Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 12, Issue. 1, January 2023, pg.24 – 27

Threat Defense through Cyber Fusion

Dr. Alex Mathew
Department of Cybersecurity & Bethany College, USA
amathew@bethanywv.edu

DOI: https://doi.org/10.47760/ijcsmc.2022.v12i01.003

Abstract— Using cyber fusion to detect advanced persistent threats (APTs) is a complex task requiring integrating and correlating multiple sources of information and data. APTs are a specific type of cyber-attack where an attacker establishes a long-term, undetected presence on a target's network to steal sensitive information or disrupt operations. Due to the nature of APTs, it can be hard to detect them and take action. However, using threat intelligence is also a key component of APT detection. It provides actionable information about new APTs and the tactics and techniques used by APT attackers, allowing organizations to adapt their defenses and be proactive in their threat response. It is also essential to have a well-coordinated incident response plan and a skilled team to manage the system to ensure that all aspects of the system are working together effectively and efficiently. Consequently, this systematic review of academic and professional literature examines latent material that covers the use of cyber fusion to detect advanced persistent threats (APTs) in different IT environments.

Keywords— Cyber fusion, cyber security, advanced persistent threats (APTs).

I. INTRODUCTION

Cyber fusion is an advanced method of cybersecurity that combines all security functions, including threat intelligence, automation, response, orchestration, incident management, and more, into a unified system [1]. This system can detect, manage, and respond to threats seamlessly and collaboratively [2]. As a concept, it involves integrating and correlating multiple sources of information and data to provide a more comprehensive and holistic view of an organization's cyber security posture [3] [4]. This approach can be used to defend against a wide range of cyber threats, such as advanced persistent threats (APTs), malware, and phishing attacks [5]. This paper focuses on the latent academic and professional literature highlighting the adoption of cyber fusion in defending different systems against APTs.

One key aspect of cyber fusion is using multiple layers of defense, including preventive and detective controls, to provide multiple points of protection against cyber threats [6] [7]. This integration of multiple defensive layers can include firewalls, intrusion detection and prevention systems (IDPS), and endpoint security solutions, as well as the use of security information and event management (SIEM) systems to aggregate and analyze event data from multiple sources. Another critical aspect of cyber fusion is using machine learning and artificial intelligence (AI) techniques to improve the efficiency and effectiveness of threat detection and response, which can include using machine learning algorithms to identify patterns in network traffic and system logs that indicate the presence of a cyber-attack and using AI-based systems to respond to and contain those attacks automatically.

Another area of emphasis in threat defense through cyber fusion is threat intelligence which provides actionable information about emerging threats and techniques used by adversaries [7]. This undertaking enables organizations to adapt their defenses and be proactive in their threat response. It is important to note that the cyber fusion approach requires a well-coordinated incident response plan and a skilled team to manage it to ensure that all aspects of the system are working together effectively and efficiently. As such, cyber fusion is a promising approach to defending against cyber threats as it provides organizations with a more comprehensive and flexible defense against cyber-attacks. Still, implementing a cyber-fusion approach can be a significant undertaking and requires significant resources and expertise.

