EMPOWERING CYBER THREAT INTELLIGENCE WITH AI

Raghad Ghawa, Jawaher Alamri, and Rawan Eid Alanazi

College of Computer and Information Sciences - Cybersecurity Joint Masters Program

ABSTRACT

Cyber Threat Intelligence (CTI) is gaining importance due to the rise in cyber attacks and crimes. It aims to increase administrators understanding of events and threats by gathering intelligence about criminal operations. However, there is a lack of literature on how AI algorithms can improve CTI automation. This research aims to understand CTI's importance and automate the CTI process, prioritizing important threats and providing recommendations for mitigation. The study reviews literature on AI algorithms with CTI to identify the best models and algorithms for improving automation. It also helps organizations understand and analyze data to reveal trends and patterns, providing in-depth understanding of threats. This research is suitable for entities with large datasets of intelligent information and sensitive data types.

KEYWORDS

Artificial Intelligence Algorithms, Cyber-Threat Intelligence Machine Learning Model and Deep Learning Model.

1. INTRODUCTION

Nowadays, the concept of “Threat Intelligence” is used, which is also called “Cyber Threat Intelligence” (CTI) is data that contains detailed knowledge about cybersecurity threats targeting an organization. CTI helps security department be more proactive. Cyber-attacks continue at an increasing pace around the world, presenting significant challenges to organizations, the most important of which is how to collect and automate these threats.

As noted, (Scott, Dean, Sean Minarda, and Atif Ahmed -2023), there is little regulatory practice regarding CTI today. In addition, how technology has transformed the traditional human-centered practice of intelligence and how organizational decision-making impacts CTI engagement among stakeholders [1]. Cyber-attacks continue at an increasing pace around the world, presenting major challenges to organizations, the most important of which is how to collect and automate these threats. As stated, (author(s) - 2023) today there is a need for open-source tools and platforms to collect and manage these threats, which enables organizations to stay informed about the rapidly changing cyber threat landscape and identify cyber threats and mitigate them cost-effectively [2]. Security teams receive much CTI from open source and close source. Over the years, these threats to Intelligence have generated big-data. Cyber-threats have a variety and large data combined with a velocity that outstrips the ability of most organizations to defend and mitigate them in the event of an attempt.[3]

Due to the sheer volume of cyber threat data, threat intelligence analysts are frequently overwhelmed with information, making it difficult to separate true threats from false positives.

This is where artificial intelligence (AI) can play a very important role. AI can help automate and enhance various aspects of threat intelligence gathering and usage, such as data collection, in-depth analysis, smart sharing, and cutting-edge technology. The analysis of these cyber-threats using Artificial Intelligence (AI) algorithms such as Machine Learning (ML) and Deep Learning (DL) to learn from historical and current data and adapt to new and evolving threats It provides analyzed and organized information about the present, past and future potential attacks that may be a security threat to the enterprise and delivers the in-depth information such as files, IP addresses, domain names and URLs that are often used in executing attacks [4]. The role of AI in threat intelligence is to leverage artificial intelligence, particularly machine learning, to detect and respond to cyber threats more effectively and rapidly than human capabilities allow. AI-driven threat intelligence tools can boost the speed, accuracy, and efficiency of threat intelligence production and enhance its automatic effectiveness.

In this paper, we will prove our hypothesis by studying some literature research related to our project research on which Al algorithms can improve or help CTI automate processes.

2. THEORETICAL FOUNDATIONS

In this section, we will present Threat Intelligence in depth to establish the foundation for the concept. This chapter outlines threat intelligence, including its definition, lifecycle, intelligence types, limitations encountering threat intelligence systems, and AI algorithms that help organizations in performing automated operations.

