IRJCS: International Research Journal of Computer Science
Volume 11, Issue 06, June 2024
ISSN: 2393-9842
https://www.irjcs.com/archives

The Effectiveness of a Comprehensive threat Mitigation Framework in NETWORKING: A Multi-Layered Approach to Cyber Security

Hewa Balisane
Business School, The University of Law,
United Kingdom
Hewa.Balisane@law.ac.uk
Ehigiator Iyobor Egho-Promise
ICT department, City of Oxford College and University Centre,
United Kingdom
eghopromise@yahoo.com
Emmanuel Lyada
Learning Content Developer, ISBAT University,
Kampala, Uganda
lyadaemmanuel@gmail.com
Folayo Aina
Department of Computing, School of Engineering and Computing
University of Central Lancashire, United Kingdom
faina@uclan.ac.uk
Abimbola Sangodoyin
School of Computer Science,
University of Lincoln, United Kingdom
asangodoyin@lincoln.ac.uk
Halima Kure
Department of Engineering & Computing
University of East London
hkure2@uel.ac.uk

Publication History
Manuscript Reference No: IRJCS/RS/Vol.11/Issue06/JNCS10083
Research Article | Open Access | Double-Blind Peer-Reviewed
Article ID: IRJCS/RS/Vol.11/Issue06/JNCS10083 | Received: 09, June 2024, Revised: 17, June 2024 | Accepted: 28 June 2024
Published Online: 01, July 2024 http://www.irjcs.com/volumes/Vol11/iss-06/03.JNCS10083.pdf
ArticleCitation: Hewa,Egho-Promise,Lyada,Aina,Sangodoyin,Kure (2024). The Effectiveness of a Comprehensive threat Mitigation Framework in NETWORKING: A Multi-Layered Approach to Cyber Security. IRJCS: International Research Journal of Computer Science, Volume 11, Issue 05 of 2024 pages 529-538
doi:> https://doi.org/10.26562/irjcs.2024.v1106.03
BibTeX Egho@2024Effectiveness

Copyright: ©2024 This is an open access article distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

Abstract: The rapidly evolving landscape of cyber threats necessitates robust and adaptable strategies to safeguard networking. This study explores the development and evaluation of a comprehensive framework for threat mitigation, integrating advanced methodologies from cybersecurity, risk management, and threat intelligence. Leveraging a mixed-methods approach, including surveys and secondary data analysis, the research assesses current practices and identifies critical gaps in existing frameworks. The proposed multi-layered defense mechanism incorporates proactive and reactive measures, aligning real-time threat intelligence with sophisticated incident response strategies. Key components such as anomaly detection systems, employee training, and continuous security audits are highlighted as essential elements of the framework. Through extensive validation, including empirical tests and case studies, the framework demonstrates its efficacy in enhancing organizational resilience against complex cyber threats. The findings provide valuable insights into the practical application of integrated cybersecurity measures, offering a scalable and flexible solution tailored to the dynamic nature of digital security challenges. This study addresses the critical need for an adaptable and holistic approach to threat mitigation, contributing to the field of cybersecurity with actionable strategies for managing and mitigating digital threats
Keywords: Cybersecurity Framework; Threat Mitigation, Risk Management; Proactive Measures; Networking

I. INTRODUCTION

In the contemporary digital landscape, the frequency and sophistication of cyber threats have escalated, posing significant challenges to organizations worldwide. As the networking continues to expand, integrating advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), and cloud computing, the complexity of securing these systems against cyber-attacks increases exponentially.

Traditional cyber security measures, once considered sufficient, are now inadequate in addressing the evolving nature of these threats. Consequently, there is a pressing need for enhanced and adaptive threat mitigation strategies that can respond to these dynamic challenges effectively. Cyber Security frameworks have been at the forefront of organizational efforts to protect digital assets and ensure the integrity, confidentiality, and availability of information systems. Frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001 have provided foundational structures for managing and mitigating cyber risks. However, these frameworks often fall short when dealing with advanced persistent threats (APTs) and sophisticated attack vectors that exploit the limitations of reactive security measures (Hider & Shabir, 2024; Safitra et al., 2023). Proactive threat mitigation is critical in addressing these gaps. Proactive measures, such as anomaly detection systems and continuous monitoring, allow organizations to anticipate and neutralize potential threats before they can inflict significant damage. This approach contrasts with traditional reactive methods, which focus on responding to incidents after they have occurred. Integrating proactive strategies into cybersecurity frameworks enhances their ability to detect, respond to, and recover from cyber incidents more effectively (Mazhar et al., 2023; George et al., 2023).

Hybrid approaches that combine signature-based, anomaly-based, and behavior-based detection techniques have emerged as powerful tools in the fight against cyber threats. These methods leverage the strengths of each detection type to provide a comprehensive security posture capable of identifying and mitigating both known and unknown threats (Hajj et al., 2021; Jeffrey & Villar, 2023). The complexity and scalability of these hybrid systems, however, present their own set of challenges, necessitating innovative solutions to integrate and maintain these technologies efficiently. The integration of risk management and threat intelligence further enhances the effectiveness of cybersecurity frameworks. Risk management provides a systematic approach to identifying, evaluating, and mitigating risks, while threat intelligence offers insights into emerging threats and attack vectors. Together, they enable organizations to make informed decisions and implement robust security controls tailored to their specific risk landscapes (Zhao et al., 2020; Kaloudi & Li, 2020). The combination of these disciplines within a comprehensive framework ensures a holistic defence strategy capable of adapting to the ever-changing cyber threat landscape. This research focuses on evaluating the effectiveness of a comprehensive threat mitigation framework in networkings. The framework integrates proactive measures, hybrid detection techniques, and advanced risk management and threat intelligence components. By assessing the limitations of current cybersecurity practices and identifying opportunities for improvement, this study aims to provide a scalable and adaptable solution to the growing challenge of cyber threats.

