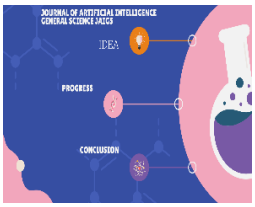
Vol.5 Issue 01 June, 2024
Journal of Artificial Intelligence General Science JAIGS

Home page https://ojs.boulibrary.com/index.php/JAIGS



The Effectiveness of Cyber Threat Intelligence in Improving Security Operations

Joshua Smallman

Anglia Ruskin University

ARTICLEINFO
Article History:
Received:
01.06.2024
Accepted:
30.06.2024
Online: 09.07.2024
Keyword:Cybersecurity, Cyber Threat Intelligence, Effective Security Operations, CTI Adoption Barriers

ABSTRACT

The purpose of this research was to comprehensively evaluate the effectiveness of Cyber Threat Intelligence (CTI) in enhancing security operations, while simultaneously identifying the various barriers to its adoption. Additionally, the study aimed to provide potential solutions to mitigate the identified barriers, to ensure successful adoption of CTI.A systematic review was undertaken to identify the main factors of enhanced security operations. Relevant questions and statements were then developed from these factors and a questionnaire was created using Google Forms. These questionnaires were then distributed via email to a sample size of 50 information technology professionals. These results were then analyzed using Microsoft Excel and SPSS. Overall, the research revealed that companies who used CTI reported significant gains in threat detection and response, risk management and threat-hunting abilities, which in turn lead to enhanced security operations. According to the research, several factors prevented organizations from adopting CTI. Among these were technological, regulatory, ignorance-related, and lack of executive support. Finally, to tackle these identified barriers the following were proposed adopting comprehensive awareness and education programs, the formation of an Executive CTI Steering Committees, structured CTI training and skills development programs, technology assessment and modernization initiative-based initiatives, proactive compliance, and legal strategies.

Introduction

This research paper investigates the effectiveness of using Cyber Threat Intelligence (CTI) to enhance security operations amid the increasing prevalence of cybersecurity breaches. Security professionals continuously seek effective strategies to combat and mitigate cyber-attacks. CTI, defined by Tounsi and Rais (2018) as the process of collecting, analyzing, and disseminating information about emerging cyber threats to support defensive measures and decision-making, plays a crucial role in addressing cyber breaches. Similarly, Scarfone, Souppaya, and Masone (2013) describe CTI as knowledge derived from data analysis about cyber threats to inform response decisions. Abu et al. (2018) further explain CTI as gathering and examining data on cyber threats and vulnerabilities to understand threat actors' methods and provide measures to prevent or reduce attack impacts. This study defines CTI as the process of gathering and analyzing cyber threat data to devise mitigation strategies. Security operations, involving activities and processes to detect, respond to, and mitigate cybersecurity threats, vary by organization size, from single-person operations in startups to large teams in enterprises (Yazdinejad et al., 2022). This study aims to assess how CTI can improve security operations within organizations.This study sets out to investigate the effectiveness of using Cyber Threat Intelligence to improve Security Operations in organizations.

This first chapter seeks to discuss the following:

- What is CTI (Cyber Threat Intelligence.
- The issues that CTI seeks to address.
- The Rationale of using Cyber Threat Intelligence to improve Security Operations in organizations.

1.1 Issue

The ever-increasing cybersecurity threats pose significant challenges for organizations to secure their assets and data. According to the Identity Theft Resource Centre (2021) cyber-attacks and security breaches have been on the rise, there were 1,632 data breaches in the United States in 2021, exposing over 555 million records. This represents a 21% increase in the number of breaches and a 300% increase in the number of records exposed compared to 2020.

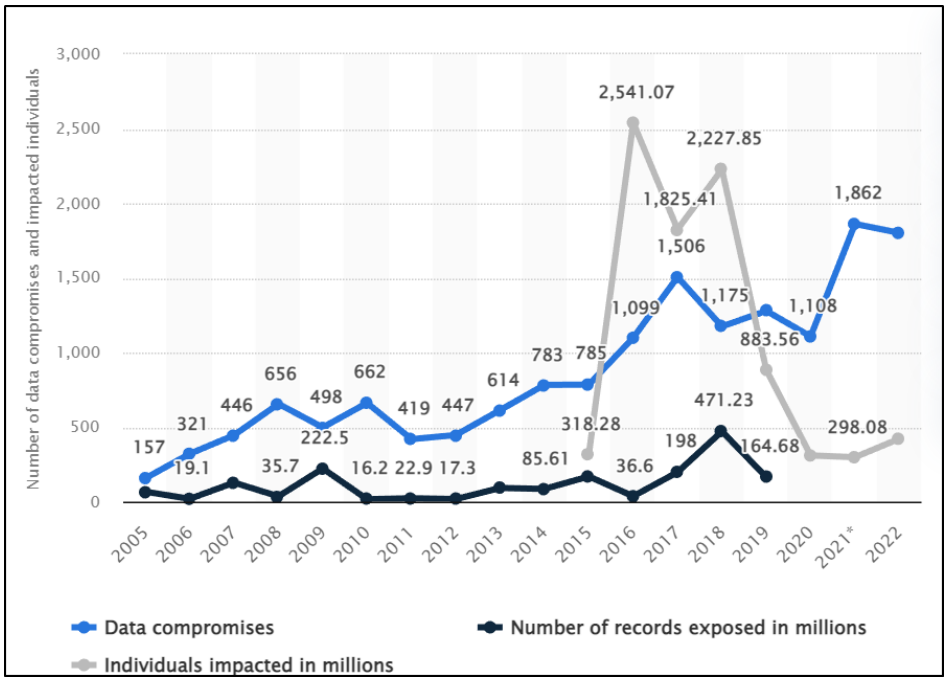


Figure 1 - Cybersecurity data breaches (Identity Theft Resource Centre, 2021).

According to the "2020 Cybersecurity Almanac" published by Cybersecurity Ventures; it is estimated that a cyberattack occurs every 11 seconds globally. This statistic considers various types of cyber incidents, including malware infections, ransomware attacks, data breaches, and phishing attempts. The frequency of cyberattacks highlights the constant and evolving threat landscape that organizations and individuals face in the digital age (Cybersecurity Ventures, 2020).

Figure 2 - 2020 Cybersecurity Almanac published by Cybersecurity Ventures

Cyber breaches are also very costly the "Cost of a Data Breach Report 2021," conducted by IBM Security and the Ponemon Institute, provides valuable insights into the financial impact of cyber breaches on organizations in 2021. According to the report, the average cost of a data breach in 2021 was $4.24 million per incident, representing a 10% increase compared to the previous year.

