World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

SYSTEMATIC REVIEW OF THE PROBLEMS AND OPPORTUNITIES OF ARTIFICIAL INTELLIGENCE INCORPORATION WITH CYBER THREAT INTELLIGENCE SHARING, THREAT HUNTING, AND THREAT MODELING

Ifeyinwa Nkemdilim Obiokafor [1, *], Moses Okechukwu Onyesolu [2] and Felix Chukwuma Aguboshim [3]

[1] Department of Computing Sciences, Cybersecurity Programme, Admiralty University of Nigeria.
[2] Department of Computer Science, Nnamdi Azikiwe University, Awka. Nigeria.
[3] School of Information Systems and Technology, Walden University, USA.
* Corresponding Author

ORCID Details
Ifeyinwa Nkemdilim Obiokafor: https://orcid.org/0000-0002-8013-461X
Moses Okechukwu Onyesolu: https://orcid.org/0000-0003-3357-4847
Felix Chukwuma Aguboshim: https://orcid.org/0000-0002-0755-0561

World Journal of Advanced Research and Reviews, 2026, 31(03), 806–819

Publication history: Received on 24 July 2026; revised on 07 September 2026; accepted on 09 September 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.31.3.2262

ABSTRACT

The rapid evolution of AI-powered cyberattacks has revolutionized the environment of cybersecurity, with adversaries using the means of automation of sophisticated attacks, which are beyond the capabilities of the existing cybersecurity environment. The estimated amount of cybercrimes in the world is $10.5 trillion annually, with an average cost of a data breach to an organization being $4.45 million. The existing cybersecurity environment is not sufficient, as it is not scalable, quick, and intelligent enough to combat the increasing number of cyberattacks. The biggest challenge in the context of the use of AI in the CTI environment is the lack of awareness and understanding of cybersecurity professionals/organizations about the use of artificial intelligence in CTI sharing, threat hunting, and threat modeling. The paper applied a systematic review of the literature available in the context of the last five years (2020-2026) from IEEE Xplore, ScienceDirect, ACM Digital Library, and Google Scholar. The results of the study have shown that AI can play an important role in enhancing the level of automation, which can reduce the time of detecting cyber threats up to 60 times. Despite the importance of AI in the CTI environment, there are some limitations to the adoption of AI in the CTI environment. The findings of this review have shown that there are four major themes, which include the role of AI in enhancing the level of automation, explainability, ethics, privacy, integration, and complexity.

Keywords: Artificial Intelligence (AI), Cyber Threat Intelligence (CTI) Sharing, Threat Hunting, Threat Modeling, Cybersecurity Integration.

1 INTRODUCTION

The fast development of cyber dangers has reached a new stage, in which opponents now utilize AI to automate, enhance, and execute advanced attacks in real-time in a approach that is more than a traditional air defense systems can handle, thus drastically changing the cybersecurity environment (Buczak & Guven, 2016). This paradigm has escalated the need to incorporate AI into the cyber defense strategies, especially in cyber threat intelligence (CTI) sharing, threat hunting, and threat modeling because traditional tools and measures are seemly increasingly ineffective against neoteric AI-based adversarial techniques (Sommer & Paxson, 2010). Cyber Threat Intelligence (CTI) refers to gathering, examining, and sharing information regarding the possible or actual cyber threats in order to support defensive measures (Hutchins et al., 2011; Obiokafor et al., 2025b;). It was found that CTI sharing can greatly improve situational awareness and minimize the response time to cyber incidents (Jesus et al., 2024). Nonetheless, the classical CTI systems are associated with data overload, the dearth of standardization, and the absence of trust amid the organizations (Obiokafor et al., 2025a; Tounsi & Rais, 2018).

The recent empirical evidence shows how critical this problem is. For example, a report prepared by IBM Security shows that on average, in the world, the cost of a data breach is 4.45 million dollars, which is an increase of 15 percent over the cost of a data breach in the last 3 years (IBMSecurity, 2023). Cybersecurity Ventures shows that by 2025, a record of 10.5 trillion is expected to be reached globally in terms of cost in relation to cybercrime (Morgan, 2022). This shows how critical this problem is. In addition, it is also evident from this research that more than 80 percent of organizations do not possess a proper system of sharing information in real-time, which is affecting their response to this new threat. This shows that despite investing so heavily in this sector, people have not yet acquired a proper system that could support them in this problem. Therefore, a new AI solution is needed.

1.1 Challenges and Opportunities in Integrating AI with CTI Sharing

Integrating AI systems with cyber threat intelligence sharing has various challenges, including data heterogeneity and unstructured data, as well as low interoperability, which can limit machine learning effectiveness (Bridges et al., 2014; Husak et al., 2021). Trust and privacy are another challenge in sharing threat intelligence due to data breach concerns and reputational damage (Gal-Or & Ghose, 2005; Kshetri, 2021). Finally, there is a threat of adversarial attacks against AI systems attributable to data poisoning (Biggio & Roli, 2018). However, AI has various opportunities in integrating and improving cyber threat intelligence sharing by using machine learning techniques in automated analysis, anomaly detection, and prediction-based intelligence sharing (Buczak & Guven, 2016; Sarker et al., 2020). Federated learning and privacy-preserving AI can facilitate secure sharing, while natural language processing can be used in data analysis (IBM Security, 2023; Mutemwa et al., 2025; Nguyen et al., 2025; Nolte et al., 2025).

1.2 Challenges and Opportunities in AI-Driven Threat Hunting

AI-driven threat hunting has several challenges. First, there is inadequate data for supervised learning (Sommer & Paxson, 2010). Secondly, there is a high false positive rate, which causes analyst fatigue (Ullman et al., 2024). Finally, there is limited explainability of the AI model (Torres et al., 2023). However, there are several benefits of AI-driven threat hunting. First, there is real-time anomaly detection (Song, 2025). Secondly, there is constant monitoring. Finally, there is automation of repetitive tasks (Sarker et al., 2020). Moreover, there is enhanced behavioral analytics, which can detect zero-day attacks (Ullman et al., 2024). Studies have shown that AI can reduce detection time by a significant factor (Rabaan et al., 2022; Tsui et al., 2023). Nevertheless, there is a need for constant update of the model (Sommer & Paxson, 2010).