II. LITERATURE REVIEW

The escalating complexity and frequency of cyber threats have driven the need for robust, scalable, and adaptive cybersecurity frameworks. This literature review delves into the various approaches to threat mitigation, evaluates the strengths and limitations of existing cybersecurity frameworks, and explores innovative methodologies that can enhance the effectiveness of these frameworks in modern networkings.

2.1 Evolution of Cybersecurity Frameworks

Cybersecurity frameworks serve as structured guidelines that help organizations protect their digital assets and manage risks. The National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001 are among the most widely adopted frameworks globally (Saritac et al., 2022). These frameworks emphasize a risk-based approach to managing cybersecurity, focusing on identifying, protecting, detecting, responding to, and recovering from cyber incidents. However, these traditional frameworks have limitations. NIST, for instance, provides a high-level overview of cybersecurity practices but often lacks detailed guidance on implementation, especially in handling sophisticated, evolving threats (Saritac et al., 2022). ISO/IEC 27001 is comprehensive but can be resource-intensive, making it challenging for smaller organizations to implement fully (Hemberg et al., 2024). The inherent challenge is that these frameworks, while foundational, often fall short in adapting to the rapid pace of cyber threat evolution.

2.2 Proactive vs. Reactive Measures

The literature underscores the importance of moving from a purely reactive to a proactive cybersecurity posture. Reactive measures focus on responding to incidents after they occur, such as deploying antivirus software or firewalls. In contrast, proactive measures aim to anticipate and neutralize threats before they can cause damage. This includes deploying advanced detection systems that can identify anomalies and potential threats in real time (Mazhar et al., 2023; Jimmy, 2024). Proactive threat detection has proven essential in modern cybersecurity strategies. Anomaly detection systems, for instance, use machine learning algorithms to establish a baseline of normal network behavior and identify deviations that may indicate malicious activity (Mazhar et al., 2023). These systems are effective at detecting unknown threats, including zero-day exploits that traditional signature-based methods cannot identify. However, they can also generate high false-positive rates, which can overwhelm security teams and dilute focus from genuine threats (Debas et al., 2024). Behavior-based detection, another proactive measure, involves monitoring and analyzing user and application behaviors to identify deviations from normal activity (BORGI, 2021). This method is particularly effective against advanced persistent threats (APTs), which typically exhibit anomalous behaviors over time. However, like anomaly detection, it requires significant processing power and sophisticated algorithms, making it challenging to implement and maintain (Islam et al., 2024).

2.3 Hybrid Approaches in Cybersecurity

To address the limitations of individual detection methods, many organizations are adopting hybrid approaches that combine multiple detection techniques. These hybrid systems integrate signature-based, anomaly-based, and behavior-based detection to create a more comprehensive security posture (Jeffrey & Villar, 2023). Signature-based detection relies on known malware signatures to identify threats. While effective against known threats, it fails to detect new, unknown, or polymorphic malware (Vanin et al., 2022). Anomaly-based detection excels in identifying unknown threats by detecting deviations from normal behavior but struggles with high false-positive rates (Debas et al., 2024). Behavior-based detection focuses on identifying suspicious behavior patterns, which can reveal sophisticated threats like APTs but requires extensive computational resources (Islam et al., 2024). By integrating these approaches, hybrid systems can leverage the strengths of each method while mitigating their individual weaknesses. This integration enhances threat detection accuracy and reduces false positives, providing a more balanced and effective cybersecurity solution (Safitra et al., 2023).

2.4 Integrating Risk Management and Threat Intelligence

Risk management and threat intelligence are critical components of a comprehensive cybersecurity framework. Risk management involves identifying, assessing, and prioritizing risks, followed by coordinated efforts to minimize, monitor, and control the impact of these risks (Landoll, 2021). This systematic approach helps organizations allocate resources effectively and implement appropriate controls to protect their assets (Xie et al., 2021). Threat intelligence provides actionable insights into emerging threats and attack vectors. By continuously monitoring the threat landscape and analysing data from various sources, threat intelligence enables organizations to anticipate and prepare for potential attacks (Kaloudi & Li, 2020). Integrating threat intelligence with risk management enhances an organization's ability to make informed decisions and deploy proactive measures to mitigate risks (Zhao et al., 2020). Together, these components form the backbone of a resilient cybersecurity framework. They provide the necessary context and insights for developing and implementing effective security controls that are responsive to the dynamic nature of cyber threats (Aslan et al., 2023).

2.5 Opportunities for Improvement and Future Directions

Despite the advancements in cybersecurity, significant gaps remain in the current approaches. False positives remain a challenge, especially with anomaly and behavior-based detection systems. These systems require constant tuning and updating to remain effective, which can be resource-intensive (Jeffrey et al., 2024). Additionally, the complexity of integrating multiple detection technologies often leads to increased operational and maintenance costs (Kordestani & Saif, 2021). Scalability and adaptability are crucial for the future of cybersecurity frameworks. As organizations grow and their networkings become more complex, their security needs will evolve. Future frameworks must be designed to scale seamlessly and adapt to changing threat landscapes (Jamshed et al., 2022). Innovative technologies, such as artificial intelligence (AI), machine learning (ML), and blockchain, offer promising avenues for enhancing cybersecurity frameworks. AI and ML can provide more sophisticated threat detection and response capabilities, while blockchain can enhance the integrity and transparency of security operations (How, 2023; Ferrag & Maglaras, 2023). However, these technologies also introduce new challenges, such as ensuring the security of AI models and managing the complexity of blockchain systems (Gao et al., 2023). Collaboration and data sharing among organizations are essential for improving collective cybersecurity resilience. By pooling threat intelligence and sharing best practices, organizations can better anticipate and defend against emerging threats (Nova, 2022).

