because of the broad consumption and connectivity of the device; the private information and data from these devices are practised on vulnerable servers that can effortlessly be violated. Even though edge computing is present, there is always a need for typical procedures for safety. (Ms. Pragati Rana, 2023).

IoT tools are increasing in popularity and importance in this new digital era. These tools are now found almost everywhere in daily life, including in homes, workplaces, commercial spaces, businesses, educational institutions, airports, and other places where their on-demand, secure services are needed. The ability to collaborate and receive recognition for the basics and effects of company activity has improved in recent years. Additionally, IoT research and data information processing enhance industry infrastructure and productivity. IoT systems now use eco-friendly technologies to enhance numerous industries. Numerous businesses and organisations have implemented safety measures. (RANA & PATIL, 2023)

CTI is a productive, protective approach that contains artificial intelligence representation to acknowledge the cyber attacks and secure information and data of IoT enabled MTS competently; as you would have thought, there are plenty of CTI-based solutions that practice the physical examination to extract the accurate threat data and information which has a less finding and more wrong pace of alarm. For the reason that to deal with the problems mentioned above, a computerised structure called DLTIF is created to represent CTI and recognise the forms of cyber threats. (Kumar et al., 2021).

A CTI was presented by Samtani et al. to enhance the present reactive position of security devices by totalling up a more practical approach. The approach is completed by consuming CTI solutions systems, which assemble and observe information and data from dark web forums through Latent Dirichlet Allocation (LDA) and SVM representative models. This information and data result from a dashboard boundary to visualise the threat performers and assets to the students and forecasters in cyberspace. Nunes et al. also introduced another CTI solution system to assemble the data and information from the threat performer's forum and those marketplaces over the dark web. This system recognises accurate data and information from different resources, for instance, posts and other product-obtainable information concerning wicked threats. It is observed that comparable to the clarinet social networking forces. It was ordinary for a threat performer to be on several sites with the proper system. This makes it easier for them to spread their products to the mass market. It explains that an extensive perspective is needed to review every potential threat to clearnet services. The same is true of dark net services.

The firm can implement CTI with the centralised team. It should train its employees to gather intelligence resources from nationwide and global security and other legal enforcement actions, the threat intelligence merchant, and a closed group of intelligence experts with the fiscal sector. The chief of the team of Threat Intelligence gathers and analyses the threat intelligence from the resources and implements the adversarial philosophy and the frameworks, such as the "Kill-Chain," a procedure for cyber attacks, which will supply reliable, well-timed, and focused suggestion in the shape of actionable CTI and organisational insights as well for the analyst of security in SOC (Kotsias et al., 2023).

2.5. Research Gap

The literature review has given a comprehensive view of the potential of threat intelligence in anticipating and avoiding cyber attacks from cyberspace in computer systems; it is acknowledged widely and smoothly. Further enlightening is emphasised on the importance of the long-term effects of the potential of cyber threat intelligence and how it gets sustainable at its own pace. There is less research on long-term effects and investigations about future threats targeting the growing capacity of threat intelligence. Business entities and organisations must understand the importance of it and how the strategies are sustained; this will assist the researchers in future research.

3. Research Methodology

The research methodology is an essential and interconnected chapter that plays a key role in managing the research outcomes validly and reliably. The process incorporates identifying, selecting, processing and analysing the information in a related research context. The following chapter is presented to achieve the research aim, which is exploring the potential of threat intelligence for anticipating and avoiding cyber attacks: a systematic review. The underlying purpose of research is to evaluate the effectiveness of CTI to anticipate and mitigate the cyber attacks that are highly relevant in today's business world. Organisations face cyber attacks, and the employees are mostly highlighted while battling with cyber crimes, and they continue to threaten organisational business exposure.CTI is a proactive approach to battle these kinds of threats since it provides the best approaches and actionable data concerning prospective cyber crimes. The perspective of the effectiveness of CTI has become fundamental for business organisations for different reasons. Therefore, to achieve the findings of this aim, the qualitative approach-based systematic review has been done to evaluate, analyse and explain the main research findings. A PRISMA chart was adopted to explain parameters in compliance with exclusion and inclusion research criteria to ensure accurate data collection. A part form that the data was presented in the form of a thematic analysis while assessing the reliability, quality and validity of the articles.

3.1. Research Questions

In purpose to achieve the research's main agenda, the research questions to be addressed are initiated as follows:

Q1. What are the key components of CTI, and how do they contribute to anticipating and mitigating cyber attacks?

Q2. How effective is CTI in identifying and responding to emerging cyber threats in real time?