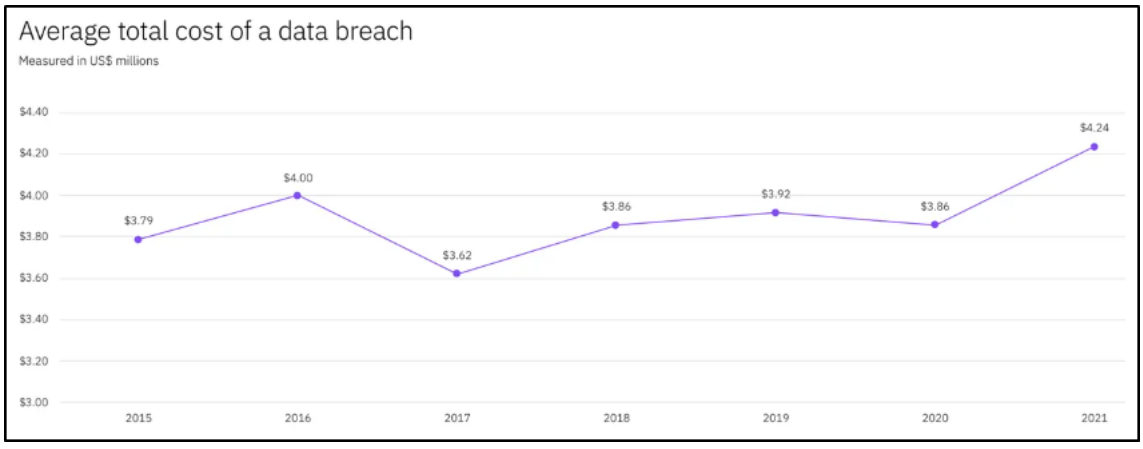


Figure 3 - Average cost of a data breach (IBM, 2021)

This statistic highlights the significant financial implications that organizations face when dealing with a cyber breach. The cost of a data breach includes various factors, such as remediation efforts, investigation, legal fees, customer notification, and potential loss of business. Additionally, indirect costs, such as reputational damage and the long-term impact on customer trust, can further contribute to the overall financial burden.

1.2 Rationale

While there is some evidence to suggest that CTI may be able to improve security operations, a systematic understanding of how CTI contributes to improved security operations is still lacking. According to Abu et al. (2018), CTI adoption is still in early state and the needs for research and development is required to fully utilize its potential.

If it is shown that CTI can significantly improve security operations, thereby reducing cyber threats. This information can greatly benefit most organisations as it would provide them with an option to reduce and mitigate cyber breaches. The benefits to organisations would include data protection, good public image, cost savings etc.

The purpose of this research is to undertake a systematic review of the data that is currently available, to better understand the corelation between CTI and security operations.

1.3 Research Question

How effective is CTI in improving security operations, and what are the barriers for its adoption?

1.4 Research Aim

The aim of this research is to comprehensively evaluate the effectiveness of Cyber Threat Intelligence (CTI) in enhancing security operations, while simultaneously identifying the various barriers to its adoption. Additionally, the study aims to provide potential solutions to mitigate the identified barriers, to ensure successful adoption of CTI.

1.5 Research Objectives

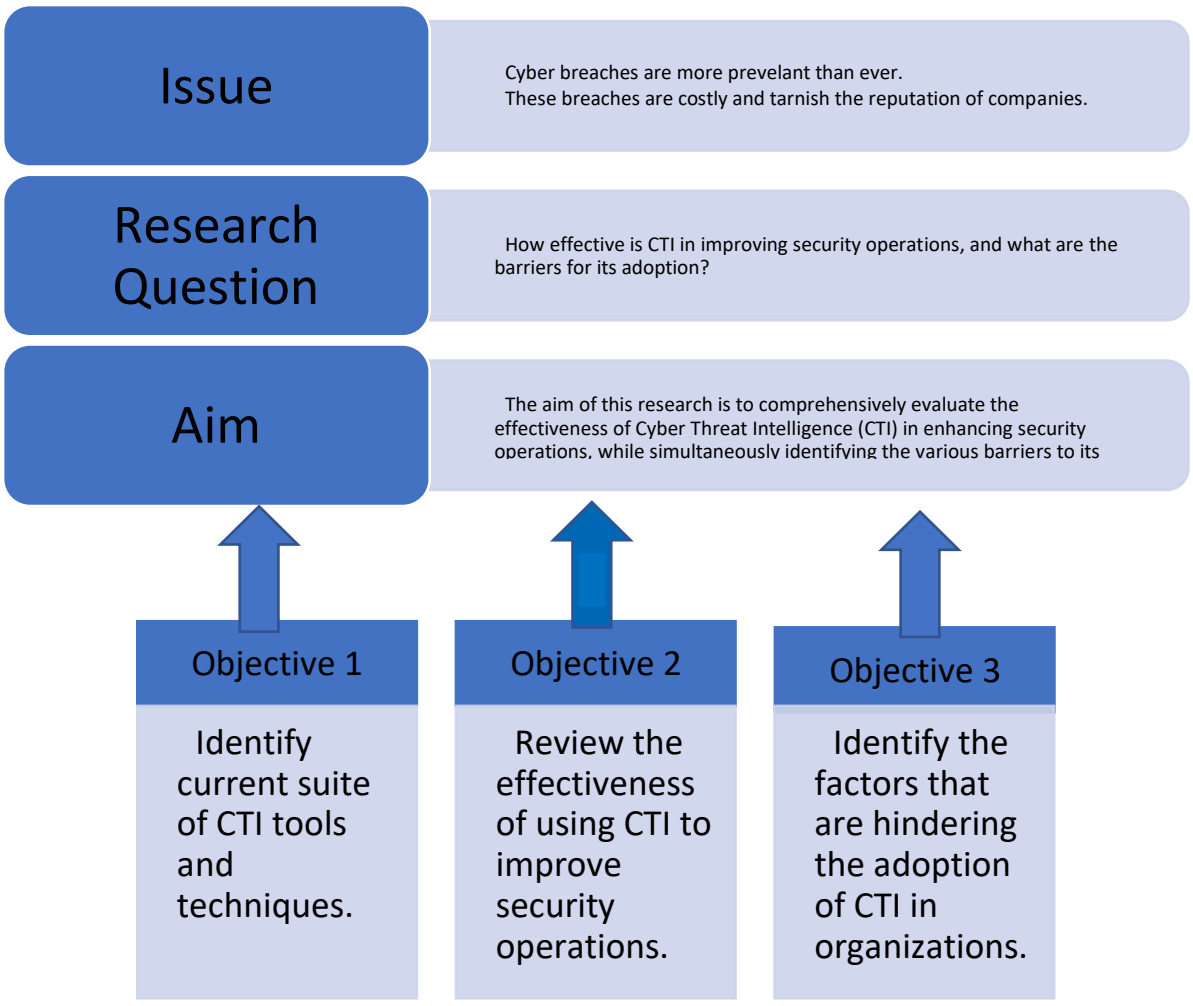
The research objectives are as follows:

1. Identify current suite of CTI tools and techniques.
2. Review the effectiveness of using CTI to improve security operations.
3. Identify the factors that are hindering the adoption of CTI in organizations.