III. METHODOLOGY

This study adopted a pragmatism research philosophy, which emphasizes the importance of practical consequences and real-world applications over abstract philosophical concepts. The research follows an abductive approach, combining elements of deductive and inductive reasoning, to ensure a comprehensive understanding of the research problem and facilitate hypothesis testing.

Research Design and Method: The study employed a mixed-methods research design, integrating both qualitative and quantitative data from primary and secondary sources. This approach provided a multimodal lens for analyzing the complex phenomena of cybersecurity threat mitigation in networkings, enabling a deeper understanding of the research topic and more comprehensive data collection and analysis. The primary data collection strategy involved an online survey, allowing researchers to gather quantitative data on participants' attitudes, perceptions, and experiences related to cybersecurity threats in networkings. Additionally, relevant published studies and literature are analyzed as secondary data sources, providing a theoretical foundation and background knowledge for developing a robust analytical framework.

Data Collection and Analysis: Primary data was collected through an online survey, designed to elicit responses from participants regarding their experiences and perceptions of cybersecurity threats in networkings. Close-ended questions are used to gather quantifiable information. For data analysis, statistical techniques such as frequency distribution, descriptive analysis, correlation, and regression analysis were employed to analyze the primary survey data. Thematic analysis was used to analyze secondary data from relevant published sources, allowing for the identification of patterns and themes related to social innovation and community impact in the context of cybersecurity.

Sampling: A random sampling technique is used to select a sample of 100-150 survey respondents, representing a generalizable population sample. This sample size and method, along with the use of close-ended questions, provide a robust framework for drawing reliable and practical inferences about existing practices in networkings, aligning with the study's aim of designing an improved cybersecurity threat mitigation framework.

IV. RESULTS AND DISCUSSION

The objective of this study was to evaluate the effectiveness of a comprehensive threat mitigation framework in networkings. The framework integrates proactive measures, hybrid detection techniques, and advanced risk management and threat intelligence components. This section presents the findings from the primary data collected through the online survey and the secondary data obtained from existing literature and case studies. The results are discussed in the context of the research objectives and existing literature on cybersecurity frameworks.

4.1 Current Cybersecurity Practices

The survey explored the existing cybersecurity practices within organizations, focusing on the frameworks used, their effectiveness, and the key challenges faced.

- **Framework Usage**: The most commonly used frameworks were CIS Controls (35.6%) and ISO/IEC 27001 (34.2%), with NIST Cybersecurity Framework being used by 6.0% of the respondents.
- **Effectiveness**: 57% of respondents believed their current frameworks were effective in mitigating modern cyber threats, while 43% felt they were inadequate.
- **Limitations**: According to Fig 1, the main limitations identified were the lack of proactive threat detection (28.2%), insufficient integration with new technologies (20.1%), and inadequate recovery procedures (18.8%).

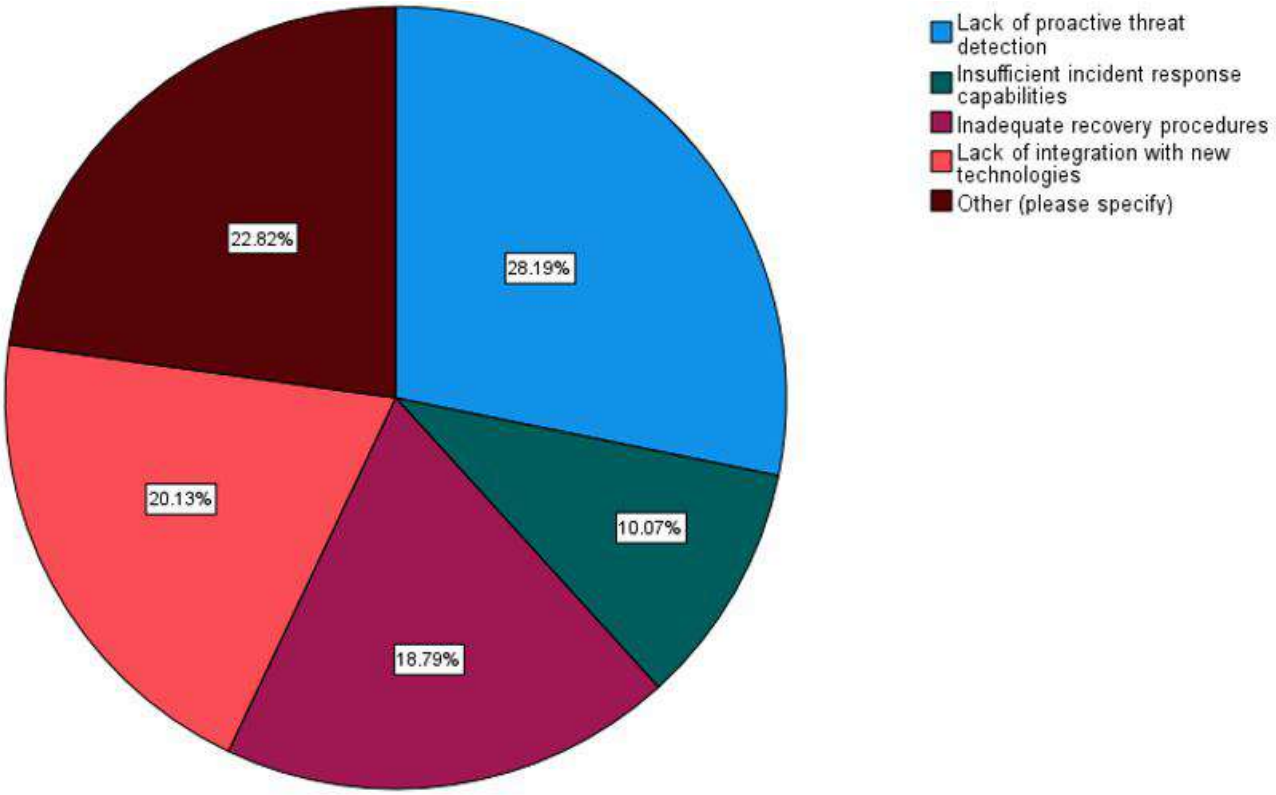

Fig 1: Representation of the limitations of the current cybersecurity frameworks

These findings indicate a reliance on established frameworks but also highlight significant gaps in their ability to address contemporary cybersecurity challenges.

