International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 30-36 www.ijaem.net ISSN: 2395-5252

The Evolution of Threat Intelligence: Trends and Innovations in Cyber Defense

Saira Sofeya Binti Abdul Harris, Mohamad Fadli bin Zolkipli
Student, School of Computing, Universiti Utara Malaysia, Kedah, Malaysia

----
Date of Submission: 25-06-2024 Date of Acceptance: 05-07-2024

ABSTRACT: In the dynamic realm of cybersecurity, understanding the evolution of threat intelligence and its associated techniques is crucial. This study explores the historical progression and contemporary trends of threat intelligence, focusing on its application in cyber defense. It investigates how artificial intelligence (AI) and machine learning (ML) are revolutionizing threat intelligence, enabling organizations to proactively identify and counter emerging threats. Furthermore, the paper examines the integration of diverse data sources and contextual information, known as threat intelligence fusion and enrichment, to enhance defense strategies. Additionally, it discusses the implications of cloud computing and the Internet of Things (IoT) on threat intelligence, emphasizing the need for tailored approaches in these environments. Through a synthesis of research and practical insights, this paper provides valuable insights for cybersecurity practitioners and researchers alike.

KEYWORDS: Threat intelligent, Artificial intelligence, Machine learning, Threat hunting

I. INTRODUCTION

Threat intelligence (TI) encompasses data essential for organizations to comprehend potential or existing cyber threats posing security risks. This information includes detailed details on threats, such as indicators of compromise (IOCs) including IP addresses, domains, file hashes, and other artifacts that indicate malicious activity.[1]Collected from diverse sources including hacker forums, security articles, and underground markets, this information sheds light on the strategies and methodologies employed by threat actors.[2]

Threat intelligence denotes data crucial for organizations to grasp potential or ongoing cyber threats that may jeopardize their security. Sourced from a variety of outlets including security researchers, governmental bodies, industry analyses, and even clandestine corners of the internet such as the dark web, this information offers valuable insights into the methods and strategies deployed by threat actors. By delving into the tactics, techniques, and procedures utilized, as well as indicators of compromise (IoCs), threat intelligence aids organizations in both detecting and responding effectively to cyber threats. Through the analysis and application of such intelligence, organizations can bolster their cybersecurity measures, proactively shielding their systems and data from malicious cyber attacks.[3]Threat hunting techniques entail the proactive exploration and detection of potential threats within an organization's network or systems, aiming to uncover sophisticated threats that may have eluded conventional security measures. These methods are designed to unearth advanced threats, such as Advanced Persistent Threats (APTs), that could be concealed within the infrastructure.[4] These techniques can include: Behavior-Based Threat Hunting involves a methodical examination of behaviors and patterns within a network to uncover potential threats by identifying deviations from normal activity. This proactive approach allows cybersecurity professionals to detect threats that may have evaded traditional security measures by analyzing anomalous behavior indicative of malicious intent.

The Hybrid Approach to threat hunting integrates offensive security strategies, techniques, and processes, incorporating adversary emulation to enhance threat detection capabilities. By adopting elements of offensive security tactics, organizations can better understand potential attack vectors and simulate adversary behaviors, thereby strengthening their defensive posture.

Behavior-Based Threat Hunting Frameworks, exemplified by tools like BTH (Behavior-Based Threat Hunting), provide structured frameworks for conducting threat hunting activities. These frameworks focus on analyzing adversarial activity profiles, enabling organizations to effectively identify and respond to threats. By leveraging such frameworks, organizations can not only detect and mitigate existing threats but also develop proactive security strategies to prevent future attacks.[5]

II. LITERATURE REVIEW

In the field of cybersecurity, Threat Hunting has become essential for spotting and neutralizing cyber threats before they inflict substantial damage. Threat Hunters play a vital role in sorting through extensive data sets, which often contain routine patterns, to pinpoint irregularities that could signal malicious behavior. To tackle the obstacles posed by the sheer volume of data and the demand for immediate analysis, the integration of Artificial Intelligence, especially Machine Learning (ML) methods, has proven pivotal in improving the speed and accuracy of threat detection.

Enhancing Threat Hunting capabilities involves leveraging advanced visualization techniques to assist specialists in comprehending the intricate challenges they encounter. By offering insightful visual representations, analysts can distinguish between benign and malicious data more effectively, thereby reducing cognitive strain and bolstering Cyber Situational Awareness (CSA). The incorporation of cutting-edge visualization models into threat hunting frameworks significantly contributes to safeguarding Critical Infrastructures, empowering Threat Hunters to make well-informed decisions based on data-driven insights.