1.6 Research Framework

In the technology driven world that we currently live in, cyber breaches are now more prevalent than ever. Besides the financial losses these cyber breaches also cost companies their reputation as well as competitive edge. Due to this companies are always looking for better address these breaches. There is some research to suggest that using Cyber Threat Intelligence can be a great tool for improving security operations and thereby reducing these breaches. However, research on this topic is still lacking. The purpose of this study is to do a systematic review of the currently available data, to examine if CTI is indeed an effective way of improving security operations in organizations.

The following framework would be used in this study:



1.7 Dissertation Structure

The following chapters addressed the researched objectives as defined above. In order to achieve these objectives and answer the research question, the researcher embarked upon the following:

- Literature Review – The literature review examines the effectiveness of Cyber Threat Intelligence in improving security operations. It also examines the barriers to adoption.
- Research Methodology – The honeycomb methodology was used. We examined existing studies and created a questionnaire based on this. This questionnaire was then distributed to IT professionals of which the results were analyzed.
- Findings and Analysis – The findings revealed that CTI was very effectiveness in improving security operations. Barriers such as lack of awareness, technical expertise, lack of executive support, were also identified.
- Conclusion – This research proved insightful as it provided a holistic view of the effectiveness of CTI as opposed to previous research which focused on specific niches. It is recommended that more research be conducted on this topic, using different methodologies such as experimentation.

Literature Review

2.1 Identify current suite of CTI tools and techniques.

Cyber threat intelligence (CTI) plays a crucial role in modern cybersecurity practices by providing organizations with actionable insights into potential threats and enabling proactive defense strategies. This section examines various tools and techniques used in cyber threat intelligence, focusing on their capabilities, benefits, and limitations. By exploring these tools and techniques, organizations can enhance their understanding of the cyber threat landscape and bolster their cybersecurity defenses.

CTI tools

Malware analysis tools facilitate the identification, classification, and analysis of malicious software, helping organizations understand their behavior and impact (Jones, 2019). Tools like VirusTotal offer online platforms for analyzing suspicious files and URLs, providing insights into malware and potential threats (VirusTotal, n.d.). These tools were crucial in dissecting the WannaCry ransomware code in 2017, revealing vulnerabilities and enabling the development of countermeasures (Chen et al., 2017). However, their precision can be resource-intensive and require expertise (Rascagneres et al., 2017). In contrast, Threat Intelligence Platforms (TIPs), such as IBM X-Force Exchange, aggregate and analyze threat data from various sources, supporting informed decisions and automated responses (Ucci, Aniello, & Baldoni, 2019; IBM Security, n.d.). TIPs were instrumental in mitigating the NotPetya ransomware attack in 2017 by providing a comprehensive view of the threat landscape (Maggi et al., 2018). However, they can be complex and costly to implement (Abawajy&Alazab, 2018). OSINT tools, like TheHarvester, gather information from public sources to provide insights into external threats, although they may miss sophisticated or non-public threats (Brown, 2018; TheHarvester, n.d.). Each CTI tool has its strengths: malware analysis tools offer precision, TIPs provide comprehensive threat data aggregation, and OSINT tools monitor external threats. A holistic cybersecurity strategy combines these tools to form a robust CTI ecosystem, enhancing organizational resilience against cyber threats.

CTI techniques

According to Johnson (2017), Indicator-Based Analysis (IBA) identifies and analyzes indicators of compromise (IOCs) such as IP addresses and file hashes to detect known threats, with Snort being a popular example of an intrusion detection system utilizing IOCs and signature-based detection (Snort, n.d.). IBA is effective in identifying threats with known patterns, using IOCs from threat intelligence feeds to detect and block malicious activity in real-time (Liao et al., 2015). However, it is reactive and ineffective against novel threats (Green, 2016). Behavioral Analysis, on the other hand, monitors and analyzes system behavior to detect anomalies and deviations from expected patterns, identifying threats without known signatures. SIEM systems like Splunk use behavioral analysis to identify insider threats and abnormal user activities (Splunk, n.d.; Jiang et al., 2019). Despite its strengths, Behavioral Analysis can produce false positives and requires significant computational resources. Threat Hunting, according to Anderson (2019), involves proactive searches for potential threats using hypotheses and human expertise, valuable for identifying advanced persistent threats (APTs) (Lassalle et al., 2018). However, it is time-

consuming and relies heavily on human skills. In conclusion, organizations should choose a CTI technique based on their threat landscape, resources, and objectives. A unified CTI strategy combining IBA, Behavioral Analysis, and Threat Hunting can dynamically defend against diverse cyber threats by leveraging the strengths of each technique.

2.2 Review the effectiveness of using CTI.

Enhancing Threat Detection and Response

According to Sedjelmaci et al. (2017) several studies have shown that integrating CTI into security operations improves threat detection and response capabilities. Deliu et al. (2018) created their own CTI algorithm using a mixture of Support Vector Machines, Topic modeling and Latent Dirichlet Allocation algorithms. The researchers accessed and conducted experiments on hacker forum data from Nulled.IO, whose raw database had already been compromised. 90% of the postings were determined to be security-irrelevant by the study using SVM filtering and topic modeling. However, the other 10% revealed numerous cyberthreats. Leaked credentials and top-level domains of compromised accounts were among the information regarding numerous cyber-threats that were revealed in the extracted subjects. Figure 4 shows that this CTI method extracted relevant, timely and actionable security related information within minutes.

Data Set Processed	**# of topics estimated**	**Time Elapsed** (minutes)
Experiment Test Data (All words)	10	238.68
Security Relevant (All words)	10	16.76
Experiment Test Data (50,000 words)	10	71.54
Security Relevant (50,000 words)	10	6.41
Experiment Test Data (All words)	25	565.16
Security Relevant (All words)	25	38.55
Experiment Test Data (50,000 words)	25	152.91
Security Relevant (50,000 words)	25	13.72

Figure 4 - Time Performance Tests (courtesy 2018, IEEE)

Similar experiments were also conducted using the traditional method of a security professional manually analyzing the data. In contrast, to the CTI experiments, which identified threats within minutes, the manual experiments took days to identify the same threats.

Elasticsearch has become a key element of SIEM systems, making it easier to collect, store, and analyze huge amounts of security-related data. Elasticsearch's real-time indexing and querying capabilities are used to correlate security events and produce alerts, according to Salonen et al. (2018). Elasticsearch has been used by researchers to examine logs produced by a variety of devices, such as firewalls, intrusion detection systems (IDS), and endpoints. For their experiment, Almohannadi et al. (2018) used two honeypots dubbed Kippo and Dionea that mimic genuine operating systems and gathered more than 500MB of log data over the course of more than a year through an Amazon Web Services (AWS) cloud. To show data, build visualizations, and a dashboard for any scale of data, they employed Elasticsearch. Figure 5 illustrates the experiment setup.