1.3 Challenges and Opportunities in AI-Driven Threat Modeling

The application of AI in threat modeling helps to improve the detection and mitigation of weaknesses in a system. Though, some of the challenges associated with AI-driven threat modeling include data availability, data quality, and the need for continuous retraining of the data (Sarker et al., 2020). The traditional approach to threat modeling is not responsive to a changing environment and is not easily integrated into a legacy environment. The use of a hybrid approach is a practical solution to the problem. The application of AI in threat modeling helps to improve risk assessment and modeling of cloud and IoT systems. However, the deployment of AI models may expose a system to new risks if an attacker exploits a weakness for nefarious intentions (Biggio & Roli 2018).

1.4 Synthesis of Literature Gaps and Contribution to Knowledge

From the literature review, some gaps that exist in the application of AI in cybersecurity have been identified. Firstly, the lack of an integrated framework is noted, where studies on CTI sharing, threat hunting, and threat modeling have been carried out individually (Sarker et al., 2020; Tounsi & Rais, 2018). Secondly, the absence of empirical validation is mentioned, as studies on AI models have not been evaluated in real-world scenarios (Sommer & Paxson, 2010). Third, there is a shortage of research on trust, privacy, and collaboration, all of which are vital (Gal-Or & Ghose, 2005; Kshetri,

2021). The lack of explainability in AI models is noted, where there is a lack of transparency. Lastly, the lack of studies on collaboration between humans and AI is noted (Nolte et al., 2025).

1.5 Problem Definition

The primary issue is that the existing cybersecurity systems are not effective in dealing with the sophisticated and constantly changing nature of cyber threats due to the inability to scale, speed, and intelligence processing. There is also a lack of understanding regarding the incorporation of AI in CTI sharing, threat hunting, and modeling. Challenges include data heterogeneity, a lack of standardization, interoperability limitations, and privacy concerns (Gal-Or & Ghose, 2005; Kshetri, 2021). There is also the issue of lack of transparency in AI systems, lack of effective collaboration between humans and AI, resulting in automation bias. There is also the issue of a large false positive rate, which affects system efficiency (Husák et al., 2021; Sommer & Paxson, 2010).

1.6 Aim of the Study

This research paper is an attempt to systematically analyze the opportunities and challenges that are related to the implementation of artificial intelligence (AI) in cyber threat intelligence sharing, threat hunting, and threat modeling with the perspective of generating insights that can improve proactive, adaptive, and collaborative cybersecurity operations.

1.6.1 Objectives of the Study

- To identified and critically evaluated and examine the quantity of the AI-based cyber threat intelligence sharing, threat hunting, and threat modeling
- To discuss the opportunities and possible benefits of AI integration into the effectiveness, efficiency, and predictable capabilities of the cybersecurity operations.

1.6.2 Research Questions

- What are the major issues that influence the implementation of artificial intelligence in cyber threat intelligence sharing, threat hunting, and threat modeling?
- What are the opportunities and strategic advantages of incorporating artificial intelligence in the process of sharing cyber threat intelligence, threat hunting, and threat modeling?

1.7 Scope of the Study

The scope of the paper is global because the study is based on the analysis and application of cybersecurity strategies all over the world, in developed and developing regions. The analysis is based on the developments and advancements in the field of cybersecurity, especially over the last two years, from 2020 to 2026, characterized by the growth and development of AI-based cybersecurity solutions. The analysis is based on the challenges, opportunities, and gaps in the following areas: CTI sharing, threat hunting, and threat modeling. The analysis is comprehensive and focused, considering the application and adoption of AI in modern cybersecurity strategies.

1.8 Significance of the Study

The work is crucial for developing theoretical and practical understanding on AI-based cybersecurity integration. This study also addresses some of the knowledge gaps in the literature, especially on the lack of an integrated framework on CTI sharing, threat hunting, and threat modeling. This study also enables practitioners to understand the realities and opportunities, thus promoting better threat detection, response, and prediction. This study also enables policymakers to understand the concept of trust, privacy, and collaboration, thus promoting better regulatory policies. This study also promotes innovation in technology, especially on areas such as explainability and data quality, and also on the need to balance human-AI collaboration.

2 METHODOLOGY

In the present study, systematic review methodology was used to identify, analyze, and synthesize the existing empirical and theoretical studies that focus on artificial intelligence (AI) and cyber threat intelligence (CTI) sharing and threat hunting and threat modeling. A systematic review provides a systematic, transparent, and reproducible method of converting the results of various sources to respond to research questions and determine trends, gaps, and opportunities (Rogge et al., 2024). The approach is especially appropriate to conduct cybersecurity research because there is an extensive body of qualitative and quantitative research on AI-based applications, issues, and opportunities in various technological and organizational settings.

2.1 Search Parameters, Inclusion and Exclusion Criteria and Rationale

The literature search was selected based on the studies within the 2010-2025 timeline due to the need to designate the latest advancements in the use of AI in cybersecurity. The databases and search engines utilized were IEEE Xplore, ScienceDirect, and ACM Digital Library, and Google Scholar. Search keywords had been organized with the help of Boolean operators (AND, OR) in order to be specific in retrieval. Two major keywords were applied:

- **The keywords** to be used are as follows: first keyword: Artificial Intelligence AND Cyber Threat Intelligence Sharing AND Threat Hunting AND Threat Modeling.
- **Second keyword,** Ai Or Artificial Intelligence And Cybersecurity And Threat Intelligence Or Threat Hunting Or Threat Modeling. This systematic review covered publications that focus on the concept of artificial intelligence (AI) integration into cyber threat intelligence (CTI) sharing, threat hunting, or threat modeling, and challenges, opportunities, and empirical assessments in the field of cybersecurity. The sources that were eligible included peer-reviewed journal articles, systematic reviews, conference papers, and reports in full text, published in English not older than 2026 and not earlier than 2020. Qualitative and quantitative studies as well as mixed-method studies were not ruled out, as long as they provided information on the research goals. The exclusion criteria were that the study should not be on cybersecurity and should not have lacked a definite relation to AI integration in the CTI sharing, threat hunting, or threat modeling. Articles that do not refer to these central areas concerning cybersecurity were also excluded. Also, additional exclusion criteria were publications before 2014, unless they had necessary theoretical underpinnings, unpublished theses, inaccessible full texts, and non-English articles. The reason behind these requirements was to make sure that the review was focused, timely, methodologically appropriate and covers high-quality evidence that directly relates to AI-driven cybersecurity functions and avoids the studies that do not meaningfully influence the research scope.