Q3. What are the best practices for implementing a CTI program within an organisation to ensure maximum effectiveness?

Q4. How can CTI be integrated with security measures to provide a comprehensive approach to cyber defence?

3.2. Research Approach

The author has incorporated an inductive research approach to accomplish the main research findings in this study. The inductive research technique uses particular observations or facts to create hypotheses or generalisations. For several reasons, employing this methodology in systematically examining threat intelligence's potential for predicting and thwarting cyber attacks is reasonable. First, as the subject is exploratory, an inductive method enables the discovery of new patterns or insights that may aid in creating novel theories or conceptualisations. Second, an inductive approach that considers various viewpoints and aspects is advantageous given the topic's complexity, which includes technological, organisational, and human issues.

Additionally, the systematic review's data-driven analysis allows the integration of results from several research, producing insightful conclusions and useful suggestions. Lastly, the inductive method makes it easier to generate theories by thoroughly studying the literature and spotting common themes or models. This helps researchers better comprehend the potential of threat intelligence and directs their future work in the area.

3.3. Research Philosophy

In the following study, interpretivism research philosophy was used. A study philosophy known as interpretivism aims to comprehend social processes through the viewpoints of people and their subjective experiences. It acknowledges that people's perceptions and meanings influence their behaviour and that reality is a social construction. Studying complicated social processes and subjects incorporating human values and cultural circumstances lends to interpretivism. It enables scientists to investigate the numerous nuances and subtleties of social interactions.

Furthermore, interpretivism strongly emphasises reflexivity, recognising the researcher's contribution to the research process and encouraging critical reflection. Due to its ability to explore new or understudied areas, it is highly suited for exploratory study and developing fresh theoretical ideas. In-depth investigation and comprehension of social phenomena are made possible by interpretivism, which advances knowledge in the social sciences.

3.4. Research Data Collection Method

The author collected secondary data to complete this study and acquire the research results. Organisational records, academic publications, government documents, published journals, and approved online content are some of the sources that may be used to gather secondary data. To collect the research data for this study, the author employed a variety of databases, including Google Scholar, Research Gate, Pro Quest, and Science Direct.

3.5. Research Design

In the following research, a qualitative research approach was selected. Qualitative research design aims to comprehend and interpret social phenomena by carefully examining people's subjective experiences, attitudes, and behaviours. It entails gathering and examining non-numerical data, including observations, interviews, and textual analysis, to understand the subtleties and complexity of human behaviour in particular circumstances. Utilising a qualitative research strategy is justified by its capacity to provide comprehensive and in-depth data regarding the social world. To fully understand the richness and variety of human experiences, researchers can dig deeply into peoples' viewpoints, beliefs, and motives. Researching subjects like cultural practices, social relationships, and personal experiences that call for a nuanced analysis, such as depth of knowledge, is very beneficial.

Additionally, qualitative research design is useful for analysing social phenomena in their original settings. Researchers can capture the complexity and subtleties of social interactions as they naturally develop by conducting observations and interviews in real-world contexts. This context-dependent approach promotes a more complete and accurate knowledge of the topic by avoiding simplifying or reducing social processes. The coding procedure was also used to assess the common categories in the following prospect to assess the study results.

3.6. Research Strategy (Article Search Strategy)

The major conclusion of the chosen subject has been found using the article search approach. Data was gathered from many sources to compile the results in the most effective, sound, and sustained manner possible, and sound attention was paid to the data's aerial perspective to choose the ideal article to address the research topic. In this phase, the researcher concentrated on the data patterns and developed a hypothesis to explain the patterns by using an inductive technique.

3.7. Inclusion and Exclusion Criteria

Our investigation only considered articles that satisfied the following criteria:

Inclusion Criteria

- Studies describe the potential of threat intelligence for anticipating and avoiding cyberattacks.
- Articles published in peer-reviewed journals between 2021 and 2023.
- Articles are written in their native language (English).

Exclusion Criteria

- The studies that did not describe the potential of cyber threat intelligence were disqualified.
- It was disregarded if no English translation of the research paper was available.