Although Machine Learning (ML) application in Threat Hunting has gained momentum, there's a pressing need for comprehensive frameworks capable of efficiently gathering, categorizing, and aggregating threat intelligence data for security purposes. While previous studies have explored the integration of ML algorithms into various cybersecurity tools such as Security Information and Event Management (SIEM) systems, Firewalls, and Intrusion Detection Systems (IDS) to enhance cyber situational awareness and threat detection capabilities, a unified architecture tailored for Critical Infrastructures Protection is still lacking.[6]

Recent research endeavors have concentrated on devising ML-based approaches for malware threat hunting in time-sensitive systems, software-defined networks, and Internet of Things (IoT) environments. These efforts underscore the significance of harnessing ML techniques to confront the evolving cyber threat landscape and streamline threat detection processes. Moreover, the fusion and enrichment of threat intelligence data sourced from diverse outlets, including open-source intelligence (OSINT), play a pivotal role in augmenting threat hunting capabilities and facilitating proactive defense strategies.

Threat intelligence fusion and enrichment serve as pivotal mechanisms in elevating the caliber and applicability of threat data, empowering organizations to make well-informed decisions and implement preemptive security measures. By amalgamating and cross-referencing threat intelligence from various origins, organizations can cultivate a comprehensive grasp of the threat landscape, thereby enhancing their capacity to detect and counter cyber threats efficiently.

Memory forensics emerges as another indispensable facet of threat hunting, offering investigators the means to scrutinize volatile memory and unveil illicit activities while pinpointing potential security breaches. Through the examination of memory dumps and analysis of memory artifacts, cybersecurity practitioners can unearth advanced malware, unauthorized access attempts, and other suspicious behaviors that may elude conventional security protocols. Integrating memory forensics into threat hunting protocols augments the depth and precision of threat detection, empowering organizations to identify and neutralize threats in their nascent stages.

Within the domain of insider threats, organizations confront the challenge of identifying and mitigating risks posed by malicious insiders exploiting their privileged access to sensitive data. A robust insider threat mitigation strategy is imperative for curtailing the impact of insider-driven risks on organizational security, mitigating potential financial and reputational repercussions. By amalgamating threat hunting methodologies with memory forensics and proactive threat intelligence initiatives, organizations can fortify their security posture and effectively defend against a broad spectrum of cyber threats.[7]

The growing number of IoT devices has resulted in an increase in malware assaults, with diverse strains spreading across malware families. Additionally, the emergence of DDoS-for-hire services on the dark web, offering botnets with significant attack bandwidth, has further intensified the threat landscape.

Detecting and categorizing malware threats is a critical challenge in cybersecurity. Malware Threat Hunting is a term commonly used to describe the process of identifying and mitigating malware threats. While extensive research exists on Windows PE-based malwares, literature on IoT-based malwares, particularly in the context of cross-architecture IoT malware threat hunting, is relatively limited.

Several valuable surveys focus on IoT malwares, emphasizing static and dynamic analysis. This document seeks to complement existing surveys by providing a thorough review of recent advancements in research methodologies for IoT malware threat hunting. It discusses the strengths and weaknesses of these methodologies, offers a contemporary taxonomy of features for identifying malwares, and examines the obstacles and considerations in conducting research on cross-architecture IoT malware threat hunting.

The primary contributions of the survey include filling gaps in existing literature, reviewing recent research methodologies, proposing a taxonomy of features for malware detection, and discussing challenges in cross-architecture IoT malware threat hunting. The document underscores the complexities involved in dealing with multiple CPU architectures, operating system platforms, and diverse target devices within a unified learning approach.[8]

In conclusion, threat hunting has become crucial to cybersecurity since it helps businesses recognize and neutralize threats before they become serious risks.The integration of Artificial Intelligence and advanced visualization techniques enhances Threat Hunting's effectiveness by improving its speed, accuracy, and Cyber Situational Awareness. While Machine Learning applications in Threat Hunting have advanced, there's a need for comprehensive frameworks tailored for protecting Critical Infrastructures. Memory forensics and proactive threat intelligence initiatives further enhance Threat Hunting capabilities, particularly in tackling insider threats. Moreover, the rise of IoT devices has increased malware threats, requiring advancements in cross-architecture IoT malware threat hunting methods. Overall, ongoing research in Threat Hunting methodologies and the integration of threat intelligence data show promise in bolstering organizations' cybersecurity defenses against evolving cyber threats.