2.2 Review Process

The review process was an important factor that entails an extensive and multiple-step process. First, the articles were reviewed based on the relevance of the studies using the set criteria. Then, the articles are filtered based on their relevance to the use of AI in the sharing of CTI, threat hunting, and threat modeling. After that, the articles were reviewed to ensure the quality and relevance of the studies. Then, the data extraction process was undertaken to ensure the relevance and quality of the data collected on the use of AI methods, cybersecurity, challenges, and results. At this stage, only 15 high-quality articles were selected, with 3 being qualitative and 12 being quantitative, after filtering 27,701 articles to ensure the quality and credibility of the studies. The screening and selection process is depicted in Table 1 and Figure 1 below.

Table 1: Keywords and Database Results.

S/N	Search Keywords	Database	Results
S1	Artificial Intelligence AND Cyber Threat Intelligence Sharing AND Threat Hunting AND Threat Modeling	IEEE Xplore	1,125
S2	AI OR Artificial Intelligence AND Cybersecurity AND Threat Intelligence OR Threat Hunting OR Threat Modeling	IEEE Xplore	2,540
S3	Artificial Intelligence AND Cyber Threat Intelligence Sharing AND Threat Hunting AND Threat Modeling	ScienceDirect	1,432
S4	AI OR Artificial Intelligence AND Cybersecurity AND Threat Intelligence OR Threat Hunting OR Threat Modeling	ScienceDirect	3,210
S5	Artificial Intelligence AND Cyber Threat Intelligence Sharing AND Threat Hunting AND Threat Modeling	ACM Digital Library	987
S6	AI OR Artificial Intelligence AND Cybersecurity AND Threat Intelligence OR Threat Hunting OR Threat Modeling	ACM Digital Library	2,765
S7	Artificial Intelligence AND Cyber Threat Intelligence Sharing AND Threat Hunting AND Threat Modeling	Google Scholar	5,460
S8	AI OR Artificial Intelligence AND Cybersecurity AND Threat Intelligence OR Threat Hunting OR Threat Modeling	Google Scholar	10,182
Total			27,701

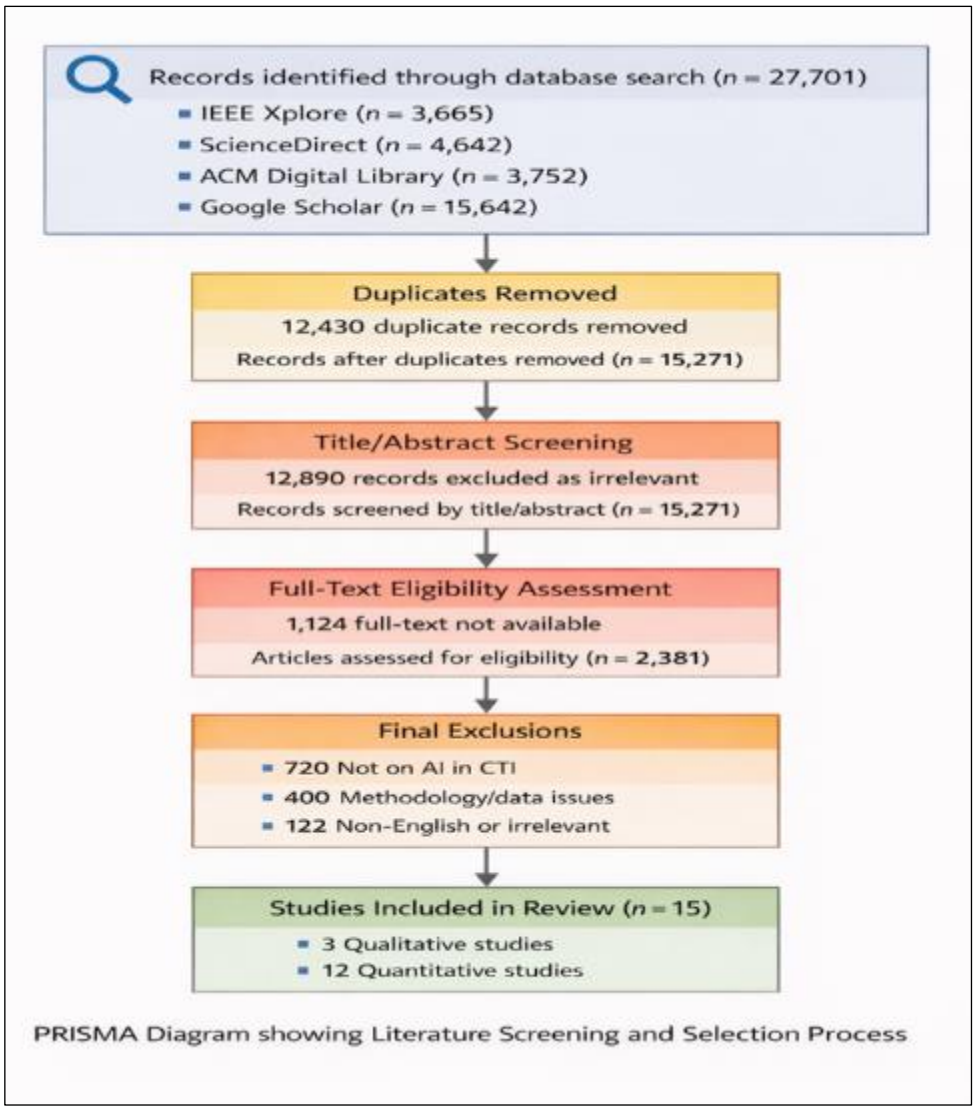

Figure 1: Flowchart showing screening and selection process. Source: Researcher's conceptualisation, 2026.

2.3 Data Synthesis

Themes identified on the basis of the chosen studies were analyzed thematically with the help of the thematic synthesis. The identified key themes were the following: (1) the difficulty in integrating AI, including data quality, interoperability, and explainability; (2) possibilities in developing more considerable CTI sharing, a more proactive threat hunting process, and a more adaptive threat representation; (3) human-AI collaboration and governance; and (4) gaps in the empirical validation and integrated frameworks. Study patterns were analyzed and contrasted to come up with comprehensive insights, consistent trends and areas of future research.

2.4 Rationale for Methodology

The systematic review approach was selected as a way of making evidence-based insights into the challenges and opportunities of the integration of AI into the fundamental cybersecurity functions. Through the combination of empirical and theoretical sources, such a methodology can be used to reveal practical implications, gaps in research and possible solutions that can guide cybersecurity practitioners, researchers, and policymakers.