2.1. Cyber-Treat Intelligence (CTI)

Cyberattack strategies and techniques have become more complex and sophisticated in recent years; it is challenging to prevent all cyberattacks. The employment of intelligence is crucial to enable the prediction of cyberattacks and the pre-emptive defense measures adopted accordingly. Cyber-threat intelligence is the process of collecting, analyzing, then classifying and sharing information about cyber threats with their actors. This information can help organizations anticipate and defend against cyberattacks, as well as improve their security posture and resilience. Indicators of Compromises (IoCs), such as hash, IP, domain name, network or host properties, tools used to attack, and tactics, techniques, and procedures (TTPs) data, are arranged and summarized by CTI which help in increasing the awareness of the trend threats, active attackers, and zero-day vulnerability.

CTI can be broken down into three classifications:

Tactical threat intelligence describes the tactics, techniques, and procedures (TTP) of threat actors, this cloud helps defenders know how their organization can be attacked and the best ways to defend and mitigate such attacks.

Operational intelligence is information about attacks, events, or organized crimes. It provides insights that help the IR team understand the nature, purpose, and time analysis of the attack.

Strategic intelligence provides an overview of the threat landscape, high-level decision-makers use it to make high-level decisions, the content is typically less technical and is delivered through reports or briefings.

Figure 1. CTI Levels [15]

Figure Label: As shown in the figure above, different levels of intelligence are grouped depending on their temporal term of use or by level of detail. Also, information that helps in making long-term decisions can be classified as strategic and tactical intelligence. On the other hand, practical information and technical focus will be used in the short term. Depending on the level of detail, tactical and technical provide low-level information. Which indicates that they focus on technical specifications. In contrast, strategy and operations make use of high-level information.

2.2. The CTI Life Cycle

The intelligence lifecycle is a process of transforming raw data into finished intelligence for decision-making and action [5]. According to [6] this cycle consists of 4 steps:

- **Plan and Guidance**

This phase involves communication between the consumer and the producer and is used to coordinate intelligence operations to best meet the needs of the consumer. Known as intelligence requirements (IRs) or priority intelligence requirements (PIRs).

- **Collection**

The second phase involves gathering large amounts of data from various resources that meet specified requirements.

- **Processing and analysis**

The third stage of the cycle involves gathering raw data and information, fusing it with information from other sources, and turning it into intelligence. During this phase, both human

and machine capabilities must be focused on meeting the requirements while upholding intelligence principles.

- **Dissemination**

The timely delivery of final intelligence products to the intended audience in a suitable format is known as dissemination. Through calls for feedback, the intelligence cycle may begin again, and the refining of existing Intelligence Requests, or by development of new ones.

- **Feedback**

The regular feedback needed to ensure that you fully understand the requirements of each group and that you adapt modifications as their priorities and requirements change.

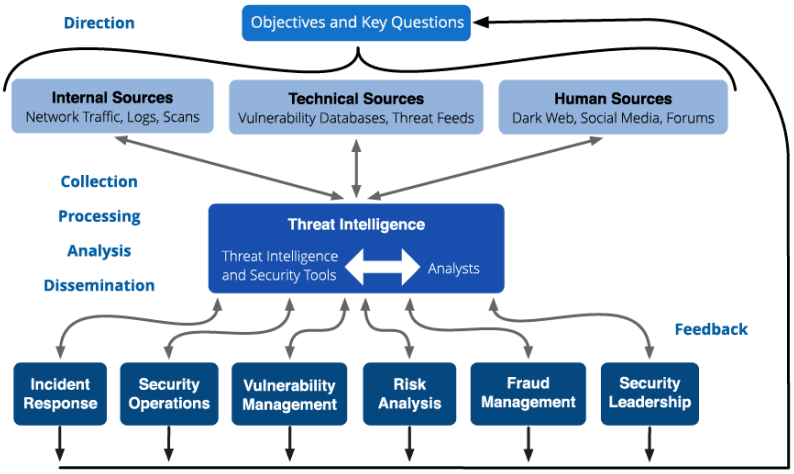

Figure 2. CTI Life Cycle [6]

.

Threat intelligence requires a lot of data, skills, and resources to perform effectively. This is where artificial intelligence (AI) can play a big role.