Figure 2: Shows the flow chart for Prisma methodology. Table 1 shows the process of search outcomes

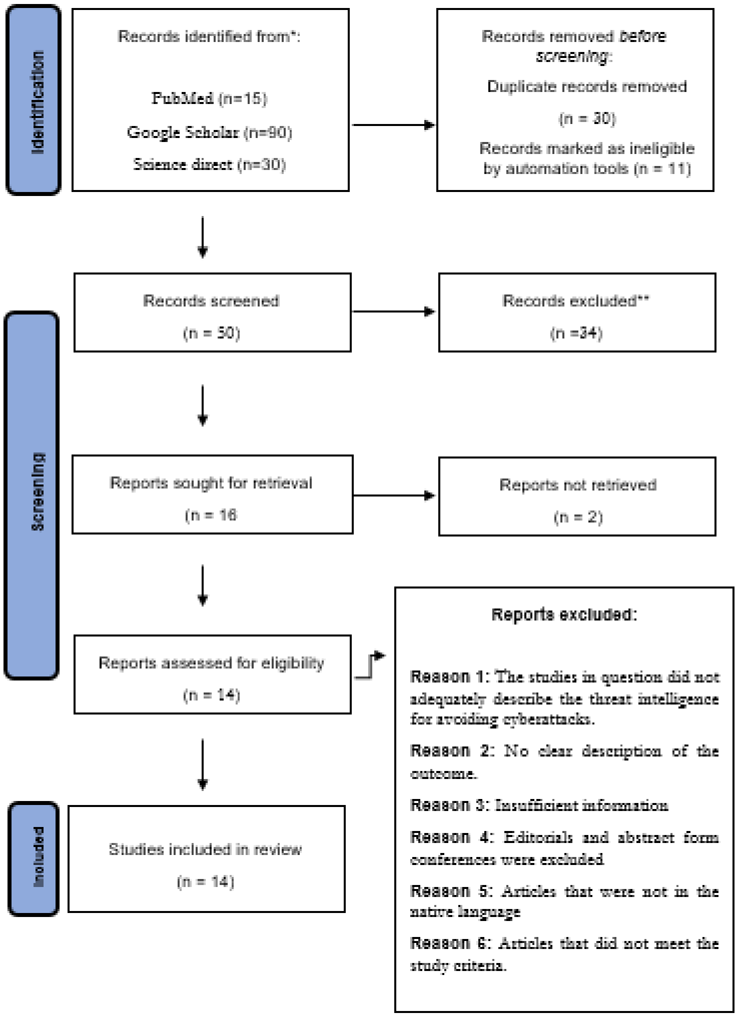
Identification
Records identified from*:
PubMed (n=15)
Google Scholar (n=90)
Science direct (n=30)
Records removed *before screening*:
Duplicate records removed
(n = 30)
Records marked as ineligible by automation tools (n = 11)
Screening
Records screened
(n = 50)
Records excluded**
(n =34)
Reports sought for retrieval
(n = 16
Reports not retrieved
(n = 2)
Reports assessed for eligibility
(n = 14)
Reports excluded:
Reason 1: The studies in question did not adequately describe the threat intelligence for avoiding cyberattacks.
Reason 2: No clear description of the outcome.
Reason 3: Insufficient information
Reason 4: Editorials and abstract form conferences were excluded
Reason 5: Articles that were not in the native language
Reason 6: Articles that did not meet the study criteria.
Included
Studies included in review
(n = 14)

Figure 1: The PRISMA flow diagram for the selected studies

Table 1: Process of search outcomes

The selected database	Selection of keywords	Limits hints	Number of articles included
Research Gate	Cyber Threat Intelligence *AND* mitigating cyber attacks *OR* emerging cyber threats, real-time visibility, security measures, approach to cyber defence	20	3
Google Scholar	Cyber Threat Intelligence *AND* mitigating cyber attacks *OR* emerging cyber threats, real-time visibility, security measures, approach to cyber defence	10	3
Pro quest	Cyber Threat Intelligence *AND* mitigating cyber attacks *OR* emerging cyber threats, real-time visibility, security measures, approach to cyber defence	5	2
NCBI	Cyber Threat Intelligence *AND* mitigating cyber attacks *OR* emerging cyber threats, real-time visibility, security measures, approach to cyber defence	8	3

Science Direct	Cyber Threat Intelligence *AND* mitigating cyber attacks *OR* emerging cyber threats, real-time visibility, security measures, approach to cyber defence	10	3

3.8. Evaluation of Selected Articles

Evaluation of some of the articles is as follows:

1. (Montasari et al., 2021): Title: "Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence." High validity, good quality. Aids businesses in understanding their CTI strategy.
2. (Kotsias et al., 2023): Title: "Adopting and integrating cyber-threat intelligence in a commercial organisation." High validity, best quality. Exemplifies action research in CTI for commercial organizations.
3. (Preuveneers & Joosen, 2021) Title: "Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence." High validity, precise quality. Demonstrates the viability of sharing ML-based threat intelligence.
4. (Kumar et al., 2021) Title: "DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems." Exclusive validity, good quality. Introduces CTIATI for IoT-enabled maritime transportation.
5. (Campos et al., 2022): Title: "Sensors for detection of cyber threats in the industrial environment using a high interaction ICS/SCADA Honeynet." Standard validity, authentic quality. Describes high-interaction ICS/SCADA Honeynets as sensors for threat detection.
6. (アリエル, 2021)Title: "A study on proactive data-driven cyber defence through threat intelligence." Best validity, good quality.
7. (Schlette et al., 2021): Title: "Measuring and visualising cyber threat intelligence quality." First-rate validity, accurate quality. Addresses CTI artifact quality evaluation.
8. (McCall Jr, 2022):s Title: "Exploring a Cyber Threat Intelligence (CTI) Approach in Thwarting Adversary Attacks: An Exploratory Case Study." High validity, precise quality. Focuses on CTI utilization gaps in businesses.
9. (Purohit et al., 2022)Title: "Cyber Threat Intelligence Sharing for Co-operative Defense in Multi-domain Entities." Reliable validity, useful quality. DefenseChain system outperforms in selecting peers.
10. (Zenebe, 2022)Title: "Cyber Threat Intelligence Discovery Using Machine Learning from the Dark Web." Best validity, accurate quality. Highlights ML accuracy in CTI discovery from the Dark Web.
11. (Hossen et al., 2021)Title: "Generating Cyber Threat Intelligence to Discover Potential Security Threats Using Classification and Topic Modeling." High validity, best quality. Utilizes ML to automate CTI discovery from hacker forums.
12. (Saraf & Malathi, 2023)Title: "Splunk-Based Threat Intelligence of Cyber-Physical System: A Case Study with Smart Healthcare." Good validity and accurate quality. Offers precise CPS security measures.
13. (Borges Amaro et al., 2022)Title: "Methodological Framework to Collect, Process, Analyse and Visualise Cyber Threat Intelligence Data." High validity, good quality. Presents a platform for CTI data analysis.
14. (Irshad & Siddiqui, 2023): Title: "Cyber threat attribution using unstructured reports in cyber threat intelligence." Good validity, high quality. Employs ML for accurate cyber threat attribution.

3.9. Comprehensive Analysis of Recent CTI Research Articles

1. **Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence** (Montasari et al., 2021): High validity. Research aim: To analyze the application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. Methodology: Primary qualitative. Conclusion: Meaningful conclusion. Strengths: Intensive investigation of complex phenomena. Limitations: Results may not apply to larger populations.
2. **Adopting and integrating cyber-threat intelligence in a commercial organisation** (Kotsias et al., 2023): High validity. Research aim: To evaluate how to focus on adopting and integrating cyber-threat intelligence in a commercial organization. Methodology: Primary qualitative. Conclusion: Good conclusion. Strengths: Rich data capture contextual nuances. Limitations: Time-consuming and resource-intensive data collection and analysis.
3. **Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence** (Preuveneers & Joosen, 2021): Exclusive validity. Research aim: To analyze the role of sharing Machine Learning Models as Indicators of Compromise for CTI. Methodology: Primary qualitative. Conclusion: Fair insight into the conclusion. Strengths: Adaptable and flexible in the face of evolving research concerns. Limitations: Subjectivity and prospective bias of the researcher can affect the findings.
4. **DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems** (Kumar et al., 2021): Standard validity. Research aim: To identify and evaluate DLTIF. Methodology: Primary qualitative. Conclusion: Fairly good. Strengths: Includes participant perspectives and subjective experiences. Limitations: Limited ability to quantify and measure variables.
5. **Sensors for detection of cyber threats in the industrial environment using a high interaction ICS/SCADA Honeynet** (Campos et al., 2022): High validity. Research aim: To determine sensors for the detection of cyber threats. Methodology: Primary qualitative. Conclusion: Adequate. Strengths: Provides a comprehensive comprehension of social phenomena. Limitations: Statistical capacity for evaluating hypotheses is insufficient.
6. **A study on proactive data-driven cyber defence through threat intelligence** (アリエル, 2021): High validity. Research aim: A study on proactive data-driven cyber defence through threat intelligence. Methodology: Primary qualitative. Conclusion: Slightly inappropriate. Strengths: Allows for the development and refinement of theories. Limitations: Possibility of researcher interference or deceptive queries.
7. **Measuring and visualising cyber threat intelligence quality** (Schlette et al., 2021): High validity. Research aim: Measuring and visualising cyber threat intelligence quality. Methodology: Primary qualitative. Conclusion: Not focused. Strengths: Facilitates the discovery of unanticipated insights. Limitations: Difficulty in guaranteeing the validity and reliability of data.
8. **Exploring a Cyber Threat Intelligence (CTI) Approach in the Thwarting of Adversary Attacks: An Exploratory Case Study** (McCall Jr, 2022):Exclusive validity. Research aim: Exploring a CTI approach. Methodology: Primary qualitative. Conclusion: Focused. Strengths: Draws attention to the significance of social and cultural context. Limitations: Susceptibility to interpretation and multiple points of view.
9. **Cyber Threat Intelligence Sharing for Co-operative Defense in Multi-domain Entities** (Purohit et al., 2022)**:** Standard validity. Research aim: CTI Sharing. Methodology: Primary qualitative. Conclusion: Sound. Strengths: Improves