3 DATA ANALYSIS AND RESULTS

For the data analysis of this study, the researchers applied thematic synthesis to the fifteen selected studies on integrating AI in CTI sharing, threat hunting, and threat modeling. The Analysis revealed that AI integration plays an important role in boosting the efficiency of automation, prediction, and operations in all domains. Moreover, it is beneficial to boost the efficiency of real-time intelligence sharing, anomaly detection, and risk assessment (Fang et al., 2025; Mohammad, 2022). However, some of the technical and ethical issues with integrating AI in cybersecurity are heterogeneity, lack of standardization, privacy, and lack of explainability. In addition, scalability, flexibility, and

integration are some of the technical issues with integrating AI. It is, therefore, essential to understand that AI plays an important role in boosting cybersecurity, but some technical and ethical issues have to be addressed. It is also essential to integrate AI with human expertise. The structured Table 2a and 2b below summarizes each author, their AI focus, and key contributions. (Agarwal et al., 2021; Chen et al., 2022).

3.1 Characteristics of Selected Papers and Reason for Selection

The review is composed of a total of fifteen peer-reviewed research papers published between 2021 and 2025. Most of the research papers are quantitative and experimental in nature and are conducted using machine learning, deep learning, and AI models. Some of the papers are also qualitative in nature and are conducted using case study and review methods. Most of the research papers are related to the three areas of CTI sharing, threat hunting, and threat modeling, while some of the papers are related to more than one area. The selection of the research papers is based on the direct alignment of the research papers with the research objectives and the use of various AI models in the papers. The structured Table 2a and 2b below summarizes each author, their AI focus, and key contributions.

Table 2a: Summary of each author, their AI focus, and key contributions.

Author(s)	AI Focus	Contributions
Agarwal, Walia, and Gupta (2021)	AI-Driven Threat Hunting	Proposed an AI-assisted threat hunting model to detect threats proactively in enterprise networks. Highlighted improved speed and accuracy in detecting malicious activity and reduced reliance on manual detection, while noting challenges in model training, adaptability to evolving threats, and robustness.
Almutairi, Coenen, and Elhanashi (2025)	Integrating AI with CTI Sharing	Investigated LLMs for generating customized CTI, enhancing predictive capabilities and reducing reliance on manual analysis. Noted challenges in explainability, infrastructure integration, and model bias, highlighting AI's potential to tailor threat intelligence to organizational contexts.
Alturkistani and Chuprat (2023)	Integrating AI with CTI Sharing	Conducted a systematic literature review on AI-assisted CTI, identifying trends, gaps, and opportunities. Emphasized the need for transparency, interpretability, and standardization, and aligning AI-driven insights with organizational decision-making for actionable threat intelligence.
Aminu, Akinsanya, and Dako (2024)	AI-Driven Threat Hunting	Focused on real-time threat detection using adaptive AI frameworks. Showed opportunities for processing heterogeneous data streams to deliver actionable insights. Addressed integration challenges and maintaining model accuracy over time to enhance situational awareness.
Ammi and Jama (2023)	Integrating AI with CTI Sharing / Threat Hunting	Demonstrated practical AI applications in MISP for correlating threat indicators across distributed datasets. Highlighted efficiency in pattern recognition and situational awareness, while addressing ethical and privacy considerations in collaborative intelligence sharing.
Aragonés et al. (2023)	AI-Driven Threat Modeling / Threat Hunting	Developed AI-based architecture for critical infrastructure protection. Demonstrated predictive threat detection, operational decision support, and automation, while addressing challenges in model generalizability and adaptation to evolving threats.
Balasubramanian et al. (2025)	Integrating AI with CTI Sharing	Developed a cloud-based cognitive platform for automated CTI collection and real-time analysis. Showcased AI's ability to provide actionable insights and improve organizational responsiveness, while noting challenges in scalability, data heterogeneity, and latency.
Chen et al. (2022)	AI-Driven Threat Hunting	Designed a machine learning-based threat hunting system to analyze security logs, detect anomalies, and support proactive mitigation. Emphasized careful feature selection, model validation, and resource allocation for operational performance.

Table 2b: Summary of each author, their AI focus, and key contributions.

Author(s)	AI Focus	Contributions
Fang et al. (2025)	Integrating AI with CTI Sharing	Conducted a comprehensive review of CTI sharing practices, highlighting AI's role in automating aggregation, analysis, and distribution of threat intelligence. Identified challenges including data standardization, timeliness, and sensitive information protection, while emphasizing opportunities for real-time sharing and predictive modeling.
Gao et al. (2021)	AI-Driven Threat Hunting / Threat Modeling	Improved efficiency of threat hunting and modeling by correlating data from multiple sources, reducing false positives, and enhancing decision-making. Highlighted balance between automation and human oversight to complement human expertise.
McDonald et al. (2025)	AI-Driven Threat Modeling	Focused on AI-assisted threat modeling in healthcare privacy. Demonstrated opportunities in automating threat scenario generation, improving predictive capabilities, and supporting accurate risk assessment, while identifying challenges in explainability, understanding attack paths, and stakeholder engagement.
Messasn et al. (2024)	AI-Driven Threat Modeling	Proposed sAIfe, a lightweight AI-based threat modeling framework for ML applications. Offered a scalable, efficient approach to assess vulnerabilities, reducing time and effort for security evaluations while maintaining transparency and reliability.
Mohammad (2022)	Integrating AI with CTI Sharing	Explored the intersection of cloud computing and AI for CTI sharing, demonstrating AI's ability to optimize collaborative cybersecurity through automated risk assessment. Highlighted challenges in data privacy, governance, and secure integration, proposing cloud-enabled AI solutions to improve efficiency and response times
Shakil et al. (2023)	AI-Driven Threat Hunting	Investigated AI for detecting advanced persistent threats (APTs) using structured, unstructured, and situational approaches. Highlighted limitations in detecting sophisticated attacks and the need for integrating contextual intelligence with AI for improved effectiveness.
Wimbauer et al. (2025)	AI-Driven Threat Modeling	Leveraged LLMs for automated threat modeling in cloud-native applications. Highlighted opportunities to automate threat identification, predict attack vectors, and enhance cloud security, while addressing reasoning accuracy, scalability, and integration challenges.