- **Automating data collection and analysis**

AI can help you gather and process large amounts of data from various sources, such as network logs, security alerts, open-source intelligence, social media, dark web, etc. AI can also filter out the noise and irrelevant information, and extract the relevant indicators of compromise (IOCs), such as IP addresses, domains, hashes, etc. AI can then analyze the data and identify patterns, trends, anomalies, and correlations that can reveal the nature, origin, and impact of the threats. This can save you time and resources and provide you with actionable insights.

- **Reinforcement CTI detection and response**

AI can help you detect and respond to threats faster and more accurately, by using machine learning and deep learning techniques to learn from historical and current data and to adapt to new and evolving threats. AI can also automate some of the response actions, such as blocking malicious traffic, isolating infected devices, notifying relevant stakeholders, etc. AI can also help

you prioritize the most critical and urgent threats and provide you with recommendations and guidance on how to mitigate them.

- **Improving threat intelligence sharing and collaboration**

AI can help you share and collaborate on threat intelligence with other organizations, such as industry peers, law enforcement, government agencies, etc. AI can help you standardize and format the threat intelligence data, and use common frameworks and protocols, such as STIX and TAXII, to exchange and communicate the data. AI can also help you enrich and validate the threat intelligence data, by cross-referencing and verifying it with multiple sources and databases. AI can also help you protect the confidentiality and integrity of the threat intelligence data, by using encryption and authentication methods.

- **Developing threat intelligence skills and knowledge**

AI can help you develop your threat intelligence skills and knowledge, by providing you with training and education resources, such as courses, tutorials, webinars, podcasts, etc. AI can also help you test and evaluate your threat intelligence capabilities, by using simulations, scenarios, quizzes, etc. AI can also help you learn from your own and other experiences, by providing you with feedback and suggestions on how to improve your threat intelligence processes and practices.

2.3. Automation CTI Programs and Applications

The volume and number of new cyberattacks have increased in recent years. Such attacks and events are characterized by a very complex process and involve different actors, organizations, and criminal patterns. However, current practices of threat analysis and intelligence discovery are still implemented in a fragmented, ad hoc manner that differs from one entity to another. For example, a modern malware analysis application can analyze a piece of malicious code itself. However, it cannot automatically identify the organizers who developed it or correlate other cyberattack patterns and events with it. Therefore, it is necessary to collect this detailed information about cybercrime events automatically by integrating threat information into data collected from different sources that may be open or closed sources. Many organizations today are moving to implement modern applications to automate the process, and the worth of these applications has proven to take all Types of threat sources into account new intelligence is discovered by linking these isolated patterns and cyber events, in addition to displaying alerts that can be classified into low, medium and high risk, which helps the organization to predict future cyber events and threats. [7]

2.4. Artificial Intelligence (AI) Models & CTI

- What is AI-based threat protection?

  In the area of threat intelligence, AI-powered threat protection entails utilizing machine learning algorithms and other forms of artificial intelligence to consistently search for and detect potential threats to a business. [8]

  AI can swiftly process and analyze extensive volumes of data in real-time, enabling it to adeptly identify issues and potential threats. By collecting valuable information regarding potential threats, AI provides businesses with the necessary insights to manage security risks proactively and effectively. [8]

- Automated decision making and response for CTI. AI can automate responses to threats and decision-making processes by isolating compromised systems, blocking malicious IP addresses, or applying patches. This technology assists organizations in staying current on emerging threats and attack techniques, consolidates data from various sources, and generates intelligence regarding the probability, severity, and potential impact of threats. These capabilities aid in prioritizing responses, reducing response times, and minimizing damage, ultimately enhancing overall security. [8]
- Cybersecurity Threat Detection using ML and DL Models:[5]

Table 1. Intrusion Classification Using ML.