comprehension of social interactions and meanings. Limitations: Potential for participant fatigue or social desirability bias.

10. **Cyber Threat Intelligence Discovery Using Machine Learning from the Dark Web** (Zenebe, 2022): High validity. Research aim: CTI Discovery. Methodology: Primary qualitative. Conclusion: Prospective. Strengths: Allows for the investigation of sensitive and personal topics. Limitations: Limited ability to establish cause-and-effect relationships.
11. **Generating Cyber Threat Intelligence To Discover Potential Security Threats Using Classification And Topic Modeling** (Hossen et al., 2021)**:** High validity. Research aim: Generating Cyber Threat Intelligence. Methodology: Primary qualitative. Conclusion: Good. Strengths: Promotes reflexivity and self-awareness of researchers. Limitations: Difficulties in replicating and confirming findings.
12. **Splunk-Based Threat Intelligence of Cyber-Physical System: A Case Study with Smart Healthcare** (Saraf & Malathi, 2023): High validity. Research aim: Splunk-Based Threat Intelligence. Methodology: Primary qualitative. Conclusion: Before findings. Strengths: Encourages participant collaboration and co-creation. Limitations: Considerations of ethics concerning confidentiality and informed consent.
13. **Methodological Framework to Collect, Process, Analyse and Visualise Cyber Threat Intelligence Data** (Borges Amaro et al., 2022)**:** High validity. Research aim: Methodological Framework. Methodology: Primary qualitative. Conclusion: Well defined. Strengths: Allows for the collection and analysis of data iteratively. Limitations: Possibility of excessive reliance on individual perspectives.
14. **Cyber threat attribution using unstructured reports in cyber threat intelligence** (Irshad & Siddiqui, 2023)**:** High validity. Research aim: Cyber threat attribution. Methodology: Primary qualitative. Conclusion: Adequate. Strengths: Provides a forum for underrepresented voices to be heard. Limitations: Difficulties in managing and analyzing massive quantities of qualitative data.

3.10. Measuring the Article's Quality Assessment

A quality assessment is a tool or procedure used to evaluate, evaluate, and document the potential risk of bias in research. It is determined by the categories of studies included in the systematic review. The evidence methodology was used to assess the content of the articles. The list is as follows: i.e. where was the article originally published?

- ➢ What is the research foundation?
- ➢ What is the author's name?
- ➢ Is the article commonly recommended?
- ➢ Are the research queries written?
- ➢ Are the limitations of the research mentioned?

3.11. Content Evaluation

The thematic analysis can be conducted immediately after the evaluation of each article. According to Gupta et al. (2019), the process of thematic analysis is described as qualitative data analysis that includes the assistance reading of transcript-based data, interview-based data, and theme pattern-based data exploration. According to Diabat, Kannan, and Mathiyazhagan's (2019) study, thematic analysis comprises six phases based on the data configuration, classification, and analysis objective. The six phases of thematic analysis were utilised in this study to achieve the research objective.

Stage 1: The author evaluated the data familiarisation procedure at this juncture. To achieve the research objective, 14 primary qualitative research articles have been selected to describe the key research findings and outcomes.

Stage 2: During this phase, coding practice was structured. Coding aims to describe the initial set of codes demonstrating visualised data's patterns and significance. The development of code includes the subsequent steps:

- Cyber Threat Intelligence
- Mitigating cyber attacks
- The emerging cyber threats
- The real-time visibility
- The security measures
- The approach to cyber defence

Stage 3: At this stage, themes are developed and stated as follows:

- Theme 1: Identifying and considering the key components of cyber threat intelligence that build up the CTI.
- Theme 2: The contribution of CTI in anticipating and avoiding cyber attacks.
- Theme 3: CTI effectiveness in the identification and responding of emerging threats in real-time
- Theme 4: Practices of implementing CTI programs for maximum effectiveness

Stage 4: At this stage, themes are finalised and presented to answer the main questions.