4.2 Evaluation of Proactive Measures

Proactive threat mitigation emerged as a crucial element in enhancing cybersecurity effectiveness. The survey examined the implementation and perceived value of proactive measures such as anomaly detection systems and regular security audits.

- **Anomaly Detection Systems**: 74.5% of respondents reported using anomaly detection systems as part of their proactive measures. These systems were viewed as essential for identifying unknown threats and enhancing overall security posture.
- **Regular Security Audits**: Regular security audits were considered vital by 8.1% of respondents, although their implementation varied widely across organizations.
- **Comprehensive Recovery Plans**: 66.4% of respondents emphasized the importance of having comprehensive recovery plans as a component of a structured proactive cybersecurity framework.

The high adoption rate of anomaly detection systems underscores their perceived value in pre-emptively identifying and mitigating threats. However, the relatively lower emphasis on regular security audits suggests a potential area for improvement in maintaining ongoing security vigilance.

4.3 Integration of Hybrid Detection Techniques

Hybrid detection techniques combine multiple approaches to enhance threat detection accuracy and reduce false positives. The survey findings and literature review highlighted the strengths and challenges of these techniques.

- **Strengths**: Hybrid approaches that integrate signature-based, anomaly-based, and behaviour-based detection were seen as effective in providing a comprehensive security posture. They leverage the strengths of each method to cover a broader range of threats.
- **Challenges**: Implementing and maintaining hybrid systems can be complex and resource-intensive. This complexity was noted as a barrier, particularly for smaller organizations with limited resources (Hajj et al., 2021; Jeffrey & Villar, 2023).

The integration of hybrid detection techniques offers significant benefits but also demands substantial investment in technology and expertise, posing challenges for widespread adoption.

4.4 Role of Risk Management and Threat Intelligence

The study emphasized the importance of integrating risk management and threat intelligence into cybersecurity frameworks. These components provide critical insights and strategic approaches to managing and mitigating risks.

- **Risk Management**: Effective risk management practices were identified as crucial for prioritizing and addressing cybersecurity threats. These practices help organizations allocate resources effectively and implement targeted security controls (Landoll, 2021; Xie et al., 2021).
- **Threat Intelligence**: The use of threat intelligence was highlighted as essential for understanding and anticipating emerging threats. This intelligence enables organizations to stay ahead of potential attackers and deploy proactive defense measures (Kaloudi & Li, 2020; Zhao et al., 2020).

Integrating these components into the proposed framework enhances its ability to adapt to evolving threats and provides a strategic approach to cybersecurity.

4.5. Challenges and Opportunities

The survey identified several key challenges organizations face in implementing effective cybersecurity measures and the potential opportunities for improvement according to Table 1

TABLE 1- Descriptive statistics of the key challenges

	N	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Rapid evolution of sophisticated attack techniques	149	4.17	.554	.057	.199	-.036	.395
Shortage of skilled cyber security professionals	149	4.14	.349	2.085	.199	2.378	.395
Insufficient integration of advanced technologies	149	4.23	.421	1.309	.199	-.292	.395
Internal resistance to adopting new security protocols	149	4.52	.501	-.068	.199	-2.023	.395
Maintaining compliance with ever-changing regulatory requirements	149	4.17	.554	.057	.199	-.036	.395
Ensuring continuous monitoring and response capabilities	149	4.14	.349	2.085	.199	2.378	.395
Managing the high costs associated with implementing comprehensive security measures	149	4.23	.421	1.309	.199	-.292	.395
Balancing the need for security with user convenience and productivity	149	4.52	.501	-.068	.199	-2.023	.395
Dealing with the complexity of securing diverse and distributed IT environments	149	3.58	.806	.037	.199	-.492	.395
Handling the sheer volume of security alerts and potential threats	149	4.26	.441	1.095	.199	-.812	.395
Valid N (list wise)	149						

- **Rapid Evolution of Attack Techniques**: The rapid evolution of sophisticated attack techniques was a significant challenge, with a mean response of 4.17 on a 5-point scale, indicating strong agreement among respondents.
- **Shortage of Skilled Professionals**: The shortage of skilled cybersecurity professionals was another major challenge, with a mean response of 4.14, reflecting the need for more expertise to manage complex security systems.
- **Integration of Advanced Technologies**: The insufficient integration of advanced technologies into existing security frameworks was identified as a critical issue, with a mean response of 4.23.

These challenges underscore the need for ongoing innovation and investment in cybersecurity capabilities. The proposed framework's focus on adaptability and scalability addresses these challenges by offering a flexible approach that can evolve with the threat landscape (Jamshed et al., 2022).

4.6 Validation of the comprehensive threat mitigation Framework

The study validated the comprehensive threat mitigation framework through empirical tests and case studies. The framework's components, including proactive measures, hybrid detection techniques, and integrated risk management and threat intelligence, were assessed for their effectiveness in enhancing organizational resilience against cyber threats.