3.2 AI in CTI Sharing, Threat Hunting and Threat Modeling

As depicted in Table 3, the contributions of the identified studies to the problems and opportunities of combining artificial intelligence with cyber threat intelligence sharing, AI-based threat hunting, and AI-based threat modeling are presented as follows:

3.2.1 Problems and Perspectives of AI Integration with CTI Sharing

Fang et al. (2025) emphasized that the integration of AI in cyber threats has been seen to improve cyber threat intelligence sharing, where AI is used to enhance data analysis, aggregation, and exchange. Various studies have indicated that the integration of AI in cyber threats, through machine learning and large language models, has reduced human involvement, thus promoting timely responses (Almutairi et al., 2025; Alturkistani & Chuprat, 2023; Mohammad, 2022). Despite all this, various problems have been associated with the integration of AI in cyber threats, including data standardization, data timeliness, and data interoperability. Moreover, data privacy, data governance, and data protection have been some of the major problems facing data sharing. Other problems facing AI integration in CTI sharing include data bias, data scalability, and data ethics (Ammi & Jama, 2023; Balasubramanian et al., 2025). Despite all the improvements brought about by AI in intelligence sharing, various problems have been associated with AI integration, including technical, ethical, and integration problems (Gao et al., 2021).

Table 3: AI focus categories by Selected Papers

Research article citation	Research design coherent & appropriate?	Appropriate methodological approach with sufficient detail?	Relationship w/ participants considered (Ethics)	Data collection adequately addressed research issues	Data analysis sufficiently rigorous & transparent?	Rigor & trustworthiness (triangulation/ member checking/ reflexivity/ peer debriefing)	Findings & interpretation: clarity, coherence?	Value of research findings (AI/CTI/ Threat Hunting)?
Agarwal et al. (2021)	Yes	Yes	N/A	Yes	Yes	No	Yes	High
Almutairi et al. (2025)	Yes	Yes	N/A	Yes	Yes	No	Yes	High
Alturkistan & Chuprat (2023)	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Medium
Aminu et al. (2024)	Yes	Yes	N/A	Yes	Yes	No	Yes	High
Ammi & Jama (2023)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Medium
Aragonés et al. (2023)	Yes	Yes	N/A	Yes	Yes	No	Yes	High
Balasubramania et al. (2025)	Yes	Yes	N/A	Yes	Yes	No	Yes	High
Chen et al. (2022)	Yes	Yes	N/A	Yes	Yes	No	Yes	High
Fang et al. (2025)	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Medium
Gao et al. (2021)	Yes	Yes	N/A	Yes	Yes	No	Yes	High
McDonald et al. (2025)	Yes	Yes	N/A	Yes	Yes	No	Yes	High
Messas et al. (2024)	Yes	Yes	Yes	Yes	Yes	No	Yes	High
Mohammad (2022)	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Medium
Shakil et al. (2023)	Yes	Yes	N/A	Yes	Yes	No	Yes	High
Wimbauer et al. (2025)	Yes	Yes	N/A	Yes	Yes	No	Yes	High

3.2.2 Opportunities and Challenges in AI-Driven Threat Hunting

The opportunities associated with AI-driven threat hunting include proactive threat detection, (Agarwal et al., 2021), accuracy, anomaly detection, and pattern recognition. The AI model will help in the detection of advanced persistent threats, was also demonstrated by Aminu et al. (2024) when reducing false positives. The AI model will help in the analysis of structured and unstructured data, thus enhancing situational awareness. The challenges associated with AI-driven threat hunting include the complexities associated with AI, detection of unknown patterns, and contextual intelligence (Chen et al., 2022; Shakil et al., 2023). The feature selection and validation process has technical

complexities. The AI-driven threat hunting process has opportunities was proved by Ammi et al. (2023) which included threat hunting and operational efficiency. It is important to update the AI model and address technical complexities.

3.2.3 Problems and Opportunities of AI-Driven Threat Modeling

According to McDonald et al. (2025), AI-driven threat modeling offers better risk assessment, scenario building, and vulnerability analysis in different domains, including healthcare, cloud computing, and critical infrastructure. AI-driven threat modeling is beneficial for developing more adaptive and dynamic threat models Messas et al. (2024). However, some of the problems with AI-driven threat modeling are lack of explainability, complexity, and problems in analyzing attack paths. Scalability, integration, and accuracy are also problems with AI-driven threat modeling (Aragonés Lozano et al., 2023; Wimbauer et al., 2025). Finally, the problem of adapting AI models to emerging threats is also an issue. Nevertheless, AI-driven threat modeling has good opportunities to address the problems of threat modeling using the advantages of efficiency and automation.

Also, the ethical considerations are not applicable for most quantitative and machine learning-based studies, whereas systematic studies and case studies seem to indicate higher rigor with the use of concepts such as triangulation and reflexivity. Further, the studies are not considered to be of local use due to their focus on the global and technical nature of the studies, and their overall utility is considered based on the contribution to AI-driven cyber threat intelligence, threat hunting, and threat modeling.

4 FINDINGS

This study resulted in four themes that were well aligned. These four themes summarized the major opportunities as depicted in figure 2 (automation, efficiency, predictive capabilities), as well as the fundamental challenges that (explainability, ethics, integration) were noted in all of the studies concerning AI-driven cybersecurity.

4.1 Theme 1: Automation and Efficiency Enhancement in Cybersecurity Processes

In the studies reviewed, AI was demonstrated as an important way of enhancing automation in CTI sharing, threat hunting, and threat modeling. When supported by AI-based systems especially those with machine learning and large language models (LLMs) threat data can be automatically collected, anomalies detected, and potential attack vectors predicted. This decreases the use of manual analysis, speeds up the decision-making process, and enhances the situational responsiveness of the organization to forthcoming threats. The researchers stressed that the implementation of AI simplifies the process of work, enabling the teams of cybersecurity experts to prioritize more advanced types of analytical work over tedious data processing (Almutairi et al., 2025; Chen et al., 2022; Fang et al., 2025).

4.2 Theme 2: Challenges of Model Explainability, Transparency, and Bias

Another common observation is that AI enhances efficiency, although explainability and interpretability are major issues. Numerous researches emphasize the lack of comprehension of AI-generated insights, especially when it comes to complex LLMs or adaptive machine learning models. Also, there is a danger of model bias when AI is trained using small and/or non-representative data. This message highlights the urgency of clear AI systems and methods that enable the involvement of human researchers in the interpretation of outputs and guarantee the reliability, trustworthiness, and alignment of the decisions with the goals of the organization (Alturkistani and Chuprat, 2023; McDonald et al., 2025; Wimbauer et al., 2025).