Stage 5: This stage has communicated the interest and relevance of the research

Stage 6: The final stage presents the main research findings

4. FINDINGS AND DISCUSSION

This is the crucial chapter of the research; it consists of the results and findings of the whole research. The thematic analysis has been used to represent the outcomes of the research. A type of critical analysis is used to demonstrate the research findings in a straighter manner. Based on the literature gathered information, thematic analysis is used to achieve the research objective, to investigate the potential of threat intelligence in anticipating and avoiding cyber attacks for the protection of the business entities and organisations presented in the following section.

1. Theme no.1: Identifying and considering the key components of CTI

Out of 100% identified literature, around 25% of the research articles indicated that the key components of CTI are data collection, analysis of techniques and methodologies for distributions, and activities based on intelligence insights. Daniel Schlette 2021 demonstrates a model of CTI with the help of phases or figures in the research; it explains the components with the help of the preparation phase, which means collecting data for the research work. The second phase is described in the research as the detection and analysis phase in which the techniques are implemented; the third phase is the recovery or eradication, in which the methodologies are evaluated; and the last phase is explained as the incident response, which is triggered and detection by an intrusion, the Intrusion Detection System (IDS) that needs incident response actions, additionally CTI feeds structured threats reports which are the possible exterior starting points of the phase. In the above literature, it is motioned that Using machine-understandable data, such as URLs, IP addresses, and hashes, actionable CTI also classifies the severity of threats and incident responses to prevent threats. The operational intelligence phase also focuses on the timing and type of cyber attacks, and it can use private or public resources like chat rooms and the dark web to learn more about how they communicate to mitigate and prevent future cyber attacks. (2022; Nimisha Goel, Mansi, Sethi). By using AI and ML, Abir Dutta, in 2020, made a CTI architectural model as mentioned above in the literature review, so there is plenty of research in which the researchers have implemented the CTI components in their creative way.

2. Theme no 2: CTI contribution to anticipating and avoiding cyber-attacks

Around 20% of research articles recognised that the contribution of CTI in anticipating and avoiding cyber attack are timeliness and connection with the organisations or business entities; most researchers found the research gap as they sought to establish methods of measurement and indicators, for example, it is stated by Ms Pragati in 2023, that the Internet of Things is less protected because of the broad consumptions and connectivity of the device, the private information and data from these devices is practised on helpless servers that can effortlessly be despoiled, whereas, the potential of CTI contribution to AI is also discussed by Sagar in 2022, that with the AI-enabled methods, it can extract meaningful models and patterns from a large amount of information and data from the cyber security which will be easier for the actionable CTI to detect the threats during cyber attacks. Cyber attacks may vary because the new technologies, methods, and techniques of threats evolve, so there are many recommendations from the researchers that need to be considered.

3. Theme no. 3 CTI effectiveness in the identification and responding to emerging threats in real-time

Around 25% of research articles pointed out that Cyber threat intelligence plays a crucial part in the identification and response to emerging threats in real-time; CTI also plays an important role in identifying the organisations to stay proactive by Cyber attacks and defend proactively against wicked acts by the threat performers, it responds the threats by threat detection, incident responses, analysis by threat intelligence and, other measures taken by CTI for proactive defence, researchers have recommended CTI and IOCs to send the word of warning before the threats when the computer system meets up with the unknown or suspicious threats. Essential information concerning a previous or ongoing cyber attack or security incident response is verified by security researchers as CTI; other than that, Although they are the most challenging, deep neural network (DNN) and ML models are better equipped to explain and describe what constitutes a cyber threat for example, the decision tree makes it easier to define a danger. It even shows that the criteria take preference over the threat's attributes. (Davy, 2021), Moreover, open-source CTI (OSCTI) to extract the indicators, the quality of OSCTI can be detected by the tactics, TTP and other formats that are used by them, focusing on producing CTI from network incidents for the enhancement of visualisation. Actionable CTI is the ability to respond to network incidents using the knowledge obtained by CTI, by which threat data can be detected. (Yi Tang, Ming Yi, 2022).