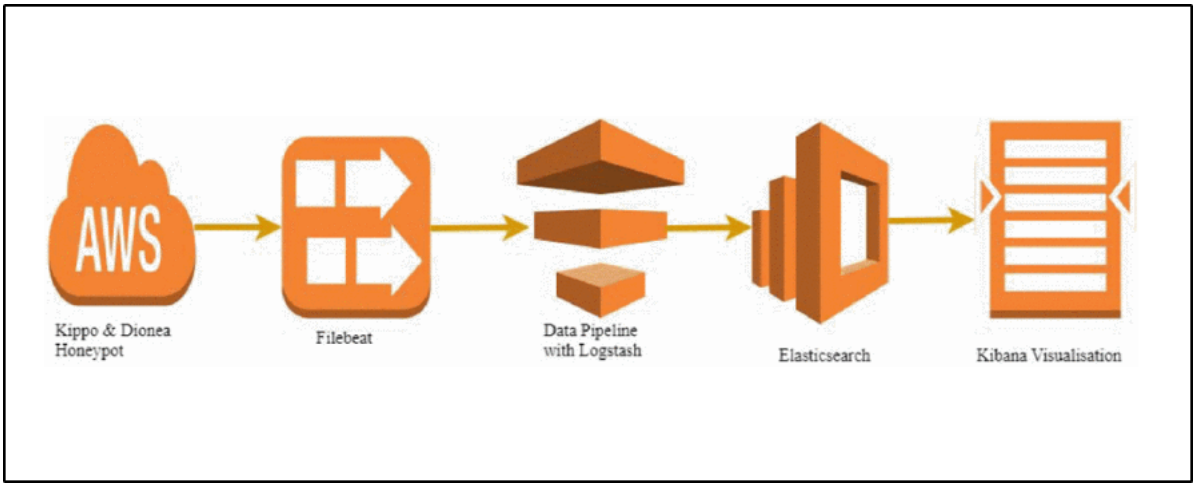


Figure 5 - Elasticsearch experiment setup (courtesy Almohannadi et al.2018)

By analysing the log data, numerous different types of attacks were found. All of the keywords that were discovered during the examination of the honeypot data are components that would be very useful in a threat detection and response. Figure 6 shows the results of the Elasticsearch analysis.

Event Name	No of time occurred	% of occurring
login attempt	1, 889, 046	11.6%
root trying auth none	3, 839, 723	23.57%
root failed auth password	3, 172, 791	19.48%
root trying auth password	3, 172, 791	18.91%
unauthorised login	1, 889, 046	11.6%
got remote error	726, 436	4.46%
got channel direct-tcpip request	351, 466	2.16%
connection lost	1, 342, 279	8.24%

Figure 6 - Elasticsearch analysis results (courtesy Almohannadi et al.2018)

Despite its benefits, Elasticsearch poses cybersecurity challenges, especially in multi-tenant environments requiring rigorous access control and encryption (Rădulescu et al., 2019). Scalability and optimizing queries to reduce false positives and enhance threat detection remain concerns (Wagner et al., 2020). CTI positively impacts threat detection; Egele et al. (2008) highlight its role in detecting APTs through global threat data. A financial institution's integration of CTI into its IDS thwarted a malware attack (Chen et al., 2019), and Rodriguez et al. (2020) describe how CTI aids in developing response playbooks. A retail company used CTI effectively against a ransomware attack (Sullivan, 2018). However, CTI can overwhelm security teams with alerts (Roberts, 2017) and its timeliness is questioned due to rapidly adapting threats (Carr, 2016). Integration challenges and relevance issues also arise (Thomas, 2019; Donovan, 2020). CTI enhances threat detection and response, but alert overload, timeliness, and integration complexities must be addressed. Organizations should evaluate their needs and capabilities to maximize CTI's cybersecurity benefits.

Improved Risk Management

TI plays a crucial role in risk management by providing timely and accurate information about emerging threats and vulnerabilities. Krombholz et al. (2019) conducted a quantitative study, analyzing data from organizations using CTI, and found that those leveraging CTI were better at identifying risks, prioritizing mitigation efforts, and allocating resources effectively. Similarly, Aljuhami&Bamasoud (2021) examined the effects of CTI on risk management in Saudi universities and concluded that using cyber threat data improves the ability to counteract evolving threats. They also noted the need for stronger cybercrime laws and a national cybersecurity strategy in Saudi Arabia (Alshammari et al., 2018). Kure et al. (2019) proposed the Integrated Cyber Security Risk Management (i-CSRM) framework to address challenges in a rapidly changing threat landscape. The framework, which includes critical asset identification, risk prediction through machine learning, and control effectiveness assessment, was tested in Nigeria's DisCos electricity company. Following a 2-week blackout due to a remote access incident, DisCos used the i-CSRM framework to improve service continuity and sustainability, demonstrating the framework's applicability and effectiveness.

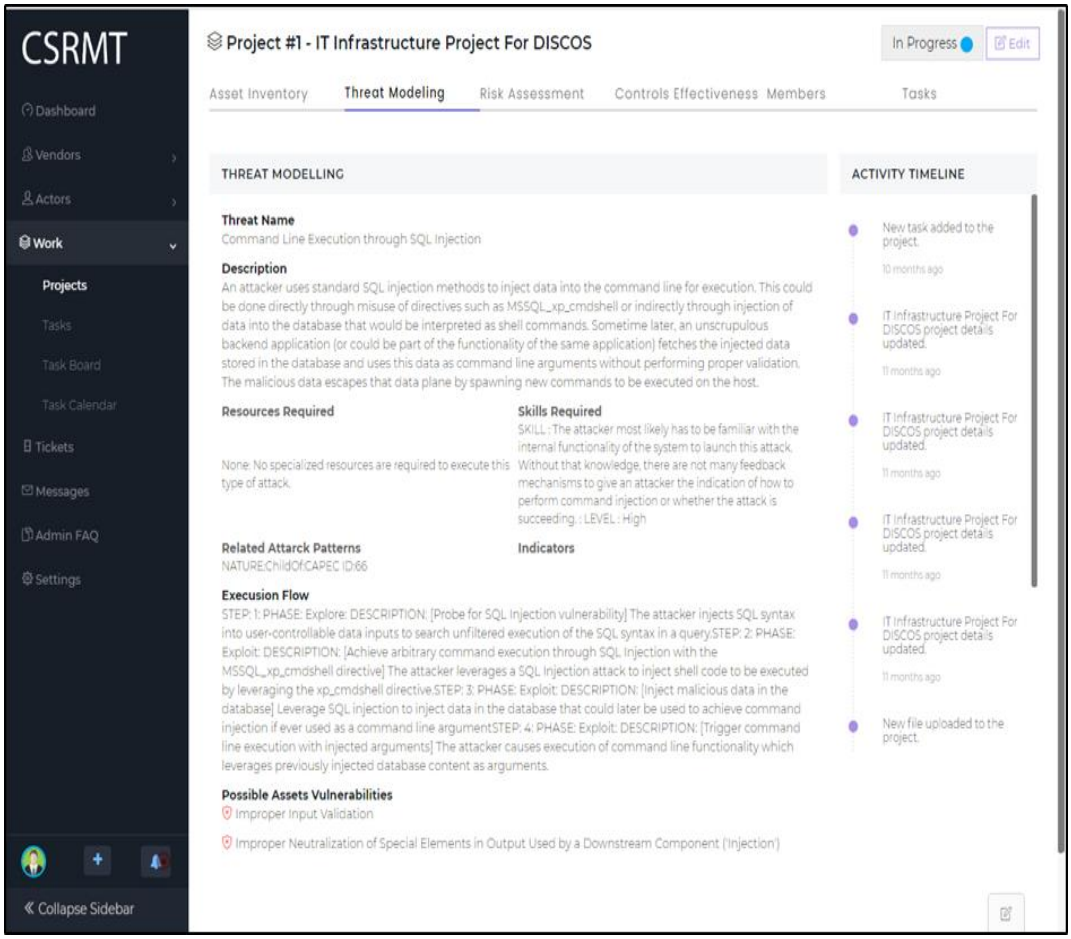


Figure 8 - Threat and vulnerability profile (courtesy Kure et al. 2019)