III. THE ROLE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN THREAT INTELLIGENCE

ML techniques are integral for automating threat detection within critical infrastructures, as they facilitate rapid data processing to identify potential security threats efficiently. By harnessing ML capabilities, organizations can significantly enhance their ability to detect anomalies, patterns, and indicators of compromise in real-time, thereby enabling proactive threat mitigation and incident response strategies.

In the realm of cybersecurity, advanced visualization techniques play a pivotal role in aiding Threat Hunters to swiftly and accurately comprehend security incidents. ML-driven visualizations serve as invaluable tools, presenting complex data in intuitive displays that enable Threat Hunters to discern trends, anomalies, and potential threats with greater ease and precision. This heightened understanding of security events facilitated by advanced visualizations ultimately leads to more informed decision-making and more effective incident response actions.[6]

Moreover, ML and data visualizations empower Threat Hunters to engage in hypothesis generation regarding ongoing security incidents. Through the analysis of data using ML techniques, Threat Hunters can formulate educated hypotheses concerning the nature of security threats and their potential impact on critical infrastructures. This ability to generate hypotheses enables Threat Hunters to better assess the severity of security events, predict potential outcomes, and take proactive measures to mitigate risks effectively.

Furthermore, the adoption of a system architecture that supports dynamic and adaptable addition of ML techniques is essential for maintaining robust threat detection capabilities. This architectural flexibility empowers Threat Hunters to select and deploy the most suitable ML algorithms based on evolving threats and specific security requirements. By incorporating dynamic ML techniques into their operations, organizations can bolster their threat detection capabilities, enhance the accuracy of security analysis, and respond more effectively to emerging cyber threats, thereby fortifying their overall cybersecurity posture.

Reliable intelligence stands as a critical foundation for proactive cybersecurity defense, enabling organizations to anticipate and counter potential cyber threats effectively. Timely and trustworthy information empowers organizations to stay ahead of malicious actors by implementing necessary preventive measures promptly.

Cyber Threat Intelligence (CTI) provides comprehensive insights into anticipated cyberattacks, offering detailed information on attack methodologies, perpetrator profiles, potential targets, and tools utilized. This knowledge equips organizations to devise robust defense strategies and mount effective responses against potential threats, thereby minimizing the impact of cyber attacks.

However, collecting and analyzing vast amounts of online threat data present significant challenges in enhancing CTI capabilities. To mitigate emerging threats effectively, organizations must develop comprehensive CTI strategies that encompass rigorous data analysis methodologies. This involves navigating complexities such as web crawling mechanisms, understanding foreign languages, decoding cyber terminology, and deciphering the intricate structures of malicious assets.[9]

Understanding the origins of malicious assets is crucial for effective threat detection. These assets, including malware, propagate across various online platforms such as repositories, IRC channels, and hacker forums, where threat actors exchange information. By gaining insights into these sources and the content shared within them, organizations can identify potential threats and vulnerabilities, enabling proactive mitigation measures to be implemented promptly and efficiently.

In summary, the integration of Machine Learning (ML) methods, advanced visualization techniques, and trustworthy intelligence is essential for bolstering cybersecurity defenses and addressing emerging cyber threats effectively. ML facilitates swift threat detection by processing data efficiently, while advanced visualizations empower Threat Hunters to swiftly interpret security incidents accurately. Furthermore, ML aids in formulating hypotheses, assisting in gauging the seriousness of security events and predicting potential outcomes to proactively mitigate risks. Flexible system architectures that accommodate ML techniques ensure adaptable threat detection capabilities. Reliable intelligence furnished by Cyber Threat Intelligence (CTI) underpins proactive defense strategies, albeit challenges persist in data collection and analysis. Understanding the origins of malicious assets is crucial for effective threat detection, enabling organizations to promptly implement mitigation measures against evolving cyber threats.

IV. THREAT INTELLIGENCE FUSION AND ENRICHMENT

Threat Intelligence Fusion and Enrichment approaches attempt to improve the quality and depth of threat intelligence databases. Fusion refers to the combination of information from several sources, such as internal records, external feeds, and publically available sources, to promote a comprehensive understanding of possible dangers. This synthesis makes it easier to correlate different data pieces, revealing detailed patterns that might otherwise go unnoticed when single sources were examined separately.