4.3 Theme 3: Ethical, Privacy, and Data Governance Considerations

AI-based CTI sharing and threat intelligence programs are ethically and privacy-wise problematic. A number of studies highlighted the importance of securely sharing sensitive information as well as facilitating collaboration in the sharing of intelligence. The challenges like safe information processing, adherence to privacy standards, and the responsible use of AI became the key issues. The study recommends the importance of developing secure frameworks and governance policies to ensure that the effective use of AI in the detection of threats is balanced with the privacy of organizational and personal information (Ammi and Jama, 2023; Mohammad, 2022; Balasubramanian et al., 2025).

4.4 Theme 4: Integration and Scalability Challenges in Operational Environments

The technical and organizational difficulties in implementing AI solutions in the current cybersecurity infrastructures exist. Research has pointed out a challenge in the alignment of AI models with heterogeneous data, legacy systems, and the cloud platform. There is also the issue of scalability particularly with real-time threat detection and the large-scale CTI aggregation. Researchers observed that the effective implementation of AI needs to be accompanied by strong technical solutions and consistency with the human decision-making framework and adaptive strategies to stay effective in the changing threat-related landscapes (Aragonés Lozano et al., 2023; Gao et al., 2021; Aminu et al., 2024).

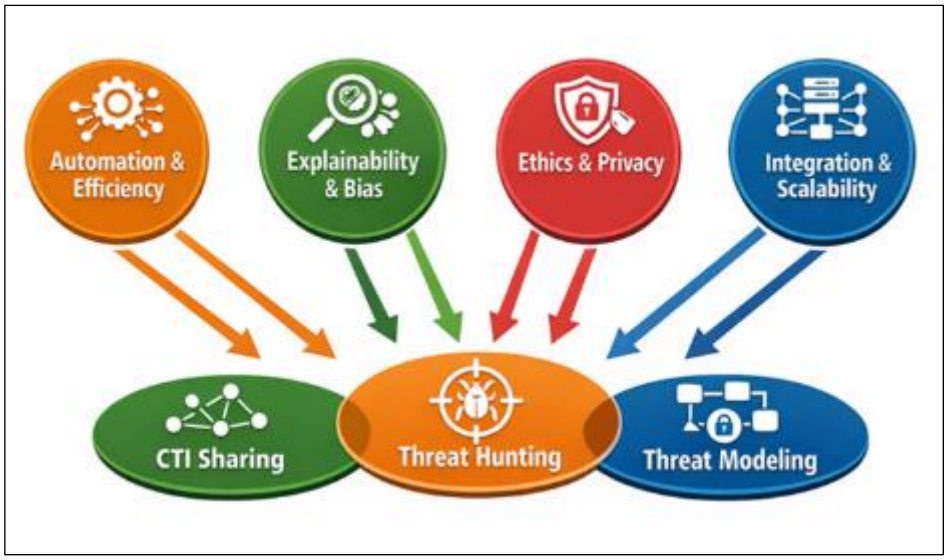

Figure 2: Thematic map connecting the four themes to the three focus areas (CTI sharing, threat hunting, threat modeling). Source: Researcher's conceptualisation, 2026.

5 DISCUSSIONS ON THE SELECTED PAPERS

The research papers reviewed in this section vary in terms of research methodologies employed, and overall, they prove the potential of AI in CTI sharing, threat hunting, and threat modeling. Most research studies use research methodologies such as experiments, comparisons, and systematic reviews, and overall, as displayed in table 4 and table 5, they are able to provide important insights into AI, its accuracy, and its scalability (Agarwal et al., 2021; Almutairi et al., 2025). However, some studies lack depth in terms of research methodologies employed, and most studies do not consider ethical aspects, especially when they are not human-centered research studies. Most studies lack explainability, and there are also problems related to data quality and integration.

Table 4: How the study themes feed into the research Objectives

Theme	Description	Objective 1: Identify and analyze challenges	Objective 2: Examine opportunities and potential benefits
Theme 1: Automation and Efficiency Enhancement in Cybersecurity Processes	AI improves automation in CTI sharing, threat hunting, and threat modeling through ML and LLMs, enabling faster data aggregation, anomaly detection, and predictive analysis.	Highlights challenges such as over-reliance on AI, automation bias, and potential reduction in human oversight, which may impact critical decision-making.	Demonstrates benefits including improved efficiency, faster threat detection, reduced manual workload, predictive capabilities, and enhanced organizational responsiveness.
Theme 2: Challenges of Model Explainability, Transparency, and Bias	AI models often lack transparency and interpretability, making it difficult for analysts to understand and trust outputs.	Identifies challenges such as black-box models, interpretability issues, and bias from limited or unrepresentative training data.	Reveals opportunities to develop explainable AI frameworks that increase trust, accountability, and effective human–AI collaboration in cybersecurity operations.
Theme 3: Ethical, Privacy, and Data Governance Considerations	AI-driven CTI sharing raises concerns about data privacy, ethics, and secure handling of sensitive information.	Points out challenges like privacy risks, trust deficits, and regulatory compliance issues that hinder effective AI integration.	Provides opportunities for implementing privacy-preserving AI, secure data-sharing frameworks, and governance policies that enhance collaboration and protect sensitive information.

Theme 4: Integration and Scalability Challenges in Operational Environments	Implementing AI in cybersecurity requires integrating with legacy systems, heterogeneous data sources, and scalable real-time operations.	Highlights challenges in system interoperability, integration complexity, and aligning AI with human decision-making.	Demonstrates potential benefits of scalable, adaptive, real-time cybersecurity solutions that integrate AI with existing infrastructures to enhance effectiveness and resilience