The participants concluded that the i-CSRM framework provides a thorough and holistic risk analysis based on assets, threats, and vulnerabilities, making it an effective strategy for managing risks in critical infrastructure. This framework, which integrates current standards with machine learning algorithms, aids stakeholders in understanding and managing potential risks. The case study highlighted the need for an all-inclusive risk management system by

comparing its findings with other studies. Several studies emphasize that Cyber Threat Intelligence (CTI) enhances risk assessments by providing up-to-date threat intelligence, allowing organizations to prioritize risk mitigation efforts effectively (Liao et al., 2019). Timely threat intelligence supports informed decision-making in risk management by assessing threat severity and allocating resources appropriately (Campbell & Sample, 2018). However, challenges include potential data overload, where organizations struggle to manage and extract actionable insights from vast CTI data (Gordon et al., 2015), and the contextual gap, where CTI may lack relevance for specific organizations (Koblitz et al., 2017). Effective CTI utilization also demands significant resources, which can be challenging for smaller organizations (Mitre Corporation, 2020). Despite these concerns, the consensus is that CTI enhances risk management through early threat detection, informed decision-making, and proactive risk mitigation, making it a valuable asset for organizations.

EnhancedThreat Hunting

The WannaCry ransomware, which emerged in May 2017, infected systems worldwide and demanded a ransom in Bitcoin for a decryption key (Herwig, 2018). Threat hunters collected Cyber Threat Intelligence (CTI) from various sources, focusing on identifying indicators of compromise (IOCs) linked to WannaCry, such as file hashes and IP addresses (Dorais-Joncas &Grees, 2017). They used controlled environments and behavioral analysis tools to uncover the malware's patterns (McMillan, 2017) and formulated incident response strategies to mitigate its impact (Hosseini et al., 2016), leading to early detection and attribution to North Korea (Thomas, 2017). Similarly, CTI was pivotal in exposing the Russian APT29, also known as Cozy Bear, by gathering extensive information on their tactics, techniques, and procedures (Gao et al., 2021; CrowdStrike, 2020). Proactive threat hunting missions based on this intelligence uncovered APT29's advanced malware and lateral movement (Doe, 2020). Despite CTI's benefits, overreliance can lead to false positives and overwhelm threat hunters (Milajerdi et al., 2019; Thomas, 2017), and smaller organizations may lack necessary resources (Dorais-Joncas &Grees, 2017). In conclusion, while CTI enhances threat hunting, a balanced approach is essential to avoid false positives, data overload, and resource constraints, ensuring effective protection against evolving threats.

2.3 Identify the factors that are hindering the adoption of CTI in organizations.

Despite the potential benefits of CTI adoption, several factors may hinder its adoption in organizations.

Lack of awareness: One factor that can hinder the adoption of CTI in organizations is the lack of awareness and understanding of CTI. A study by the Ponemon Institute (2019) sheds light on this issue, revealing that a significant portion of cybersecurity professionals remains uninformed about CTI or lacks a comprehensive understanding of its potential benefits. The research findings indicate that merely 26% of the surveyed professionals demonstrated familiarity with CTI. More concerningly, only 13% of the respondents reported having implemented CTI practices within their respective organizations. According to Kott et al. (2019) this lack of awareness and limited integration of CTI may be attributed to several factors. First, the rapidly evolving nature of the cybersecurity landscape makes it

challenging for professionals to stay updated with new concepts and technologies like CTI. Second, the terminology and concepts associated with CTI can be complex and technical, potentially discouraging professionals who are not directly involved in threat intelligence. Thirdly, budgetary constraints and resource limitations can also hinder the adoption of CTI. Implementing CTI effectively often requires dedicated tools, technologies, and skilled personnel, which may not be readily available to all organizations.

Organizational Factors: Organizational factors play a significant role in hindering the adoption of CTI. One of the primary factors is the lack of executive sponsorship and support, which has been identified as a major barrier (Gong, 2019). Without the backing of top management, CTI initiatives may struggle to secure the necessary resources and support for successful implementation. Additionally, organizational culture and resistance to change can impede CTI adoption (Risling, 2019). In some cases, organizational silos and communication gaps between different departments hinder the sharing and utilization of CTI across the organization (Powers et al., 2021). Overcoming these challenges requires a holistic approach that involves leadership commitment, cultural transformation, and cross-functional collaboration.

Lack of Expertise: According to Zibak& Simpson (2019) expertise is crucial because CTI involves complex processes such as data collection, analysis, interpretation, and timely response to emerging threats. He further explains that understanding the nuances of specific malware families or advanced persistent threats (APTs) is crucial for effective CTI analysis (Jones, 2019). To address the lack of technical expertise, researchers such as Alves et al. (2016) and Das and Yelure (2019) propose a structured CTI training and skills development program. This program includes technical training modules, certifications, and mentorship initiatives to empower the workforce with the necessary expertise for effective CTI adoption.

Technological Factors: Technological factors also contribute to the challenges in CTI adoption. Integration complexities arise due to the heterogeneity of existing security systems and tools within organizations (Aljohani et al., 2019). Lack of interoperability between CTI platforms and existing security infrastructure can hamper the effective sharing and utilization of intelligence. Organizations need to invest in technologies that facilitate seamless integration and data exchange between different security solutions. Furthermore, the scarcity of skilled cybersecurity personnel poses a significant challenge (Nakashima et al., 2022). Organizations often struggle to find and retain professionals with the necessary expertise to effectively leverage CTI. To address this, investments in training and development programs, as well as collaboration with educational institutions, are essential.

Operational Factors: Operational factors can impede CTI adoption by affecting its integration into existing operational workflows. The lack of standardized processes for CTI utilization hinders its effective incorporation into security operations (Grue et al., 2020). Organizations should establish standardized procedures and frameworks that enable the seamless integration of CTI into incident response, threat hunting, and vulnerability management processes. Furthermore, limited access to high-quality and timely CTI data sources poses challenges in obtaining accurate and actionable intelligence (Cariño et al., 2021). Organizations should foster collaborations with trusted

CTI providers, industry peers, and government agencies to enhance their access to diverse and reliable sources of intelligence. Moreover, the dynamic nature of cyber threats requires continuous monitoring and updating of CTI, which can strain resources and hinder its adoption. Automation and orchestration tools can help organizations streamline these processes and ensure the timely delivery of actionable intelligence.