In contrast, enrichment comprises improving existing threat intelligence by adding more context or features, resulting in a more complex picture of prospective dangers. This enrichment process may include metadata such as geographical information, threat actor profiles, or insights on linked vulnerabilities.In the provided content, the notion of blending and enhancing threat intelligence is discussed within the realm of Cyber Threat Intelligence (CTI). It stresses the significance of integrating, correlating, and enriching raw data from diverse sources to offer a more comprehensive understanding of potential threats. By merging data from various feeds and tools, organizations can develop a more holistic perspective of potential threats.

The significance of enhancing raw threat intelligence data with additional details like Indicators of Compromise (IoCs), tactics, techniques, and procedures (TTPs), along with contextual information. This process of enriching aims to increase the value and practicality of threat intelligence for decision-making within cybersecurity operations.

Through the combination of fusion and enrichment strategies, organizations can enhance their capacity to comprehend and address cybersecurity threats efficiently. This proactive approach to threat intelligence empowers organizations to anticipate potential threats, prioritize responses, and bolster their overall cybersecurity posture.[4]

In the cybersecurity field, combining Threat Intelligence Fusion and Enrichment is key to building strong defenses against changing cyber threats. Threat Intelligence Fusion involves carefully collecting data from different places like hacker forums and security articles to understand the current threat landscape better. By bringing together these various insights, organizations can spot emerging patterns and potential weaknesses more effectively.

Moreover, Threat Intelligence Enrichment adds more detail to the raw threat data, making it more useful. By adding extra information like details about threat actors, signs of compromise, and specific attack methods, organizations can get a deeper understanding of potential threats. This enriched intelligence helps cybersecurity teams make smarter decisions and take action to stop cyber attacks before they happen.[9]

Overall, integrating Threat Intelligence Fusion and Enrichment into cybersecurity strategies not only helps organizations strengthen their defenses but also encourages a proactive approach to dealing with threats. By combining data from different sources, spotting emerging trends, and improving detection capabilities, organizations can greatly improve their cybersecurity stance and better safeguard their assets against the ever-changing world of cyber threats.

V. THREAT INTELLIGENCE IN THE CLOUD AND IOT ERA

In today's digital world, cloud computing has become an essential component of many firms' IT infrastructure. As organizations increasingly rely on cloud services to store, analyze, and manage data, maintaining the security of these environments is critical. One of the key features of cloud security is the shared responsibility model, which defines the roles of cloud service providers and their clients. According to this approach, cloud service providers are responsible for safeguarding the underlying infrastructure, whilst customers are responsible for securing their data and applications on the cloud. Threat intelligence complements this shared responsibility approach by providing enterprises with actionable information into new threats and vulnerabilities unique to their cloud environments.Organizations may significantly improve their cloud security posture and minimize risks by employing threat intelligence.

Continuous monitoring is a cornerstone of effective cloud security practices. Given the dynamic nature of cyber threats, organizations must employ continuous monitoring tools and techniques to detect and respond to security incidents in real-time. Threat intelligence feeds are instrumental in this regard, enabling organizations to stay abreast of the latest threat landscape and identify potential security breaches proactively. Through continuous monitoring, organizations can bolster their security defenses, detect anomalies, and respond swiftly to emerging threats, thereby minimizing the impact of cyber attacks on their cloud environments.

With the proliferation of Internet of Things (IoT) devices, ranging from smart thermostats to industrial sensors, the IoT landscape has become increasingly interconnected and complex. This interconnected ecosystem introduces new cybersecurity challenges, as each IoT device represents a potential entry point for cyber attackers. Threat intelligence plays a pivotal role in addressing these challenges by providing organizations with valuable insights into IoT-specific threats and vulnerabilities. By analyzing threat intelligence data, organizations can identify potential risks associated with IoT devices, such as device hijacking, data breaches, and botnet attacks. Armed with this intelligence, organizations can implement robust security measures to protect their IoT devices and networks from cyber threats.

Behavioral analysis is a critical component of IoT security. By leveraging threat intelligence to analyze the behavior of IoT devices, organizations can detect anomalous activities indicative of a security breach. This proactive surveillance method allows enterprises to detect and respond to security problems in real time, reducing the effect of cyber assaults on their IoT infrastructure. Additionally, threat intelligence enables organizations to stay ahead of emerging IoT threats and adapt their security strategies accordingly, ensuring the continued integrity and resilience of their IoT networks.