Intrusion classification using machine learning	**Fileless malware detection**
Utilizing a filter-based univariate feature selection method to identify the most pertinent features.	Detecting malware through the analysis of malicious patterns in processes, registry, file system changes, and event logs.
Applying an oversampling technique, specifically SMOTE, to address the imbalance in the dataset.	A systematic approach for managing and examining file-less malware attacks across various stages, including memory analysis, incident analysis, and investigation

Table 2. Malware And Botnet Using ML & DL

Malware classification using DL	**Botnet classification using ML**
Classifying malware through the application of transfer learning	Applying a chi-square scoring method for filter-based feature selection to identify the most pertinent features.
Classifiers operate based on visual features without the need for prior knowledge of binary code analysis	Applying a lightweight gradient boosting model for the classification of botnet attacks.

- How can AI improve your CTI?

  Optimizing data collection and analysis through automation AI adeptly manages extensive data from diverse sources, filtering out irrelevant details and extracting meaningful indicators of compromise. The system analyzes this refined data to uncover patterns, trends, anomalies, and correlations, delivering actionable insights while conserving valuable time and resources. [9]

  - **Improving the detection and response to threats**

    AI boosts the identification and handling of threats through the application of machine learning and deep learning methods. It automates responsive measures prioritizes crucial threats, and offers suggestions for mitigation, thereby elevating both efficiency and accuracy. [9]

  - **Enhancing the sharing and collaboration of threat intelligence**

    AI facilitates the sharing and collaborative efforts related to threat intelligence among diverse organizations. It standardizes the data format, enriches, and validates it through cross-referencing, and ensures its confidentiality and integrity using encryption and authentication methods. [9]

- **Building Proficiency in Threat Intelligence**

  AI enriches proficiency in threat intelligence through the utilization of training resources, simulations, scenarios, and quizzes. Additionally, it provides valuable feedback and suggestions for improvement, empowering users to evaluate and refine their capabilities effectively. [9]

- **Advanced Machine learning algorithms:**

  Sophisticated algorithms, integral to the field of artificial intelligence (AI), enable computers to learn from data, streamlining the process of making predictions and informed decisions. The following provides an overview of some advanced learning algorithms commonly utilized in cybersecurity.

  - **Supervised learning:**

    - Support Vector Machines (SVM): Specifically employed for binary classification, SVMs excel in distinguishing between legitimate network traffic and malicious activities. Their high capability lies in effectively identifying patterns within data. [10]

    - Random Forest: Essentially, it is an ensemble learning technique that combines multiple decision trees to enhance classification accuracy. Its primary application lies in detecting various types of malware and intrusion attempts. [10].

  - **Unsupervised learning:**

    - K-means Clustering: Its primary application involves grouping data points into clusters based on their similarity levels. In the context of cybersecurity, it proves beneficial for detecting anomalies. [10]
    - Auto-encoders: Neural networks designed for feature learning, prove invaluable in identifying unusual patterns in both network traffic and system behaviour. [10]

  - **Deep learning**

    - Neural Networks (CNNs): Widely utilized in threat detection scenarios involving images, such as the identification of malware within files or the recognition of malicious content in images. [10]
    - Long Short-Term Memory (LSTM) Networks: Like RNNs but designed specifically for sequential data, these networks excel at detecting subtle patterns in time-series data. This makesthem particularly well-suited for the task of intrusion detection. [10]

  - **Ensemble learning:**

    - AdaBoost: This method specifically targets the shortcomings of individual models and is frequently employed for the detection of malware.[10]
    - Gradient Boosting Machines (GBM): Employing this ensemble technique involves combining predictions from multiple models to enhance accuracy in various cybersecurity tasks, like the detection of phishing emails. [10]

- **Semi-Supervised learning:**

  - Label Propagation: These methods can be utilized to extend labels from a smaller, labeled dataset to a larger, unlabelled dataset, often applied in the realm of threat detection. [10]

3. METHODOLOGY

In this section, we will explain comparative analysis and systematic review methods. The section goes further to look at related studies on the concern that this thesis aims to address.

3.1. Systematic Review

This paper utilizes a literature review to gather information about the current state of CTI and its importance and points out the automation of CTI using AI & ML algorithms; advantages, challenges, and potential research gaps have been discussed. It draws from both academic and gray literature sources.