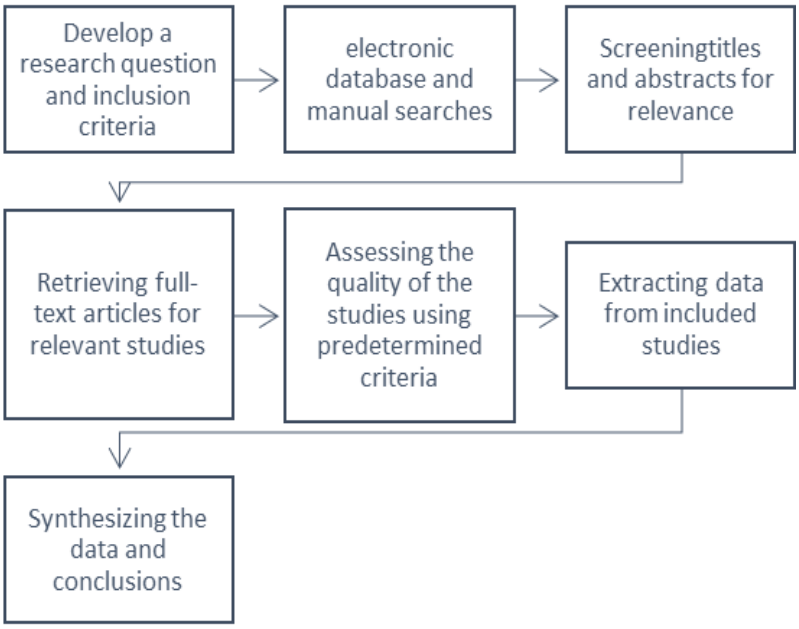
II. PROPOSED METHODOLOGY

A systematic review of the literature was conducted to evaluate the latent professional and academic evidence on adopting cyber fusion in defending different systems against advanced persistent threats (APTs). A comprehensive search of electronic databases (e.g., PubMed, Scopus, Springer, the Cochrane Library, and Web of Science) was conducted to recognize appropriate studies published between 2019 and 2023. The search was restricted to studies published in English and included studies that examined the adoption of cyber fusion in defending different systems against APTs. The reviewer screened the research titles and abstracts and examined their eligibility for inclusion in the evaluation. More importantly, data were extracted from the included studies and analyzed using qualitative and quantitative methods.

A. ALGORITHM

1. Develop a straightforward research question and inclusion criteria. For instance, "What is the role of cyber fusion in defending different systems against APTs?"
2. Conduct electronic database searches and manual searches to categorize appropriate studies published between 2019 and 2023.
3. Screen titles and abstracts for relevance.
4. Retrieve full-text articles for relevant studies.
5. Assess the quality of the studies using predetermined criteria.
6. Extract data from included studies.
7. Synthesize the data, analyse it, and make conclusions.

B. BLOCK DIAGRAM OR FLOW CHART



III. RESULT ANALYSIS

Cyber fusion is a relatively new concept in cyber security and is becoming increasingly crucial as APTs become more sophisticated and difficult to detect [8]. There are several key components of cyber fusion in defense against APTs. These constructs include the integration of multiple sources of data, such as network logs, endpoint data, and threat intelligence; the use of advanced analytics, such as machine learning and artificial intelligence, to analyze this data; and the incorporation of human expertise in the form of incident response teams and threat hunters [9] [10] [11]. Here, combining multiple types of data creates a more comprehensive view of an organization's cyber security posture that can include using SIEM systems to aggregate and analyze event data from multiple sources, as well as using machine learning algorithms to identify patterns in that data that indicate the presence of an APT. Another approach is integrating multiple layers of defense, such as firewalls, intrusion detection and prevention systems (IDPS), and endpoint security solutions, to provide multiple points of protection against APTs. These systems can be integrated with SIEMs to share information and help improve threat detection accuracy.

One of the main benefits of cyber fusion is that it allows organizations to quickly and accurately detect APTs [12]. By integrating multiple data sources from different systems, organizations can get a complete picture of what is happening on their networks. They can identify patterns and anomalies that may indicate the presence of an APT [13]. Advanced analytics, such as machine learning and artificial intelligence, can be used to analyze this data and identify potential APT activity. These analytics can be configured to detect specific indicators of compromise and to look for patterns in the data that are consistent with APT behavior [10]. Additionally, human expertise can be brought to bear to interpret the data and decide how to respond to a detected threat [11]. By combining the insights of advanced analytics and human expertise, organizations can improve their ability to detect and respond to APTs. Additionally, having a cyber fusion center can provide a centralized location where all the data, experts, and tools can be brought together to provide a holistic view of the organization's security posture, increasing the effectiveness of detection and response.

Still, it is worth mentioning that APTs are constantly evolving, so the defense mechanisms should be continually updated and reinforced [14]. Cyber security is constantly evolving, and APTs are no exception. As APTs become more sophisticated, it is necessary to constantly update and reinforce the defense mechanisms used to detect and respond to them. Thus, organizations must stay updated with the latest research, technologies, and best practices in the field [15]. One way to do this is to implement a continuous improvement process, where the organization regularly reviews its cyber security practices, identifies areas for improvement, and implements new techniques and technologies to enhance its defenses. Organizations should also invest in training for their employees to ensure they are knowledgeable about the latest threats and have the skills necessary to defend against them. Another important aspect is the use of threat intelligence services, which can provide timely and relevant information about APTs, their tactics, techniques, and procedures, and the actors behind them. It also allows organizations to anticipate and protect against APTs and react quickly and effectively when detected.

IV. CONCLUSIONS

In conclusion, cyber fusion is a promising approach to defending against advanced persistent threats (APTs) and other cyber threats. By integrating multiple sources of information and data, advanced analytics, and human expertise, organizations can improve their ability to detect and respond to APTs. The use of threat intelligence, security automation, incident response, and security orchestration also help to improve the efficiency and effectiveness of threat detection and response. However, implementing a cyber-fusion approach can be a significant undertaking and requires significant resources and expertise, a well-coordinated incident response plan, a skilled team to manage the system, and a continuous improvement process, to keep up with the evolving APTs. Overall, through a systematic review of the literature, it has been found that the adoption of cyber fusion in defending different systems against APTs is a promising approach to increase the overall cyber security level of an organization.