The integration of threat intelligence into cloud and IoT security strategies is essential for developing a holistic approach to cybersecurity. By consolidating threat intelligence feeds from various sources, organizations can gain a comprehensive understanding of the threat landscape across their cloud and IoT environments. This integrated approach enables organizations to detect, analyze, and respond to cyber threats more effectively, thereby enhancing the overall security posture of their cloud and IoT infrastructure. Furthermore, by automating response mechanisms based on threat intelligence insights, organizations can streamline incident response processes and mitigate the impact of security incidents on their operations.[9]

Within the realm of cloud computing, the document emphasizes the critical role of threat intelligence in safeguarding data and applications hosted in cloud environments. With the proliferation of cloud services, organizations encounter novel security challenges, such as misconfigurations and unauthorized access. Here, AI-driven technologies emerge as pivotal tools, harnessing vast amounts of data to detect anomalies and predict potential risks. By integrating AI-powered analytics with threat intelligence platforms, organizations can bolster their ability to detect and respond to cloud-based threats in real-time.[10]

Moving on to the Internet of Things (IoT), the document highlights the unique threat landscape presented by interconnected devices. The diverse nature of IoT devices introduces a myriad of security vulnerabilities, necessitating robust threat intelligence measures. AI and ML technologies play a pivotal role in this domain as well, enabling organizations to analyze device behavior, detect anomalies, and identify potential security breaches. Moreover, in the IoT era, threat intelligence fusion and enrichment are essential for aggregating data from IoT devices and automating threat detection and response processes. AI-powered tools empower organizations to scale their IoT security efforts and effectively mitigate risks posed by IoT-specific threats.

While the benefits of threat intelligence in cloud and IoT security are undeniable, organizations also face significant challenges in managing threat intelligence at scale. The sheer volume of data generated by interconnected devices and cloud services can overwhelm organizations, making scalability a primary concern. However, this challenge also presents opportunities for organizations to leverage advanced analytics and machine learning algorithms to process threat intelligence data more efficiently. Additionally, collaboration between cloud service providers, IoT manufacturers, and cybersecurity experts is essential for sharing threat intelligence and best practices for securing cloud and IoT ecosystems. By working together, organizations can strengthen their defenses against evolving cyber threats and ensure the security and resilience of their cloud and IoT infrastructure.

VI. CONCLUSION

In summary, the evolution of threat intelligence and its utilization in cybersecurity, notably within the realms of cloud computing and the Internet of Things (IoT), underscores the fluid nature of contemporary digital threats and the necessity for proactive defense strategies. This study has extensively examined the historical development and current trends in threat intelligence, investigating how artificial intelligence (AI) and machine learning (ML) are transforming the landscape of threat detection and response.

AI and ML technologies have emerged as pivotal assets in augmenting the capabilities of threat intelligence, empowering organizations to preemptively identify and counter emerging threats with heightened accuracy and efficiency. Through the application of these advanced technologies, organizations can sift through vast volumes of data, identifying anomalies and foreseeing potential security risks in real-time, thus fortifying their cybersecurity stance.

Moreover, the amalgamation of various data sources and contextual insights, referred to as threat intelligence fusion and enrichment, enriches defense strategies by furnishing a comprehensive comprehension of potential threats. By amalgamating data from diverse origins and enhancing it with supplementary context, organizations can cultivate a more holistic understanding of potential threats, facilitating informed decision-making and proactive mitigation measures.

In the era of cloud computing and IoT, threat intelligence assumes a pivotal role in safeguarding data and applications hosted in cloud environments and securing interconnected IoT devices. The shared responsibility model in cloud environments accentuates the importance for organizations to harness threat intelligence to enhance security measures, identifying anomalies, and promptly responding to security incidents.

Additionally, the proliferation of IoT devices introduces a multifaceted threat landscape, necessitating robust threat intelligence measures and the integration of AI and ML technologies. Through the analysis of device behavior, detection of anomalies, and automation of threat detection and response processes, organizations can effectively mitigate risks posed by IoT-specific threats.