CTI is essential for predicting and preventing cyberattacks before they occur. Numerous organisations became interested in working more proactively rather than just reactively as a result of this information. Sharing information about the recent threats and vulnerabilities with stakeholders helps them to become aware of the situation. This is the fundamental premise underlying threat intelligence sharing. Moreover, CTI can support stakeholders in deciding tactical decision. Thomas, Khaled Mahbuba, Esther Palomara , and Ali E. Abdallaha [1] and to establish future directions for study on CTI sharing and its characteristics. Scholarly search engines, university catalogues, and journal databases were used to find relevant material. With a focus on CTI sharing or similar subjects, they examined 102 publications, papers, and government bills. They then classified the articles into several groups according on how much a focus was placed on the following aspects: data interoperability, trust, reputation, relevance, anonymity, and timeliness. The focus was on what information can be shared, with whom, and how to automate some of the collaboration processes. Scott, Dean, Sean Maynarda, and Atif Ahmad [2] furthermore discovered that there is an absence of the organisational practise perspective on CTI. They investigated and examined 206 articles.They discussed the need for research on how technology has changed the traditional human-cantered intelligence practise and how organisational decision-making impacts stakeholders' sharing of CTI.[1]

Joe Barr's cyber threat intelligence [1]-[4] and ML for cyber threats have been emphasized as an important component of defensive security and cyber-Protection with illustrative examples dating back to its created Financial Sector Data Sharing and Analysis (FS) (ISAC) in 1998. Automated process are needed today to keep up with the huge volume of attacks around the world. Cyber threat information must be actionable, up-to-date and reliably validated if it is to be absorb it into computer-operated defense systems. This paper illustrative some of the progress made in applying AI software as well as the challenges associated with using machine learning to improve the threat intelligence process. In addition, Joe Barr discussed some ideas to help the variety of methods that have been developed to create ML and DL algorithms that can be combined with firewalls, networks, rules, and heuristics. Also, significant work is needed to effectively support the limited number of dedicated human man-hours to assess the landscape of high-priority cyber threats flagged as attack in a Security Operations Center (SOC) environment. This big data aspect of threat intelligence has been realizationed by academic, commercial, and government and minsitry researchers. Finally, Joe Barr's research is leading to the development of systems that comply and help protect the integrity, confidentiality, and availability of large, distributed

organizations at low cost and effort, while also enhancing the time between fast detection and incident . Identification is even possible, if the user can publish processing and recovery steps.[2] Al-Dmour and colleagues [1]-[7] developed SecurityKG, an AI-driven system utilizing NLP technologies to collect and oversee Open-Source Cyber Threat Intelligence (OSCTI). The system builds a security knowledge graph by extracting elevated threat behavior details from various sources. The system offers a user-friendly interface for exploring this knowledge graph, facilitating organizations in staying abreast of dynamic cyber threats and cost-effectively identifying and mitigating them. Utilizing a unified ontology, SecurityKG describes OSCTI reports and information, ensuring flexibility for application-specific details. The system adeptly tackles the challenge of extracting threat information from unstructured OSCTI documents, encompassing entities and connections to monitor threat behaviors. Employing a Data-Programming Approach for building extensive training corpora, SecurityKG features a UI for knowledge graph exploration, SecurityKG incorporates an internal system for collecting Open-Source Cyber Threat Intelligence (OSCTI) components and employs a scalable critical escrow model to guarantee security, handling over 350 reports per minute. Essentially, it utilizes OSCTI, a security knowledge ontology, and diverse tools to collect and process security reports, thereby enhancing the security of digital assets within an organization.[3]