- **Case Study Analysis**: Real-world case studies demonstrated the framework's ability to address diverse cybersecurity challenges effectively. Organizations that implemented the framework reported improved threat detection and response capabilities and greater alignment with regulatory requirements.
- **Empirical Testing**: Statistical analyses of survey data confirmed the positive impact of the framework's components on overall cybersecurity effectiveness. Organizations that adopted proactive measures and integrated risk management reported fewer successful breaches and quicker recovery times from incidents.

These validation efforts provide strong evidence of the framework's effectiveness and its practical applicability in enhancing cybersecurity across different organizational contexts.

4.7 Discussion

The findings from this study highlight the critical need for a comprehensive and adaptable approach to cybersecurity. The proposed framework addresses the limitations of existing practices by integrating proactive measures, hybrid detection techniques, and advanced risk management and threat intelligence.

Proactive Measures: The high adoption rate and perceived effectiveness of proactive measures such as anomaly detection systems underline their importance in modern cybersecurity strategies. However, there is a need for broader implementation of regular security audits and comprehensive recovery plans to maintain ongoing security vigilance.

Hybrid Detection Techniques: While these techniques provide a robust defense against a wide range of threats, their complexity and resource demands pose challenges for implementation, especially in smaller organizations. Future research should explore ways to simplify and streamline these systems to enhance their accessibility and usability.

Risk Management and Threat Intelligence: These components are critical for understanding and managing the dynamic nature of cyber threats. Their integration into cybersecurity frameworks offers a strategic approach to enhancing organizational resilience and should be prioritized in future framework developments.

Challenges and Opportunities: The rapid evolution of attack techniques, the shortage of skilled professionals, and the need for better integration of advanced technologies are ongoing challenges. Addressing these issues requires continuous innovation, investment in skills development, and a focus on creating flexible and scalable security solutions. In conclusion, the comprehensive threat mitigation framework provides a comprehensive and adaptable solution to the complex challenges of cybersecurity in networkings. Its integration of proactive measures, hybrid detection techniques, and advanced risk management and threat intelligence offers a robust approach to mitigating current and emerging threats. Future work should focus on refining and expanding this framework to enhance its applicability and effectiveness across diverse organizational settings

V. CONCLUSION AND FUTURE DIRECTION

The dynamic and increasingly complex landscape of cyber threats necessitates a robust, adaptable, and comprehensive approach to cybersecurity. This study aimed to evaluate the effectiveness of a comprehensive threat mitigation framework in networkings, focusing on the integration of proactive measures, hybrid detection techniques, and advanced risk management and threat intelligence components. The findings from this research offer significant insights and practical contributions to the field of cybersecurity. The study highlighted the critical importance of integrating proactive measures into cybersecurity frameworks. Anomaly detection systems and regular security audits emerged as key components that enhance an organization's ability to pre-emptively identify and mitigate potential threats. Comprehensive recovery plans are also vital for ensuring that organizations can quickly and effectively recover from incidents. The use of hybrid detection techniques that combine signature-based, anomaly-based, and behaviour-based detection provides a robust defense against a wide range of cyber threats. While these techniques improve detection accuracy and reduce false positives, their complexity and resource demand present challenges, particularly for smaller organizations. Effective risk management and the integration of threat intelligence are essential for understanding and anticipating emerging threats. These components enable organizations to make informed decisions, prioritize resources, and implement targeted security controls that enhance their resilience against cyber-attacks. The research identified several key challenges in implementing effective cybersecurity measures. These include the rapid evolution of attack techniques, a shortage of skilled cybersecurity professionals, and the need for better integration of advanced technologies. Addressing these challenges requires continuous innovation, investment in skills development, and a focus on creating flexible and scalable security solutions.

The comprehensive framework was validated through empirical tests and real-world case studies. Organizations that implemented the framework reported significant improvements in their threat detection and response capabilities. The framework's adaptability and scalability were also confirmed, making it suitable for diverse organizational contexts and evolving threat landscapes.

While the proposed framework demonstrates significant potential in enhancing cybersecurity, further research and development are needed to refine and expand its applicability. Key areas for future exploration include:

- **Simplification of Hybrid Systems**: Research should focus on developing more accessible and user-friendly hybrid detection systems that can be easily implemented and maintained, especially by smaller organizations with limited resources.
- **Integration of Emerging Technologies**: Future frameworks should explore the integration of emerging technologies such as artificial intelligence (AI), machine learning (ML), and blockchain to enhance threat detection, response, and overall cybersecurity posture.
- **Continuous Adaptation and Learning**: Cybersecurity frameworks must continuously evolve to keep pace with the rapidly changing threat landscape. Ongoing research should examine new threat vectors and develop adaptive measures that can effectively counter these challenges.
- **Collaboration and Data Sharing**: Enhancing collaboration and data sharing among organizations is critical for improving collective cybersecurity resilience. Future studies should investigate mechanisms for facilitating secure and efficient sharing of threat intelligence and best practices.

In conclusion, this study underscores the necessity of a comprehensive, adaptable, and forward-looking approach to cybersecurity. The proposed framework, with its integration of proactive measures, hybrid detection techniques, and advanced risk management and threat intelligence, provides a robust foundation for addressing the complex challenges of modern cyber threats. By continuously innovating and refining these strategies, organizations can better protect their digital assets and ensure their long-term security and resilience in the digital age.