Regulatory Factors: Finally, regulatory, and legal factors can also hinder the adoption of CTI in organizations. CTI involves the collection and analysis of sensitive data, and organizations must comply with data privacy and security regulations when implementing CTI. Additionally, legal issues related to the sharing of CTI among organizations can pose significant challenges to effective CTI adoption (Menges, Sperl, &Pernul, 2019).

Conclusion: The adoption of CTI in organizations is hindered by various factors, including organizational, technological, and operational challenges. Addressing these barriers is crucial to fully realize the potential benefits of CTI in enhancing cybersecurity posture. To overcome these hindrances, organizations need to prioritize executive sponsorship, foster a culture of collaboration and information sharing, address technological integration issues, invest in skill development, establish standardized processes, and ensure access to high-quality CTI data sources. By recognizing and addressing these factors, organizations can enhance their ability to effectively adopt and utilize CTI in their cybersecurity strategies.

2.4 Conceptual Framework

To achieve the research objectives and aim of answering the research question, the conceptual framework illustrated in **Figure 14** shows the necessary steps:

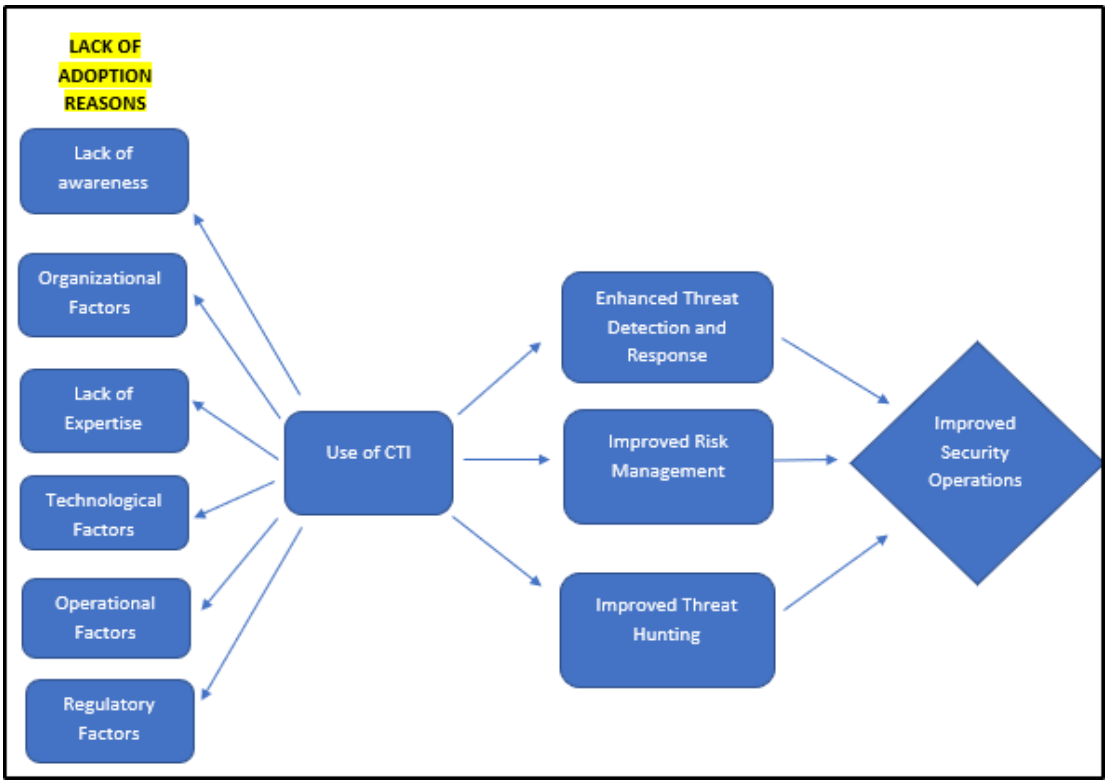


Figure 16 - Conceptual Framework (courtesy Smallman 2023)

References

- Abawajy, J. H., &Alazab, M. (2018). Cyber Threat Intelligence Sharing: Survey and Research Directions. Computers & Security, 78, 398-416.
- Abu, M.S., Selamat, S.R., Ariffin, A. and Yusof, R., 2018. Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), pp.371-379.
- Annual Data Breach Report. (n.d.). ITRC. https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/
- Aldawood, A., Alazab, M., & Venkatraman, S. (2021). Cyber threat intelligence sharing: A review of best practices and recommendations. Computers & Security, 104, 102216.
- Aljuhami, A. M., &Bamasoud, D. M. (2021, April 4). Cyber Threat Intelligence in Risk Management. Cyber Threat Intelligence in Risk Management. https://doi.org/10.14569/IJACSA.2021.0121018
- Alqahtani, S., Alsaqer, H., &Albakr, S. (2021). An intelligent system for cyber threat intelligence sharing. Computers & Security, 108, 102290.
- Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. Archives of Business Research, 6(12).
- Babbie, E. R. (2016). The practice of social research. Cengage Learning.
- Bahnsen, A. C., Castillo, C. D., Staudemeyer, R. C., & de Bem, R. M. (2021). Cyber threat intelligence for intrusion detection using machine learning. Computers & Security, 107, 102307.
- Beechey, M., Kyriakopoulos, K.G. and Lambotharan, S., 2021. Evidential classification and feature selection for cyber-threat hunting. Knowledge-Based Systems, 226, p.107120.
- Bhardwaj, A. and Goundar, S., 2019. A framework for effective threat hunting. Network Security, 2019(6), pp.15-19.
- Bryman, A. (2016). Social research methods. Oxford University Press.
- Burrell, G., & Morgan, G. (1979). Sociological paradigms and organizational analysis: Elements of the sociology of corporate life. Routledge.
- Chang, T., Huang, M., & Chen, Y. (2019). Cyber threat intelligence analysis through machine learning for SMEs. Journal of Information Security and Applications, 50, 197-210.
- Cisco. (2021). Cisco Threat Intelligence. Retrieved from https://www.cisco.com/c/en/us/products/security/threat-intelligence.html
- Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approach. Sage publications.
- Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research. Sage Publications.