Goel et al. [1]-[6] Cyber Threat Intelligence (CTI) involves using information-driven strategies to counter cyber threats. It helps organizations identify and prioritize threats, assess potential impacts, and formulate effective responses. CTI offers insights into the Tactics, Techniques, and Procedures (TTPs) employed by threat actors, along with Indicators of Compromise (IOCs) for detecting and mitigating cyber threats. Platforms like Cisco Umbrella, DeCYFIR, Echosec, and Grey Noise play a crucial role in safeguarding sensitive information. This discussion covers diverse CTI tools such as ElasticSearch, FeedRank, and Forensic Readiness Model, emphasizing their role in threat detection and information sharing. Researchers contribute by exploring methods like Attribute-Based Encryption and a Policy-Sharing Platform to enhance threat annotation accuracy. The integration of infrastructure nodes through a graph convolutional network-based approach and the implementation of an AI-based honey spy system highlights the innovative techniques employed in CTI. Overcoming challenges such as threat prioritization, response time, alerting, data standards, and privacy concerns is essential for organizations to effectively combat cyber threats. [4]

3.2. Comparative Analysis

To defend against different cyber-attacks, several CTI technologies and platforms are available today. We have collected the main contributions from various relevant studies. The primary information from each study is presented in Table.

Table 3. Comparative Analysis.

Authors	**Proposed Model**	**Explanation**	**Future Work**	**Results**
J. Cha, S. K. Singh, Y. Pan, and J. H. Park [11]	Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing	The model proposed in this paper is a collaborative architecture that mitigates problems such as data collection issues and requirements that may arise during the data collection process for sharing threat information, reliability, privacy, efficiency, and scalability [7]	Authers will study an extensible framework that can efficiently and automatically apply security policies of information consumer organizations through data analysis as well as data collection.	Experimental results show that the proposed model saves about 15% of storage space compared to total network resources in a limited test environment.
J. Zhao, Q. Yan, J. Li, M.Shao, Z. He, and B. Li [12]	TIMine Framework	This paper proposes TIMiner, a novel CTI extraction framework, is proposed to automatically extract IOCs and generate categorized CTIs with domain tags from social media.. This framework is based on neural network (CNN) based to identify which domain a cyber threat intelligence belongs to [8].	N/A	Experimental results confirm that the proposed CTI domain recognizer and IOC extraction achieve superior performance with the accuracy exceeding 84% and 94%, respectively.
J. Liu et al. [13]	Trigger enhanced discovery system for actionable CTI	The authors presented a technique to determine the correlation between IOCs and campaign stages, or the terms that activate actionable CTI. The authors trained a classification model using Natural Language Processing (NLP) techniques [9]	The introduction of dependency parse trees is a helpful. We may create a dependency parse tree by linking potential IOCs to the contexts they rely on,	Experimental results shows an accuracy of over 86.99%, Tri CTI was applied to 29,000 cyber security-related reports.
M. Odemis, C. Yucel, and A. Koltuksuz [14]	A Honey spy system	The proposed model aims to find a correlation between a hacker's behavior/logs on the server and the personality, expertise, and psychology of the hacker. The predictions were made using various ML algorithms [10]	The study will be implementing real time log analysis in the future, and Honey spy system will be integrated into SIEM tool, and thus will be monitored online.	By using Ensemble (Bagged Tree), Support Vector Machine (SVM), and Naive Bayes, the accuracy achieved an 11% increasing

4. CHALLENGES & DISCUSSION

This section presents some challenges of this research.

1. Achieving a harmonious collaboration between humans and AI – Finding the optimal equilibrium between human analysts and AI
2. Meeting Regulatory Standards – The use of AI in threat intelligence may demand organizations to navigate through intricate and dynamic regulatory frameworks, posing potential challenges in terms of time and cost. [1]
3. Adversarial attacks – Advanced threat actors may try to outsmart AI systems by creating attacks tailored to bypass detection, thus compromising the efficacy of AI-driven threat intelligence. [1]
4. Concerns about bias – AI models have the potential to internalize and propagate biases present in their training data or algorithms, leading to skewed or misleading evaluations. [1]

5. RESULTS

In this section, focuses on assessing the research and affirms that a systematic and disciplined approach was adhered to throughout the study.