4. Theme no. 4 Premium practices of implementing CTI programs for maximum effectiveness

The best practices for creating a CTI plan for optimal effectiveness have been covered in about 15% of the literature. The procedure entails planning for integration by identifying the system applications that must be merged, followed by personnel training and execution. According to the literature, actionable threat intelligence may be employed as one of the best practices an organisation can use. In 2022, Nimisha Goel claimed that actionable CTI possesses various qualities, including prioritisation, accuracy, just-in-time, efficiency, and applicability. The strategic phase, the tactical intelligence phase, and the operational intelligence phase are the three strategic phases of the actionable CTI. Additionally, it is advised that CTI initiatives might benefit from ongoing improvement.

5. CONCLUSION

Following a thorough analysis of threat intelligence's potential for foreseeing and preventing cyber attacks, many important conclusions are drawn. The review's results highly support the effectiveness of threat intelligence, which shows that threat intelligence may significantly improve an organisation's capacity to foresee and thwart cyber attacks. The examined literature repeatedly emphasised threat intelligence's benefits in enhancing incident response, spotting new threats, and bolstering overall cyber security posture. The study emphasises the need for a thorough strategy while gathering threat information. Organisations should use various internal and external threat intelligence sources, including commercial products, open-source feeds, and data they have developed internally. Organisations may acquire a comprehensive view of the threat environment and effectively foresee and reduce possible cyber threats by combining these different sources. The review shows the need for teamwork and information sharing, which also highlights the importance of these factors in the field of threat intelligence. The ability of government agencies, business sectors, and organisations to share actionable information may improve collective security. The success of threat intelligence initiatives may be considerably increased by developing a culture of cooperation, engaging in information-sharing forums, and encouraging collaborations. The review emphasises the relevance of sophisticated detection and response systems, which also highlights the value of spending money on these systems. These systems make use of threat information. Technologies like SIEM solutions, intrusion detection systems, and analytics tools powered by artificial intelligence may improve an organisation's capacity to identify and react to complex cyber-attacks quickly. The evaluation emphasises how important it is for cybersecurity workers to have ongoing training and education. Organisations should provide regular training programs to improve the capabilities and expertise of their cyber security teams in exploiting threat information successfully. Analysts may make educated judgments and aggressive actions to foresee and prevent possible cyber attacks by keeping up to speed on the most recent threat patterns. This comprehensive assessment concludes by highlighting the enormous potential of threat intelligence for detecting and preventing cyber-attacks. Organisations may dramatically improve their cyber security posture and reduce the risks of emerging cyber threats by taking a holistic strategy, encouraging teamwork, investing in cutting-edge technology, and offering ongoing training. Businesses may achieve a proactive defence against prospective threats and the protection of vital assets by embracing these observations and suggestions.

6. Recommendations

The recommendations are initiated as follows:

Improve Information Sharing and Collaboration: Encourage cooperation between businesses, industries, and governmental bodies to enhance threat information exchange. To jointly improve cyber security defences, set up information-sharing platforms, join relevant groups, and encourage collaborations.

Spend money on sophisticated threat detection and response tools: Set aside funds to implement cutting-edge technology for threat detection and defence. Improve cyber threat mitigation capabilities using intrusion detection systems, SIEM solutions, and analytics tools powered by artificial intelligence.

Develop thorough threat intelligence strategies. Create and put into practice through threat intelligence strategies that combine external and internal information sources. Improve prediction and avoidance of cyber attacks by integrating open-source feeds, commercial products, and internally created data to view the threat environment comprehensively.

Provide Constant Training and Education. Invest in cyber security personnel's ongoing training and education programs to improve their abilities to use threat intelligence successfully. Provide specific instruction in incident response, threat intelligence analysis, and new threat patterns. Update cyber security personnel on the most recent innovations and best practices to ensure they are well-prepared to foresee and counter growing cyber threats.

These suggestions are intended to improve the efficiency and use of threat intelligence for foreseeing and preventing cyber attacks. Organisations may improve their cyber security posture and proactively counter possible attacks by employing collaborative methods, using cutting-edge technology, building comprehensive plans, and investing in the capabilities of cyber security specialists.

7. Research Limitations

The research limitations are initiated as follows:

- The availability and quality of literature sources are limited.
- The review's scope and concentration may restrict the breadth of research.
- Time constraints could limit the quantity and depth of studies reviewed.
- Possible fallacies in published studies, including publication bias and selective reporting.
- Inability to comprehend the most recent developments in the swiftly advancing field of threat intelligence.
- The findings have limited applicability across industries, organisational sizes, and geographies.