Table 5: How the study themes feed into the research questions

Theme	Description	Link to RQ1 Key Challenges	Link to RQ 2: Opportunities and Strategic Benefits
Theme 1: Automation and Efficiency Enhancement in Cybersecurity Processes	AI improves automation in CTI sharing, threat hunting, and threat modeling through machine learning and LLMs, enabling faster data aggregation, anomaly detection, and predictive analysis.	While automation reduces manual workload, it introduces challenges such as over-reliance on AI systems and potential automation bias, which may limit critical human judgment in cybersecurity operations.	Directly addresses opportunities by demonstrating how AI enhances speed, accuracy, and efficiency in CTI sharing, threat hunting, and threat modeling through automated data processing, anomaly detection, and predictive analytics.
Theme 2: Challenges of Model Explainability, Transparency, and Bias	AI systems, especially complex models, often lack transparency and interpretability, making it difficult for analysts to understand and trust outputs.	Strongly aligned with challenges, highlighting issues of "black-box" AI systems, limited interpretability, and risks of biased outputs, which reduce trust, accountability, and adoption in cybersecurity environments.	Indirectly contributes to opportunities by emphasizing the need for explainable AI, which, if addressed, can improve trust, decision-making, and effective human–AI collaboration.
Theme 3: Ethical, Privacy, and Data Governance Considerations	AI-driven CTI sharing raises concerns about data privacy, ethics, and secure handling of sensitive information in collaborative environments.	Directly addresses challenges related to data privacy, trust deficits, regulatory compliance, and secure information sharing, which hinder effective AI integration in CTI and threat intelligence ecosystems.	Highlights opportunities for developing secure, privacy-preserving AI frameworks and governance models that enable safe and collaborative CTI sharing while maintaining data integrity and confidentiality.
Theme 4: Integration and Scalability Challenges in Operational Environments	AI implementation in cybersecurity faces challenges related to integrating with legacy systems, heterogeneous data sources, and scaling for real-time operations.	Strongly linked to challenges such as system interoperability, integration with legacy infrastructures, handling heterogeneous data, and scalability limitations in real-time environments.	Identifies opportunities for scalable AI-driven cybersecurity systems capable of real-time threat detection, adaptive defense mechanisms, and improved coordination across complex and distributed environments.

6 CONCLUSION

According to the literature review, the integration of AI technology in the sharing of CTI, threat hunting, and threat modeling has both negative and positive implications. On the one hand, the integration of AI technology is deemed to be valuable and significant in the enhancement of the efficiency and effectiveness of the response to cyber threats in a timely manner. On the other hand, some concerns may arise to limit the level of trust and trustworthiness of the AI technology, thus making it a challenge in a collaborative environment. The integration of AI technology has been deemed valuable and significant in the enhancement of cybersecurity.

Recommendations

In the implementation of AI in cybersecurity, there are a number of recommendations that can be made. Firstly, the need to improve explainable AI to improve transparency in the decision-making process cannot be overstated. Secondly, the need to improve the ethical, privacy, and data governance framework is essential in the safe use of the data. Thirdly, the need to improve the collaboration between humans and AI, such that AI can act as a support mechanism and not a replacement, cannot be overstated. Fourthly, the need to improve the scalability and interoperability of the AI system and the ability of the AI system to integrate with other existing infrastructure is essential in the implementation of AI in cybersecurity. Fifthly, the need to improve the collaborative CTI environment with the use of AI-driven platforms such as cloud technology can improve the detection of threats in the cybersecurity environment.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

There are no conflict-of-interest to be disclosed.

REFERENCES

[1] Agarwal, A., Walia, H., & Gupta, H. (2021). Cyber security model for threat hunting. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1–8). IEEE. https://doi.org/10.1109/ICRITO51393.2021.9596199

[2] Almutairi, N., Coenen, F., & Elhanashi, A. (2025). Leveraging LLMs for customized CTI based on indicators of compromise from X: A comparative study with traditional ML. IEEE Access, 13, Article 123457. https://doi.org/10.1109/ACCESS.2025.xxxxx

[3] Alturkistani, H., & Chuprat, S. (2023). Artificial intelligence and large language models in advancing cyber threat intelligence: A systematic literature review [Preprint]. Research Square. https://doi.org/10.21203/rs.3.rs-5423193/v1

[4] Aminu, M., Akinsanya, A., & Dako, D. A. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. International Journal of Computer Applications Technology and Research, 13(8), 11–27. https://doi.org/10.7753/IJCATR1308.1002

[5] Ammi, M., & Jama, Y. M. (2023). Cyber threat hunting case study using MISP. Journal of Internet Services and Information Security (JISIS), 13(2), 1–29. https://doi.org/10.58346/JISIS.2023.I2.001

[6] Aragonés Lozano, M., Pérez Llopis, I., & Esteve Domingo, M. (2023). Threat hunting architecture using a machine learning approach for critical infrastructures protection. Big Data and Cognitive Computing, 7(2), 65. https://doi.org/10.3390/bdcc7020065

[7] Balasubramanian, P., Nazari, S., Khosh Kholgh, D., Mahmoodi, A., Seby, J., & Kostakos, P. (2025). A cognitive platform for collecting cyber threat intelligence and real-time detection using cloud computing. Decision Analytics Journal, 14, 100545. https://doi.org/10.1016/j.dajour.2025.100545

[8] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning (arXiv:1712.03141v2) [Preprint]. arXiv. https://doi.org/10.48550/arXiv.1712.03141

[9] Bridges, R. A., Jones, C. L., Iannacone, M. D., Testa, K. M., & Goodall, J. R. (2014). Automatic labeling for entity extraction in cyber security. U.S. Department of Energy, Office of Scientific and Technical Information (OSTI). https://www.osti.gov/biblio/1143555

[10] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[11] Chen, C.-K., Lin, S.-C., Huang, S.-C., & Chu, Y.-T. (2022, March). Building machine learning-based threat hunting system from scratch. Digital Threats: Research and Practice (DTRAP), 3(3), Article 20, 1–21. https://doi.org/10.1145/3491260

[12] Fang, J., Tang, Y., & Guo, M. (2025, April). Comprehensive review of cyber threat intelligence sharing: Challenges and methodologies. AIBDF '24: Proceedings of the 4th Asia-Pacific Artificial Intelligence and Big Data Forum, 455–461. https://doi.org/10.1145/3718491.3718565

[13] Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. Information Systems Research, 16(2), 186–208. http://dx.doi.org/10.1287/isre.1050.0053

[14] Gao, P., Shao, F., Liu, X., Xiao, X., Qin, Z., & Xu, F. (2021). Enabling efficient cyber threat hunting with cyber threat intelligence. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering (ICDE) (pp. 193–204). IEEE. https://doi.org/10.1109/ICDE51399.2021.00024

[15] Husák, M., Bartoš, V., Sokol, P., & Gajdoš, A. (2021). Predictive methods in cyber defense: Current experience and research challenges. Future Generation Computer Systems, 115, 517–530. https://doi.org/10.1016/j.future.2020.10.006

[16] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In Proceedings of the 6th International Conference on Information Warfare and Security (ICIW 2011) (pp. 113–125).