REFERENCES

[1]. Cyware Labs. "What is Threat Intelligence in Cyber Fusion and How is It Evolving?" *Cyware Labs*, 22 Feb. 2021, cyware.com/educational-guides/cyber-fusion-and-threat-response/role-of-threat-intelligence-in-cyber-fusion-b0dd. Accessed 10 Jan. 2023.

[2]. Cyware Labs. "What Are the Key Principles of Virtual Cyber Fusion Centres." *Cyware Labs*, 22 Feb. 2021, cyware.com/educational-guides/cyber-fusion-and-threat-response/key-principles-of-virtual-cyber-fusion-centers-vcfc-481d. Accessed 10 Jan. 2023.

[3]. Jonville, Paul-Arthur. "A Cyber Fusion Center Powered by a SOAR is Best to Prop Up Your Security Teams." *Mindflow*, 23 Feb. 2022, mindflow.io/cyber-fusion-center-cybersecurity/. Accessed 10 Jan. 2023.

[4]. Anomali Center. "What is a Cyber Fusion Center?" 2022, www.anomali.com/resources/what-is-a-cyber-fusion-center. Accessed 10 Jan. 2023.

[5]. Department of Homeland Security. "Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers." *Homeland Security Digital Library*, May 2019, www.hsdl.org/c/view?docid=808477.

[6]. Zheng, Yu, et al. "Dynamic Defences in Cyber Security: Techniques, Methods and Challenges." *Digital Communications and Networks*, vol. 8, no. 4, 2022, pp. 422-435. https://doi.org/10.1016/j.dcan.2021.07.006

[7]. Cyware Labs. "What is Threat Intelligence in Cyber Fusion and How is It Evolving?" 22 Feb. 2021, cyware.com/educational-guides/cyber-fusion-and-threat-response/role-of-threat-intelligence-in-cyber-fusion-b0dd. Accessed 11 Jan. 2023.

[8]. Wang, Puming, et al. "Data Fusion in Cyber-Physical-Social Systems: State-of-the-Art and Perspectives." *Information Fusion*, vol. 51, 2019, pp. 42-57.

[9]. Sundaram, K.T. (2022) "Digital Transformation with AI/ML & Cybersecurity," *International Journal of Computer Science and Mobile Computing*, 11(11), pp. 1–3. Available at: https://doi.org/10.47760/ijcsmc.2022.v11i11.001.

[10]. Sundaram, K.T. (2022) *Five key steps to realize the digital transformation value and ensuring a successful SAP HANA transformation in Global Organizations*, *Free Press Journal*. Available at: https://www.freepressjournal.in/business/five-key-steps-to-realize-the-digital-transformation-value-and-ensuring-a-successful-sap-hana-transformation-in-global-organizations.

[11]. Sundaram, K.T. (2022) "Five key steps realize the digital transformation value and ensure a successful SAP HANA transformation in Global Organizations," *International Journal of Computer Science and Mobile Computing*, 11(10), pp. 116–118. Available at: https://doi.org/10.47760/ijcsmc.2022.v11i10.009.

[12]. Samtani, Sagar, et al. "Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective." *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, pp. 135-154. https://doi.org/10.1007/978-3-319-78440-3_8

[13]. Chen, Sen, et al. "Top-Down Human-Cyber-Physical Data Fusion Based on Reinforcement Learning." *IEEE Access*, vol. 8, 2020, pp. 134233-134245. https://doi.org/10.1109/ACCESS.2020.3011254

[14]. Yan, Jihong, Mingyang Zhang, and Zimin Fu. "An Intralogistics-Oriented Cyber-Physical System for Workshop in the Context of Industry 4.0." *Procedia Manufacturing*, vol. 35, 2019, pp. 1178-1183. https://doi.org/10.1016/j.promfg.2019.06.074

[15]. Cheng, Xiang, et al. "Predicting the APT for Cyber Situation Comprehension in 5G-Enabled IoT Scenarios Based on Differentially Private Federated Learning." *Security and Communication Networks* vol. 2021, 2021, pp. 1-10. https://doi.org/10.1155/2021/8814068

[16]. Qi, Yulu, et al. "FSM-Based Cyber Security Status Analysis Method." *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*. IEEE, 2019. https://doi.org/10.1109/DSC.2019.00083

[17]. Husari, Ghaith, et al. "Learning APT Chains from Cyber Threat Intelligence." *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*. 2019, pp. 1-2. https://doi.org/10.1145/3314058.3317728

[18]. Assenza, Giacomo, et al. "Cyber Threats for Operational Technologies." *International Journal of System of Systems Engineering*, vol. 10, no. 2, 2020, pp. 128-142. https://doi.org/10.1504/IJSSE.2020.109127