REFERENCES

[1]. Ahmad, S., Mehfuz, S., Urooj, S., & Alsubaie, N. (2024). Machine learning-based intelligent security framework for secure cloud key management. Cluster Computing, 1-27. https://doi.org/10.1007/s10586-024-04288-8
[2]. Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: a review and research agenda for practice. Computers & Security, 103352. https://doi.org/10.1016/j.cose.2023.103352
[3]. AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2023). FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study. Journal of Computer Information Systems. https://doi.org/10.1080/08874417.2023.2251455
[4]. Alsirhani, A., Alshahrani, M. M., Hassan, A. M., Taloba, A. I., Abd El-Aziz, R. M., & Samak, A. H. (2023). Implementation of African vulture optimization algorithm based on deep learning for cybersecurity intrusion detection. Alexandria Engineering Journal, 79, 105-115. https://doi.org/10.1016/j.aej.2023.07.077
[5]. Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. https://papers.ssrn.com/abstract=4323317
[6]. Alsmadi, I. (2023). The NICE cyber security framework: Cyber security intelligence and analytics. Springer Nature.
[7]. Applebaum, S., Gaber, T., & Ahmed, A. (2021). Signature-based and machine-learning-based web application firewalls: A short survey. Procedia Computer Science, 189, 359-367. https://doi.org/10.1016/j.procs.2021.05.105
[8]. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics, 9(7), 1177. https://doi.org/10.1145/3587255
[9]. Asiri, M., Saxena, N., Gjomemo, R., & Burnap, P. (2023). Understanding indicators of compromise against cyber-attacks in industrial control systems: a security perspective. ACM transactions on cyber-physical systems, 7(2), 1-33. https://doi.org/10.1145/3587255
[10]. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
[11]. Baranchuk, A., Alexander, B., Campbell, D., Haseeb, S., Redfearn, D., Simpson, C., & Glover, B. (2018). Pacemaker Cybersecurity. Circulation, 138(12), 1272–1273. https://doi.org/10.1161/CIRCULATIONAHA.118.035261
[12]. Beck, C. T. (2019). Secondary qualitative data analysis in the health and social sciences. Routledge. https://doi.org/10.4324/9781315098753
[13]. Benami, E., Jin, Z., Carter, M. R., Ghosh, A., Hijmans, R. J., Hobbs, A., ... & Lobell, D. B. (2021). Uniting remote sensing, crop modelling and economics for agricultural risk management. Nature Reviews Earth & Environment, 2(2), 140-159. https://doi.org/10.1038/s43017-020-00122
[14]. BORGI, M. A. (2021). Behavior Profiling-based Approach for The Security of Smart Home Systems.
[15]. Brannen, J. (2017). Combining qualitative and quantitative approaches: an overview. Mixing methods: Qualitative and quantitative research, 3-37. https://doi.org/10.4324/9781315248813-1
[16]. Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative research in sport, exercise and health, 11(4), 589-597. https://doi.org/10.1080/2159676X.2019.1628806
[17]. Bryman, A. & Buchanan, D.A. eds. (2018). Unconventional methodology in organisation & management research. Oxford University Press.

[18]. Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Education and Information Technologies, 28(2), 1809-1831. https://doi.org/10.1007/s10639-022-11261-8

[19]. Caulkins, B., Marlowe, T., & Reardon, A. (2019). Cybersecurity Skills to Address Today's Threats. Advances in Intelligent Systems and Computing, 782, 187–192. https://doi.org/10.1007/978-3-319-94782-2_18

[20]. Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP, 4162018,7.

[21]. Dastane, D. O. (2020). The effect of bad password habits on personal data breach. International Journal of Emerging Trends in Engineering Research, 8(10).

[22]. Davidson, E., Edwards, R., Jamieson, L., & Weller, S. (2019). Big data, qualitative style: a breadth-and-depth method for working with large amounts of secondary qualitative data. Quality & quantity, 53, 363-376. https://doi.org/10.1007/s11135-018-0757-y

[23]. Debas, E., Alhumam, N., & Riad, K. (2024). Similarity learning; Siamese networks; MCESTA; triplet loss; similarity metrics. International Journal of Advanced Computer Science & Applications, 15(3).

[24]. Domínguez-Dorado, M., Carmona-Murillo, J., Cortés-Polo, D., & Rodríguez-Pérez, F. J. (2022). CyberTOMP: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels. IEEE Access, 10, 122454-122485. https://doi.org/10.1109/access.2022.3223440

[25]. Dufour, I. F., & Richard, M. C. (2019). Theorizing from secondary qualitative data: A comparison of two data analysis methods. Cogent Education, 6(1), 1690265. https://doi.org/10.1080/2331186X.2019.1690265

[26]. Duggineni, S. (2023). Impact of controls on data integrity and information systems. Science and Technology, 13(2), 29-35. https://doi:/10.5923/j.scit.20231302.04

[27]. Ferrag, M. A., & Maglaras, L. (2019). DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. IEEE Transactions on Engineering Management, 67(4), 1285-1297. https://doi.org/10.1109/tem.2019.2922936

[28]. Ganesh, A. D., & Kalpana, P. (2022). Future of artificial intelligence and its influence on supply chain risk management–A systematic review. Computers & Industrial Engineering, 169, 108206. https://doi.org/10.1016/j.cie.2022.108206

[29]. Gao, X., Wen, Z., & Hu, J. (2023). A Survey of Security Challenges in Cloud-Based SCADA Systems. Sensors, 21(4), 1234. https://doi.org/10.3390/s21041234

[30]. George, A. S., George, A. H., & Baskar, T. (2023). Digitally immune systems: building robust defences in the age of cyber threats. Partners Universal International Innovation Journal, 1(4), 155-172. https://doi.org/10.5281/zenodo.8274514

[31]. Habeeb, R. A. A., Nasaruddin, F., Gani, A., Hashem, I. A. T., Ahmed, E., & Imran, M. (2019). Real-time big data processing for anomaly detection: A survey. International Journal of Information Management, 45, 289-307. https://doi.org/10.1016/j.ijinfomgt.2018.08.006

[32]. Hajj, S., El Sibai, R., Bou Abdo, J., Demerjian, J., Makhoul, A., & Guyeux, C. (2021). Anomaly-based intrusion detection systems: The requirements, methods, measurements, and datasets. Transactions on Emerging Telecommunications Technologies, 32(4), e4240. https://doi.org/10.1002/ett.4240

[33]. Hemberg, E., Turner, M. J., Rutar, N., & O'reilly, U. M. (2024). Enhancements to Threat, Vulnerability, and Mitigation Knowledge for Cyber Analytics, Hunting, and Simulations. Digital Threats: Research and Practice, 5(1), 1-33. https://doi.org/10.1145/3615668

[34]. Hider, B. & Ghulam Shabir. (2024). Cybersecurity Threats and Mitigation Strategies in the Digital Age: A Comprehensive Overview.