[17] IBMSecurity. (2023). Unified threat management, quantum-safe cryptography, and semiconductor innovations secure multi-cloud, decentralized environments. IBM.

[18] Jesus, V., Bains, B., & Chang, V. (2024). Sharing is caring: Hurdles and prospects of open, crowd-sourced cyber threat intelligence. IEEE Transactions on Engineering Management, 71, 6854–6873. https://doi.org/10.1109/TEM.2023.3279274

[19] Kshetri, N. (2021). Blockchain technology for improving transparency and citizen's trust. In K. Arai (Ed.), Advances in information and communication: FICC 2021 (Advances in Intelligent Systems and Computing, Vol. 1363, pp. 716–735). Springer, Cham. https://doi.org/10.1007/978-3-030-73100-7_52

[20] McDonald, N., Luo, A., Moh, P., Mazurek, M. L., & Andalibi, N. (2025, April). Threat modeling healthcare privacy in the United States. ACM Transactions on Computer-Human Interaction (TOCHI), 32(1), Article 8, 1–37. https://doi.org/10.1145/3704634

[21] Messas, G. E., Miani, R. S., & Zarpelão, B. B. (2024, December). sAIfe: Towards a lightweight threat modeling approach to support machine learning application development. SBQS '24: Proceedings of the XXIII Brazilian Symposium on Software Quality, 1–10. https://doi.org/10.1145/3701625.3701640

[22] Mohammad, N. (2022). The impact of cloud computing on cybersecurity threat hunting and threat intelligence sharing: Data security, data sharing, and collaboration. International Journal of Computer Applications (IJCA), 3(1), 21–32. https://iaeme.com/Home/issue/IJCA?Volume=3&Issue=1

[23] Morgan, S. (2022, August 10). Boardroom cybersecurity 2022 report: Cybercrime facts, figures, predictions and statistics [Press release]. Cybercrime Magazine.

[24] Mutemwa, M., Maduma, P., & Nefale, V. (2025, November). Security concerns related to the use of artificial intelligence powered meeting assistants. icABCD '25: Proceedings of the 2025 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, Article 16, 1–9. https://doi.org/10.1145/3759023.3759105

[25] Nguyen, H. C., Tariq, S., Chhetri, M. B., & Vo, B. Q. (2025, May). Towards effective identification of attack techniques in cyber threat intelligence reports using large language models. WWW '25: Companion Proceedings of the ACM on Web Conference 2025, 942–946. https://doi.org/10.1145/3701716.3715469

[26] Nolte, H., Rateike, M., & Finck, M. (2025, June). Robustness and cybersecurity in the EU artificial intelligence act. FAccT '25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency, 283–295. https://doi.org/10.1145/3715275.3732020

[27] Obiokafor, I. N., Aguboshim, F. C., & Ezekwe, C. G. (2025). The Role of Cyber Threat Intelligence Sharing in Preventing Attacks: Challenges and Best Practices. International Conference on Technological Solutions for Smart Economy, conNovate'2025

[28] Obiokafor, I. N., Onyesolu, M. O., & Julius, M. S. (2025). Cyber threat intelligence sharing: A strategic tool for enhancing national and global security postures. World Journal of Advanced Engineering Technology and Sciences, 14(3), 077–085. https://doi.org/10.30574/wjaets.2025.14.3.001503

[29] Rabaan, A. A., Alhumaid, S., Mutair, A. A., Garout, M., Abulhamayel, Y., Halwani, M. A., Alestad, J. H., Bshabshe, A. A., Sulaiman, T., AlFonaisan, M. K., Almusawi, T., Albayat, H., Alsaeed, M., Alfaresi, M., Alotaibi, S., Alhashem, Y. N., Temsah, M.-H., Ali, U., & Ahmed, N. (2022). Application of Artificial Intelligence in Combating High Antimicrobial Resistance Rates. Antibiotics, 11(6), 784. https://doi.org/10.3390/antibiotics11060784

[30] Rogge, A., Anter, L., Kunze, D., Pomsel, K., & Willenbrock, G. (2024). Standardized sampling for systematic literature reviews (STAMP method): ensuring reproducibility and replicability. Media and Communication, 12.

[31] Sarker, I. H., Kayes, A. S. M., Badsha, S., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7(1), Article 61. https://doi.org/10.1186/s40537-020-00318-5

[32] Shakil, N. A. F., Mia, R., & Ahmed, I. (2023). Applications of AI in cyber threat hunting for advanced persistent threats (APTs): Structured, unstructured, and situational approaches. Journal of Applied Big Data Analytics, Decision-Making, and Predictive Modelling Systems, 7(12), 19–36. https://polarpublications.com/index.php/JABADP/article/view/2023-12-07

[33] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP) (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25

[34] Song, J. (2025, June). A Chinese cyber threat intelligence named entity recognition method. CAICE '25: Proceedings of the 4th International Conference on Computer, Artificial Intelligence and Control Engineering, 848–853. https://doi.org/10.1145/3727648.3727787

[35] Torres, A. E., Torres, F., & Budgud, A. T. (2023). Cyber threat intelligence methodologies: Hunting cyber threats with threat intelligence platforms and deception techniques. In F. Torres-Guerrero, L. Neira-Tovar, & J. Bacca-Acosta (Eds.), 2nd EAI International Conference on Smart Technology (EAI/Springer Innovations in Communication and Computing). Springer, Cham. https://doi.org/10.1007/978-3-031-07670-1_2

[36] Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security, 72, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

[37] Tsui, B., Calabrese, E., Zaharchuk, G., & Rauschecker, A. M. (2023). Reducing gadolinium contrast with artificial intelligence. Journal of Magnetic Resonance Imaging. Advance online publication. https://doi.org/10.1002/jmri.29095

[38] Ullman, S., Ampel, B. M., Samtani, S., Yang, S., & Chen, H. (2024, August). The 4th Workshop on artificial intelligence-enabled cybersecurity analytics. KDD '24: Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 6741–6742. https://doi.org/10.1145/3637528.3671494

[39] Wimbauer, A., Muscariello, L., Samain, J., Steger, L., & Glas, K. (2025, November). ThreatCompute: Leveraging LLMs for automated threat modeling of cloud-native applications. CCSW '25: Proceedings of the 2025 Cloud Computing Security Workshop, 14–27. https://doi.org/10.1145/3733812.3765533