While the advantages of threat intelligence in cloud and IoT security are apparent, organizations encounter challenges in managing threat intelligence at scale. However, these challenges also offer opportunities for organizations to leverage advanced analytics, machine learning algorithms, and collaborative efforts among stakeholders to fortify their cybersecurity defenses and ensure the security and resilience of their digital assets amidst the evolving threat landscape.

In essence, the culmination of research findings and practical insights articulated in this study underscores the significance of threat intelligence in bolstering cybersecurity defenses and effectively addressing emerging cyber threats. Through the adoption of AI, ML, and advanced threat intelligence methodologies, organizations can remain proactive in outmaneuvering malicious actors, predicting potential threats, and safeguarding their digital assets in today's interconnected and dynamic cybersecurity environment.

VII. ACKNOWLEDGMENT

The authors would like to thank all members of the School of Computing who participated in this study.This study was carried out as part of the System and Network Security Project. This work was supported by Universiti UtaraMalaysia.

REFERENCES

[1]. W. I. B. W. Kamal, "Security Monitoring Tool System Using Threat Intelligence vs Threat Hunting," Journal of Universal Computer Science,, 2019.

[2]. FATIMAH ALDAUIJI, OMAR BATARFI and ANAL BAYOUSEF, "Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks:," A Survey of the State of the Art, vol. 10, 2022.

[3]. M. v. H. e. al., "A Shared Cyber Threat Intelligence Solution for SMEs," Electronics, vol. 10, no. 12, p. 21, 2021.

[4]. P. Khordadpour, "Toward Efficient Protecting Cyber-Physical Systems with Cyber Threat Hunting and Intelligence," IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 3, pp. 1-10, 2020.

[5]. D. e. a. Javeed, "An Efficient Approach of Threat Hunting," International Journal of Computer Networks and Communications Security, vol. 8, no. 5, pp. 38-29, 2020.

[6]. M. A. Lozano, "Threat Hunting Architecture Using a Machine Learning Approach for Critical Infrastructures Protection," Big Data Cogn. Comput, vol. 7, p. 65, 2023.

[7]. D. J. e. al., "An Efficient Approach of Threat Hunting Using Memory Forensics," International Journal of Computer Networks and Communications Security, vol. 8, no. 5, pp. 37-45, 2020.

[8]. A. &. I. Y. Durai Raju, "A Survey on Cross-Architectural IoT Malware Threat Hunting," IEEE Access, vol. 9, pp. 91694-91705, 2020.

[9]. F. B. O. &. B. M. Aldauiji, "Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art," IEEE, vol. 10, 2020.

[10]. H. Azam et al., "Innovations in Security: A study of cloud Computing and IoT," International Journal of Emerging Multidisciplinary Computer Science & Artificial Intelligence, 2023.

[11]. Sarah Brown et al., From Cyber Security Information Sharing to Threat Management, pp. 43-49.

[12]. P. Z. a. Y. E. R. Puzis, "ATHAFI: Agile Threat Hunting And Forensic Investigation," 2020.

[13]. J. A. A. &. S. R. Kotsias, "Adopting and integrating cyber-threat intelligence in a commercial organisation," European Journal of Information Systems, vol. 32, no. 1, pp. 35-51, 2023.

[14]. B. E. R. G. a. V. N. V. S. M. Milajerdi, "Poirot: Aligning Attack Behavior with Kernel Audit Records for Cyber Threat Hunting," 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), pp. 1-18, 2019.

[15]. M. A. S. C. M. M. N. A. a. S. u. I. A. B. Ajmal, "Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation," IEEE Access, vol. 9, pp. 116746-116756, 2021.

[16]. M. D. G. P. K. a. K. A. Z. E. W. Burger, "Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies," Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, pp. 51-60, 2022.

[17]. K. K. ,. A. A. ,. A. A. Akashdeep Bhardwaj, "BTH: Behavior-Based Structured Threat Hunting Framework to," Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence, vol. 12, p. 1205, 2022.

[18]. Potter, Kaledio & Oloyede, Joy & f, olaoye. (2024). Securing the Internet of Things (IoT) Ecosystem: Challenges and Solutions in Cybersecurity. Journal on Internet of Things.

[19]. Deep learning for cyber threat detection in IoT networks: A review. (2023). Internet of Things and Cyber-Physical Systems, 110–128. https://doi.org/10.1016/j.iotcps.2023.09.003

[20]. Bai, Ming & Fang, Xiang & Khan, Muskan. (2024). Machine Learning-Based Threat Intelligence for Proactive Network Security.