- Crotty, M. (1998). The Foundations of Social Research: Meaning and Perspective in the Research Process. SAGE Publications.
- CrowdStrike. (2021). Threat Intelligence. Retrieved from https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
- Cybersecurity Ventures. (2020). 2020 Cybersecurity Almanac. Retrieved from https://cybersecurityventures.com/cybersecurity-almanac-2020/
- Dacier, M. (2018). Cyber Threat Intelligence: When Machine Learning Meets Human Intelligence. Journal of Cybersecurity, 4(1), 1–12.
- Daniel, P.S. and Sam, A.G., 2011. Research methodology. Gyan Publishing House.
- Daly, J. (2018). Cyber threat intelligence sharing: Exploring the challenges and opportunities. Journal of Cybersecurity, 4(1), 1-12.
- Deliu, C. Leichter and K. Franke, "Collecting Cyber Threat Intelligence from Hacker Forums via a Two-Stage, Hybrid Process using Support Vector Machines and Latent Dirichlet Allocation," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 5008-5013, doi: 10.1109/BigData.2018.8622469.
- Denzin, N. K., & Lincoln, Y. S. (2017). The Sage handbook of qualitative research. Sage publications.
- DeWalt, J. & Wheeler, D. (2015). Threat intelligence: Collecting, analyzing, and sharing information. Elsevier.
- Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). Internet, phone, mail, and mixed-mode surveys: The tailored design method. John Wiley & Sons.
- Doherty, B., & Deeks, D. (2018). Cyber Threat Intelligence: Challenges and Opportunities. Journal of Information Warfare, 17(1), 21-36.
- Dacier, M., et al. (2015). Threat Intelligence From Heterogeneous Data Sources. In 2015 International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS).
- Dressler, F., et al. (2017). Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. IEEE Access, 5, 20227-20252.
- E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, et al., "Darknet and deepnet mining for proactive cybersecurity threat intelligence", 2016 IEEE Conference on Intelligence and Security Informatics (ISI). Institute of Electrical and Electronics Engineers (IEEE), pp. 7-12, Sept 2016.
- Ficco, M., et al. (2018). Big Data Analytics for Cyber-Physical-Social Systems: A Survey. IEEE Access, 6, 35315-35336.
- Galliers, R. D. (1991). Choosing information systems research approaches. In J. I. DeGross, C. K. Kemerer, & S. S. Lyytinen (Eds.), Information Systems Research: Contemporary Approaches and Emergent Traditions (pp. 69-92). Elsevier Science Publishers B.V.
- Das, S., &Yelure, B. (2019). Challenges in Cyber Threat Intelligence Sharing Mechanism: A Comprehensive Review. Journal of Network and Computer Applications, 127, 26-48.

- Egele, M., Scholte, T., Kirda, E. and Kruegel, C., 2008. A survey on automated dynamic malware-analysis techniques and tools. ACM computing surveys (CSUR), 44(2), pp.1-42.
- Google. (2021). Google Forms. Retrieved from https://www.google.com/forms/about/
- Gao, P., Shao, F., Liu, X., Xiao, X., Qin, Z., Xu, F., Mittal, P., Kulkarni, S.R. and Song, D., 2021, April. Enabling efficient cyber threat hunting with cyber threat intelligence. In 2021 IEEE 37th International Conference on Data Engineering (ICDE) (pp. 193-204). IEEE.
- Gordon, J. (2019). Cyber threat intelligence: What it is and why it matters. Security Intelligence. Retrieved from https://securityintelligence.com/what-is-cyber-threat-intelligence/
- Gorman, M., & Sands, K. (2014). Cyber threat intelligence: A call to action. Georgetown Journal of International Affairs, 15(2), 13-18.
- Green, B. D., et al. (2020). Towards Understanding the Impact of Regulatory Compliance on Cybersecurity Investments. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security.
- Gong, N., 2019. Barriers to adopting interoperability standards for cyber threat intelligence sharing: an exploratory study. In Intelligent Computing: Proceedings of the 2018 Computing Conference, Volume 2 (pp. 666-684). Springer International Publishing.
- Haas, T., & Goetz, E. (2019). Improving Cyber Threat Intelligence for Enhanced Security Operations. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1), 31-52.
- Hendrickx, S., Muylle, S., & Wauters, K. (2018). Exploring cyber threat intelligence in financial institutions: A case study. Journal of Computer Information Systems, 58(1), 1-11.
- Herjavec, R. (2021). Cybercrime damages to cost the world $6 trillion annually by 2021. Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
- IBM Security &Ponemon Institute. (2021). Cost of a Data Breach Report 2021. Retrieved from https://www.ibm.com/security/data-breach
- Jackson, S. L. (2011). Research Methods and Statistics: A Critical Thinking Approach. Cengage Learning.
- Johnson, B., & Smith, H. (2018). The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry. Oxford University Press.
- Kolias, C., Kambourakis, G., Stavrou, A., &Gritzalis, D. (2020). A systematic review of cyber threat intelligence sources, sharing, and models. Computers & Security, 91, 101687
- Kott, A., Coleman, J., & Arnold, R. (2019). A survey of cyber threat intelligence use in large organizations. Journal of Cybersecurity, 5(1), tyz001.
- Krombholz, K., Merzdovnik, G., &Weippl, E. (2019). Can cyber threat intelligence reduce the effectiveness of risk-driven security metrics? IEEE Transactions on Dependable and Secure Computing, 16(4), 646-658.
- Kshetri, N., &Voas, J. (2018). Blockchain-enabled cybersecurity and privacy: A framework and research agenda. Computer Standards & Interfaces, 59, 1-8.

- Kure, H.I. and Islam, S. (2019), Assets focus risk management framework for critical infrastructure cybersecurity risk management. IET Cyber-Physical Systems: Theory & Applications, 4: 332-340. https://doi.org/10.1049/iet-cps.2018.5079
- Li, S., Yao, X., & Li, J. (2020). Cyber threat intelligence adoption in organizations: A multi-stakeholder perspective. Journal of Business Research, 116, 279-289.
- Libicki, M. C. (2017). Cyberspace in peace and war. Cambridge University Press.
- Mavroeidis, V. and Jøsang, A., 2018, March. Data-driven threat hunting using sysmon. In Proceedings of the 2nd international conference on cryptography, security and privacy (pp. 82-88).
- Mavroeidis, V. and Bromander, S., 2017, September. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In 2017 European Intelligence and Security Informatics Conference (EISIC) (pp. 91-98). IEEE.
- McKeen, D. (2021). Cyber Threat Intelligence (CTI). In M. Gupta, J. Walp, & J. Bishop (Eds.), Handbook of Research on Cyber Threat Intelligence and Detection Automation (pp. 1-19). IGI Global.
- Mell, P., Scarfone, K., & Romanosky, S. (2018). Creating a cyber threat intelligence–driven security operations center. National Institute of Standards and Technology.
- Menges, F., Sperl, C. and Pernul, G., 2019. Unifying cyber threat intelligence. In Trust, Privacy and Security in Digital Business: 16th International Conference, TrustBus 2019, Linz, Austria, August 26–29, 2019, Proceedings 16 (pp. 161-175). Springer International Publishing.
- Milajerdi, S.M., Eshete, B., Gjomemo, R. and Venkatakrishnan, V.N., 2019, November. Poirot: Aligning attack behavior with kernel audit records for cyber threat hunting. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security (pp. 1795-1812).
- Mohurle, S. and Patil, M., 2017. A brief study of wannacry threat: Ransomware attack 2017. International journal of advanced research in computer science, 8(5), pp.1938-1940.
- Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.
- Rass, S., et al. (2020). Utilizing Cyber Threat Intelligence for Enhancing Network Security. In Proceedings of the 53rd Hawaii International Conference on System
- Pernik, I. (2020). Cyber Threat Intelligence Sharing and Privacy: The Challenge of Non-Personal Data. In Proceedings of the 15th International Conference on Availability, Reliability, and Security (ARES).
- National Cybersecurity and Communications Integration Center. (2019). Cyber Threat Intelligence Integration Center (CTIIC). United States Department of Homeland Security. Retrieved from https://www.cisa.gov/national-cybersecurity-and-communications-integration-center
- Nunnery, C., Fenstermacher, L., & Bear, J. (2018). The benefits of using cyber threat intelligence for organizations. Journal of Information Warfare, 17(1), 19-29.
- O'Brien, N., 2022. Assessing the importance of modern security tools and frameworks to help detect and defend against Cozy bear (Doctoral dissertation, Dublin, National College of Ireland).