[35]. Hong, Z., Chen, W., Huang, H., Guo, S., & Zheng, Z. (2019). Multi-hop cooperative computation offloading for industrial IoT–edge–cloud computing environments. IEEE Transactions on Parallel and Distributed Systems, 30(12), 2759-2774. https://doi.org/10.1109/tpds.2019.2926979

[36]. How, M. L., & Cheah, S. M. (2023). Business Renaissance: Opportunities and challenges at the dawn of the Quantum Computing Era. Businesses, 3(4), 585-605. https://doi.org/10.3390/businesses3040036

[37]. Hughes, K., Frank, V. A., Herold, M. D., & Houborg, E. (2023). Data reuse across international contexts? Reflections on new methods for International Qualitative Secondary Analysis. Qualitative Research, 23(4), 1155-1168. https://doi.org/10.1177/14687941211052278

[38]. Islam, M. M., Hasan, M. K., Islam, S., Balfaqih, M., Alzahrani, A. I., Alalwan, N., ... & Ghazal, T. M. (2024). Enabling pandemic-resilient healthcare: Narrowband Internet of Things and edge intelligence for real-time monitoring. CAAI Transactions on Intelligence Technology. https://doi.org/10.1049/cit2.12314

[39]. Jamshed, M. A., Ali, K., Abbasi, Q. H., Imran, M. A., & Ur-Rehman, M. (2022). Challenges, applications, and future of wireless sensors in Internet of Things: A review. IEEE Sensors Journal, 22(6), 5482-5494. https://doi.org/10.1109/jsen.2022.3148128

[40]. Jawaid, S. A. (2022). Data Protection in Organization by the Implementation of Cyber Security. https://doi:/10.20944/preprints202211.0371.v1

[41]. Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. Electronics, 12(15), 3283. https://doi.org/10.3390/electronics12153283

[42]. Jeffrey, N., Tan, Q., & Villar, J. R. (2024). A hybrid methodology for anomaly detection in Cyber–Physical Systems. Neurocomputing, 568, 127068. https://doi.org/10.1016/j.neucom.2023.127068
[43]. Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2(1), 129-171. https://doi.org/10.60087/jaigs.v2i1.102
[44]. Jøsang, A., Ødegaard, M., & Oftedal, E. (2015). Cybersecurity through secure software development. IFIP Advances in Information and Communication Technology, 453, 53–63. https://doi.org/10.1007/978-3-319-18500-2_5
[45]. Kalla, D. and Kuraku, S., 2023. Advantages, disadvantages and risks associated with chatgpt and ai on Cybersecurity. Journal of Emerging Technologies and Innovative Research, 10(10).
[46]. Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34. https://doi.org/10.1145/3372823
[47]. Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 2020, 1-18. https://doi.org/10.1186/s13635-020-00111-0
[48]. Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. Applied Research in Artificial Intelligence and Cloud Computing, 6(8), 1-21. https://researchberg.com/index.php/araic/article/view/159
[49]. Kinyua, J., & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. Intelligent Automation & Soft Computing, 28(2). https://doi:/10.32604/iasc.2021.016240
[50]. Knapp, E. D. (2024). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Elsevier.
[51]. Komasawa, N.(2024).Revitalizing Postoperative Pain Management in Enhanced Recovery After Surgery via Inter-departmental Collaboration Toward Precision Medicine: A Narrative Review. https://doi:/10.7759/cureus.59031
[52]. Kordestani, M., & Saif, M. (2021). Observer-based attack detection and mitigation for cyberphysical systems: A review. IEEE Systems, Man, and Cybernetics Magazine, 7(2), 35-60. https://doi.org/10.1109/msmc.2020.3049092
[53]. Kshetri, N., & Murugesan, S. (2013). EU and US cybersecurity strategies and their impact on businesses and consumers. Computer, 46(10), 84–88. https://doi.org/10.1109/MC.2013.350
[54]. Kumar, A., & Somani, G. (2022). Security Infrastructure for Cyber Attack Targeted Networks and Services. In Recent Advancements in ICT Infrastructure and Applications (pp. 209-229). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-2374-6_9
[55]. Kunduru, A. R. (2023). Industry best practices on implementing oracle cloud ERP security. International Journal of Computer Trends and Technology, 71(6), 1-8.
[56]. Landoll, D. (2021). The security risk assessment handbook: A complete guide for performing security risk assessments. CRC press. https://doi.org/10.1201/9781003090441
[57]. Luh, F., & Yen, Y. (2020). Cybersecurity in Science and Medicine: Threats and Challenges. Trends in Biotechnology, 38(8), 825–828. https://doi.org/10.1016/J.TIBTECH.2020.02.010
[58]. Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. https://www.doi.org/10.56726/IRJMETS32644
[59]. Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2022). Host-based IDS: A review and open issues of an anomaly detection system in IoT. Future Generation Computer Systems, 133, 95-113. https://doi.org/10.1016/j.future.2022.03.001
[60]. Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. Future Internet, 15(2), 83. https://doi.org/10.3390/fi15020083
[61]. McCall Jr, G. C. (2022). Exploring a Cyber Threat Intelligence (CTI) Approach in the Thwarting of Adversary Attacks: An Exploratory Case Study (Doctoral dissertation, Northcentral University).Mik-Meyer, N. (2020). Multimethod qualitative research. Qualitative research, 5, 357-374.
[62]. Meltzer, J. P. (2020). Cybersecurity, Digital Trade, and Data Flows: Re-thinking a Role for International Trade Rules. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.3595175
[63]. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820
[64]. Nova, K. (2022). Security and resilience in sustainable smart cities through cyber threat intelligence. International Journal of Information and Cybersecurity, 6(1), 21-42.
[65]. Okunlaya, R. O., Syed Abdullah, N., & Alias, R. A. (2022). Artificial intelligence (AI) library services innovative conceptual framework for the digital transformation of university education. Library Hi Tech, 40(6), 1869-1892. https://doi.org/10.1108//LHT
[66]. Ortega Vázquez, C., vanden Broucke, S., & De Weerdt, J. (2023). A two-step anomaly detection based method for PU classification in imbalanced data sets. Data Mining and Knowledge Discovery, 37(3), 1301-1325. https://doi.org/10.1007/s10618-023-00925-9
[67]. Poth, C. N. (2019). Rigorous and ethical qualitative data reuse: Potential perils and promising practices. International Journal of Qualitative Methods, 18, 1609406919868870. https://doi.org/10.1177/1609406919868870