Table 4. Adv. of AI in CTI

Advantages of AI Algorithms in CTI	
Improved performance	Ongoing observation
Enhanced accuracy	Improved security
Capabilities for prediction	Improved speed and efficiency
Scalability	

6. CONCLUSIONS

Cyber threat intelligence equips organizations with vital information to swiftly and efficiently implement preventive and defensive measures. It plays a crucial role in ongoing security monitoring and serves as a valuable resource in responding to security incidents. This paper briefly explains what CTI is, its importance, and outlines the application of AI algorithms for its automation. Additionally, it highlights several widely used algorithms that contribute to the automation of CTI processes.

REFERENCES

[1] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, “Cyber threat intelligence sharing: Survey and research directions,” Computers & Security, vol. 87, p. 101589, Nov. 2019. doi:10.1016/j.cose.2019.101589

[2] S. Ainslie, D. Thompson, S. Maynard, and A. Ahmad, “Cyber-threat Intelligence for Security Decision-making: A review and research agenda for practice,” Computers & Security, vol. 132, p. 103352, 2023. doi:10.1016/j.cose.2023.103352

[3] Al-Dmour, N.A., Hasan, M.K., Ajmal, M., Ali, M., Naseer, I., Ali, A., Al Hamadi, H. and Ali, N., 2023, March. An Automated Platform for Gathering and Managing Open-Source Cyber Threat

Intelligence. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-7). IEEE.

[4] Goel, Nimisha & Mansi, & Sethi, Nandini. (2022). Cyber threat intelligence: a survey on progressive techniques and challenges.

[5] Sudhakar. 2021. Cybersecurity Threat Detection using Machine Learning and Deep Learning Techniques. In Proceedings of First International Conference on AI-ML Systems, Banglore, India.

[6] What is threat intelligence?, https://www.recordedfuture.com/threat-intelligence

[7] K. Baker, "What is Cyber Threat Intelligence? [beginner's guide]," WHAT IS CYBER THREAT INTELLIGENCE?, https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

[8] Fonseca, M. (2023a) Ai in threat intelligence, Silobreaker. Available at: https://www.silobreaker.com/glossary/ai-in-threat-intelligence / (Accessed: 26 November 2023).

[9] Mimecast (2023) Ushering in AI to automate Cyberthreat Intelligence, Mimecast. Available at: https://www.mimecast.com/blog/ushering-in-ai-to-automate-cyberthreat-intelligence / (Accessed: 26 November 2023).

[10] Hasan, A. (2023) The Future of Cyber Threat Intelligence: Ai-driven .. - researchgate. Available at: https://www.researchgate.net/publication/375005172_The_Future_of_Cyber_Threat_Intelligence_AI-Driven_Predictive_Analysis (Accessed: 25 November 2023).

[11] J. Cha, S. K. Singh, Y. Pan, and J. H. Park, "Blockchain-based Cyber Threat Intelligence System Architecture for Sustainable Computing," Sustainability, vol. 12, no. 16, p. 6401, 2020.

[12] J. Zhao, Q. Yan, J. Li, M. Shao, Z. He, and B. Li, "TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from Social Data," Computers & Security, vol. 95, p. 101867, 2020.

[13] J. Liu, J. Yan, J. Jiang, Y. He, X. Wang, Z. Jiang, P. Yang, and N. Li, "TRICTI: An actionable cyber threat intelligence discovery system via trigger-enhanced neural network," Cybersecurity, vol. 5, no. 1, 2022

[14] M. Odemis, C. Yucel, and A. Koltuksuz, "Detecting user behavior in cyber threat intelligence: Development of honeypsy system," Security and Communication Networks, vol. 2022, pp. 1–28, 2022.

[15] FBI IC3, "FBI: Internet Crime Report 2020," Computer Fraud & Security, vol. 2021, (4), pp. 4, 2021. Available: https://dx.doi.org/10.1016/S1361-3723(21)00038-5. DOI: 10.1016/S1361-3723(21)00038-5.