8. Research Future Directions

Concerning the capability of threat intelligence for expecting and staying away from interruptions, there are various roads to investigate regarding future research exploration. In the first place, extra exploration can foster further developed and refined models and calculations for threat intelligence that influence AI, artificial consciousness, and information examination procedures. This would permit associations to work on the precision and snappiness with which they recognise and answer threats. The future examination could likewise focus on advancing normalised structures and conventions for the powerful sharing and cooperation of threat intelligence across associations, industry areas, and government substances. This would work with consistent data trade, improving aggregate protection abilities.

What's more, there is a requirement for research that assesses the effect and viability of threat intelligence in unambiguous industry settings and areas, as various ventures might confront unmistakable threats and difficulties. Investigating the fuse of new advancements, for example, blockchain and the IoT, with threat intelligence could give new chances to develop network protection and proactive threat moderation further. By tending to these planned examination bearings, we can propel the field of threat intelligence and work on our capacity to expect and forestall cyber attacks.

Declaration and Statement

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.

REFERENCES

Borges Amaro, L. J., Percilio Azevedo, B. W., Lopes de Mendonca, F. L., Giozza, W. F., Albuquerque, R. d. O., & García Villalba, L. J. (2022). Methodological framework to collect, process, analyze and visualize cyber threat intelligence data. *Applied Sciences*, *12*(3), 1205.

Campos, M., Gomes, E., & Machado, R. (2022). Sensors for detection of cyber threats on industrial environment using a high interaction ICS/SCADA Honeynet. 2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0&IoT),

Dutta, A., & Kant, S. (2020). An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning. Information Systems Security: 16th International Conference, ICISS 2020, Jammu, India, December 16–20, 2020, Proceedings 16,

Goel, N. M., & Sethi, Nandini. . (2022). CYBER THREAT INTELLIGENCE: A SURVEY ON PROGRESSIVE TECHNIQUES AND CHALLENGES.

Hossen, M. I., Islam, A., Anowar, F., Ahmed, E., & Rahman, M. M. (2021). Generating cyber threat intelligence to discover potential security threats using classification and topic modeling. In *Cyber Security Using Modern Technologies* (pp. 141-153). CRC Press.

Irshad, E., & Siddiqui, A. B. (2023). Cyber threat attribution using unstructured reports in cyber threat intelligence. *Egyptian Informatics Journal*, *24*(1), 43-59.

Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, *32*(1), 35-51.

Kumar, P., Gupta, G. P., Tripathi, R., Garg, S., & Hassan, M. M. (2021). DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*.

McCall Jr, G. C. (2022). *Exploring a Cyber Threat Intelligence (CTI) Approach in the Thwarting of Adversary Attacks: An Exploratory Case Study* Northcentral University].

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.

Orbinato, V., Barbaraci, M., Natella, R., & Cotroneo, D. (2022). Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study:(Practical Experience Report). 2022 IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE),

Preuveneers, D., & Joosen, W. (2021). Sharing machine learning models as indicators of compromise for cyber threat intelligence. *Journal of Cybersecurity and Privacy*, *1*(1), 140-163.

Purohit, S., Neupane, R., Bhamidipati, N. R., Vakkavanthula, V., Wang, S., Rockey, M., & Calyam, P. (2022). Cyber threat intelligence sharing for co-operative defense in multi-domain entities. *IEEE Transactions on Dependable and Secure Computing*.

RANA, M. P., & PATIL, D. (2023). CYBER SECURITY THREATS DETECTION AND PROTECTION USING MACHINE LEARNING TECHNIQUES IN IOT. *Journal of Theoretical and Applied Information Technology*, *101*(7).

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

Samtani, S., Chen, H., Kantarcioglu, M., & Thuraisingham, B. (2022). Explainable artificial intelligence for cyber threat intelligence (XAI-CTI). *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2149-2150.

Saraf, K. R., & Malathi, P. (2023). Splunk-Based Threat Intelligence of Cyber-Physical System: A Case Study with Smart Healthcare. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(2), 537-549.

Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, *20*, 21-38.

Van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcătăian, A., Baumgartner, L., Fricker, S., & Ruiz, J. F. (2021). A shared cyber threat intelligence solution for smes. *Electronics*, *10*(23), 2913.

Zenebe, A. (2022). Cyber Threat Intelligence Discovery using Machine Learning from the Dark Web. *Communications of the IIMA*, *20*(2).

Zhiqun, W. D., Adeyemo & Akinrayo, Akinsoto. . (2023). Summary of Cyber Threat Intelligence.

アリエル, ロ. (2021). *A study on proactive data-driven cyber defense through threat intelligence* 九州大学].