[68]. Rani, V., Kumar, M., Mittal, A., & Kumar, K. (2022). Artificial intelligence for cybersecurity: Recent advancements, challenges and opportunities. Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities, 73-88. https://doi.org/10.1007/978-3-030-96737-6_4

[69]. Ruggiano, N., & Perry, T. E. (2019). Conducting secondary analysis of qualitative data: Should we, can we, and how?. Qualitative Social Work, 18(1), 81-97. https://doi.org/10.1177/1473325017700701

[70]. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369. https://doi.org/10.1177/1473325017700701

[71]. Saritac, U., Liu, X., & Wang, R. (2022, February). Assessment of cybersecurity framework in critical infrastructures. In 2022 IEEE Delhi Section Conference (DELCON) (pp. 1-4). IEEE. https://doi.org/10.1109/delcon54057.2022.9753250

[72]. Saunders, M. N., Lewis, P., Thornhill, A., & Bristow, A. (2015). Understanding research philosophy and approaches to theory development. http://catalogue.pearsoned.co.uk/educator/product/.

[73]. Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. Computer Science Review, 44, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

[74]. Shaikh, A., Khan, A. A., Zebanaaz, S., Shaikh, S., & Akhter, N. (2021). Exploring recent challenges in cyber security and their solutions. International Journal of Creative Research Thoughts, 9(12), 6.

[75]. Siwakoti, Y. R., Bhurtel, M., Rawat, D. B., Oest, A., & Johnson, R. C. (2023). Advances in IOT security: Vulnerabilities, enabled Criminal Services, attacks and countermeasures. IEEE Internet of Things Journal. https://doi.org/10.1109/jiot.2023.3252594

[76]. Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry, 13(4), 597. https://doi.org/10.3390/sym13040597

[77]. Szabó, Z. (2018, September). Cybersecurity issues in industrial control systems. In 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY) (pp. 000231-000234). IEEE. https://doi.org/10.1109/SISY.2018.8524613

[78]. Tahmasebi, M. (2024). Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises. Journal of Information Security, 15(2), 106-133. https://doi:/10.4236/jis.2024.152008

[79]. Talaat, F. M., & ZainEldin, H. (2023). An improved fire detection approach based on YOLO-v8 for smart cities. Neural Computing and Applications, 35(28), 20939-20954. https://doi.org/10.1007/s00521-023-08809-1

[80]. Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3-e3. https://doi.org/10.4108/EAI.7-7-2021.170285

[81]. Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. Computers & Security, 83, 22-37. https://doi.org/10.1016/j.cose.2019.01.011

[82]. Ukwandu, E.,Farah,M.A. B.,Hindy, H.,Brosset, D.,Kavallieros,D., Atkinson,R.,& Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. Sensors, 20(24), 7148. https://doi.org/10.3390/s20247148

[83]. Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. (2021). Risk management in sustainable smart cities governance: A TOE framework. Technological Forecasting and Social Change, 167, 120743. https://doi.org/10.1016/j.techfore.2021.120743

[84]. Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. Applied Sciences, 12(22), 11752. https://doi.org/10.3390/app122211752

[85]. Verma, P., & S. Sangle, P. (2023). Role of Digital Transformation in Inspection and Certification. In Handbook of Quality System, Accreditation and Conformity Assessment (pp. 1-29). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-4637-2_28-1

[86]. Xie, S., Dong, S., Chen, Y., Peng, Y., & Li, X. (2021). A novel risk evaluation method for fire and explosion accidents in oil depots using bow-tie analysis and risk matrix analysis method based on cloud model theory. Reliability Engineering & System Safety, 215, 107791. https://doi.org/10.1016/j.ress.2021.107791

[87]. Zeng, P., Fang, W., Zhang, H., & Liang, Z. (2023). Cost-Benefit Analysis of the Wuxikou Integrated Flood Management Project Considering the Effects of Flood Risk Reduction and Resettlement. International Journal of Disaster Risk Science, 14(5), 795-812. https://doi.org/10.1007/s13753-023-00520-y

[88]. Zhao, J., Yan, Q., Li, J., Shao, M., He, Z., & Li, B. (2020). TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Computers & Security, 95, 101867. https://doi.org/10.1016/j.cose.2020.101867

[89]. Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks, 8(4), 422-435. https://doi.org/10.1016/j.dcan.2021.07.006

[90]. Zoppi, T., Ceccarelli, A., Capecchi, T., & Bondavalli, A. (2021). Unsupervised anomaly detectors to detect intrusions in the current threat landscape. ACM/IMS Transactions on Data Science, 2(2), 1-26. https://doi.org/10.1145/3441140