- Ovelar, R., Ramadhan, D., Wilke, B., van der Lubbe, J., & Asghari, H. (2020). A comparative study of public-private partnerships in cyber threat intelligence sharing. IEEE Transactions on Dependable and Secure Computing, 1-1.
- Petróczki, K., Fejes, A., &Buttyán, L. (2018). A survey on cyber threat intelligence sharing mechanisms. Computers & Security, 78, 222-241.
- Rania, (2017 oct 20). Saudi Arabia is more than Middle Eastern countries vulnerable to cyber-attacks. Retrieved from https://www.aleqt.com/2017/10/19/article_1269641.html
- Rajasekar, D. and Verma, R., 2013. Research methodology. Archers & Elevators Publishing House.
- S. Samtani, K. Chinn, C. Larson and H. Chen, "AZSecure hacker assets portal: Cyber threat intelligence and malware analysis", 2016 IEEE Conference on Intelligence and Security Informatics (ISI). Institute of Electrical and Electronics Engineers (IEEE), pp. 19-24, Sept 2016.
- SANS Institute. (2019). Using Cyber Threat Intelligence to Improve Security Operations. Retrieved from https://www.sans.org/white-papers/40287/
- Scarfone, K., Souppaya, M., & Masone, K. (2013). Guide to Cyber Threat Information Sharing. National Institute of Standards and Technology (NIST) Special Publication, 800-150.
- Schmittner, C., State, R., Weber, K., Probst, C. W., & Riedel, N. (2018). CTI sharing standardization: An industry perspective. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2025-2027.
- SentinelOne. (2021). Threat Intelligence. Retrieved from https://www.sentinelone.com/blog/threat-intelligence/
- Schwarz, J., Fiebig, T., & Kirchner, C. (2020). The economics of cyber threat intelligence. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2685-2687.
- Schauer, S., & Feldman, S. (2019). Cyber Threat Intelligence Sharing: Investigating the Moderating Role of Regulatory Uncertainty. In Proceedings of the 52nd Hawaii International Conference on System Sciences.
- Sieber, J. E. (1992). Planning ethically responsible research: A guide for students and internal review boards. Sage Publications.
- Silverman, D. (2017). Qualitative research. Sage publications.
- Snyder, H., 2019. Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, pp.333-339.
- Sood, A. K., & Enbody, R. J. (2013). Intrusion detection in industrial control systems with SNORT. In Proceedings of the 2013 IEEE Conference on Technologies for Homeland Security (pp. 278-283). IEEE.
- Splunk. (2021). Splunk Security Solutions. Retrieved from https://www.splunk.com/en_us/solutions/solution-areas/security-and-compliance.html
- Stein, D.J. and Nesse, R.M., 2011. Threat detection, precautionary responses, and anxiety disorders. Neuroscience & Biobehavioral Reviews, 35(4), pp.1075-1079.

- Tavakoli, R., & Abu-Shanab, E. (2021). Cybersecurity incident detection and response: A systematic literature review. Journal of Network and Computer Applications, 184, 103005. https://doi.org/10.1016/j.jnca.2021.103005
- Thomas, R., & Brown, D. (2021). Challenges in Implementing Cyber Threat Intelligence for Security Operations. Cybersecurity Review, 6(3), 123-145.
- Tounsi, W. and Rais, H., 2018. A survey on technical threat intelligence in the age of sophisticated cyber-attacks. Computers & security, 72, pp.212-233.
- Turner, J., & Singletary, T. (2018). Operationalizing Cyber Threat Intelligence. Journal of Information Warfare, 17(2), 47-60.
- Ucci, D., Aniello, L. and Baldoni, R., 2019. Survey of machine learning techniques for malware analysis. Computers & Security, 81, pp.123-147.
- Verma, A. K., & Srivastava, G. (2017). A novel approach to network security using cyber threat intelligence. In Proceedings of the 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 426-431). IEEE.
- Wang, L., & Chen, H. (2022). The Role of Cyber Threat Intelligence in Enhancing Security Operations. Computers & Security, 99, 101-116.
- Wei, R., Cai, L., Zhao, L., Yu, A. and Meng, D., 2021. Deephunter: A graph neural network-based approach for robust cyber threat hunting. In Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6–9, 2021, Proceedings, Part I 17 (pp. 3-24). Springer International Publishing.
- Wilson, J. (1981). "Research methods: the honeycomb model." Philosophy of the Social Sciences, vol. 11, no. 3, pp. 245-266.
- Yamin, M. A., et al. (2019). Cyber Threat Intelligence: Challenges and Opportunities. In Proceedings of the 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS).
- Yazdinejad, A., Dehghantanha, A., Parizi, R.M., Hammoudeh, M., Karimipour, H. and Srivastava, G., 2022. Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks. IEEE Transactions on Industrial Informatics, 18(11), pp.8356-8366.
- Yen, S. S., & Chen, Y. H. (2015). Establishing a Cyber Threat Intelligence Sharing Platform for an Industrial Control System. Journal of Information Hiding and Multimedia Signal Processing, 6(6), 1052-1062.
- The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). The Belmont report: Ethical principles and guidelines for the protection of human subjects of research. US Department of Health, Education, and Welfare.
- Zhang, T., & Liao, Q. (2019). Application of Cyber Threat Intelligence in Network Security Defense. Journal of Physics: Conference Series, 1286(1), 012074.

- Zibak, A. and Simpson, A., 2019, August. Cyber threat information sharing: Perceived benefits and barriers. In Proceedings of the 14th international conference on availability, reliability and security (pp. 1-9).
- Zutshi, A., & Swarup, V. (2015). An agent-based framework for cyber threat intelligence. In Proceedings of the 2015 IEEE International Conference on Agent-Based Modeling and Simulation (ABMS) (pp. 172-177). IEEE.
- Z. Fang, X. Zhao, Q. Wei, G. Chen, Y. Zhang, C. Xing, et al., "Exploring key hackers and cybersecurity threats in chinese hacker communities", 2016 IEEE Conference on Intelligence and Security Informatics (ISI). Institute of Electrical and Electronics Engineers (IEEE), pp. 13-18, Sept 2016.
- Zawoad, S., et al. (2017). A Survey of Cyber Threat Intelligence Solutions. IEEE Access, 5, 2045-2063.
- Zwitter, A., & Kruegel, C. (2014). Cyber threat intelligence. IEEE Security & Privacy, 12(5), 38-49.