CYBERSECURITY INCIDENT RESPONSE DYNAMICS: UNVEILING EMERGING TRENDS AND CONFRONTING PERSISTENT CHALLENGES

Waleed A Al Maamari[1,3], Muhammad R Ahmed[2, 3], Rusmawati Binti Said[1], Mohammad H Marhaban[2]

[1] School of Business and Economics, Universiti Putra Malaysia, Selangor, Malaysia
[2] Faculty of Engineering, Universiti Putra Malaysia, Selangor, Malaysia
[3] Military Technological College, Muscat, Oman

ABSTRACT

In the current cybersecurity environment, incident response holds paramount importance for organizations concerned with the need to maintain security processes and mitigate potential breaches. Therefore, this paper analyzes the emerging trends and persistent challenges that shape incident response practices. These emerging trends—ransomware attacks, the integration of AI and ML, proactive threat hunting, cloud security incident response, and threat intelligence sharing—also bring with them new opportunities for the development of incident response. However, current challenges to incident response effectiveness include resource constraints, skill shortages, issues of regulatory compliance, organizational silos, and cultural barriers. These can be addressed through investment in advanced technologies, ongoing training, collaborative partnerships, and proactive efforts in regulatory compliance. Organizations can strengthen their incident response postures and effectively mitigate cyber risks by prioritizing leadership commitment, fostering a cybersecurity-aware culture, and embracing proactive measures to meet the exigencies of the changing cybersecurity landscape.

KEYWORDS

Incident Response, Cybersecurity, Emerging Trends, Persistent Challenges, Organizational Resilience.

1. INTRODUCTION

In the digital age, we have witnessed an era of unprecedented connectivity, but it has come at a cost. Considering the constant changes in the nature of cybersecurity threats, such as data breaches and ransomware attacks, it is important that both individuals and organizations prepare for these changes [1]. Many incidents have occurred where sensitive data and critical systems have been compromised, posing a great risk to their integrity, confidentiality, and availability [2].

With the ever-escalating threats, incident response has become a keystone in cybersecurity. It's a systematic approach to managing and mitigating security breaches, including detection, analysis, containment, eradication, and recovery. The long-term goal of cyber incident response is not just

David C. Wyld et al. (Eds): SPTM, AIS, SOENG, AMLA, NLPA, IPPR, CSIT – 2024
pp. 45-10, 2024. CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.141104

to prevent the immediate effect rather, it is to prevent future incidents by strengthening defences and learning from past experiences [3].

A cyber incident response team is similar to a fire department when it comes to fighting attacks that take place on the front lines of the digital world. They are ever-prepared to jump into action, whether it be a targeted cyberattack, a data breach, or a malware infection. Their response time is very critical in limiting damage and restoring normalcy as quickly as possible [4].

The importance of strong incident response capabilities cannot be overemphasized in today's world, with almost complete connectivity and total dependence on digital resources. A wide variety of organizations rely on their services to safeguard their operations, to protect sensitive data, and to ensure the trust of their stakeholders. These organizations vary from federal agencies to financial institutions to healthcare providers and businesses of all sizes [5].

Yet, the world of incident response is far from static, dynamically shaped by three key factors: technological advances, threats, and regulatory developments. The more organizations adopt cloud computing, IoT devices, and other emerging technologies, the more new attack vectors and vulnerabilities arise, putting pressure on traditional incident response methods. The rise of nation-state actors, Advanced Persistent Threats (APTs), organized cybercrime groups, and malicious insiders fuels the development of increasingly complex, persistent, and targeted attacks. This places continuous vigilance and adaptation of incident response practices on security teams [6]. Ever-evolving regulations add an additional layer of complexity to the incident response landscape. Thus, teams have to keep abreast of compliance requirements to ensure their response is within legal frameworks.

This paper explores current trends and challenges faced by incident response in the cybersecurity domain. It aims to provide a comprehensive understanding of current practices by drawing insights from recent research, real-world case studies, and expert perspectives.

Ransomware-as-a-Service (RaaS) has become one of the most prominent emerging trends in recent years, using artificial intelligence and machine learning techniques, and adopting nation-state sponsored attacks have become more common. Such trends require security teams to think anew in strategies and approaches.

In contrast, some of the persistent challenges are resource constraints, skills shortages, coordination issues, and regulatory complexities. Many organizations struggle with limited budgets and personnel to build robust incident response capabilities. Finding and retaining qualified security professionals with the skills to deal with sophisticated threats effectively remains an ongoing challenge [7]. Effective incident response often necessitates collaboration among various departments, which could be hampered by internal communication silos. In order to ensure compliance with evolving legal requirements, incident response teams must constantly stay vigilant and adapt to the changes.

Identifying these trends and challenges, this paper intends to provide organizations with the knowledge and strategies to strengthen their incident response capabilities. Ultimately, this approach fosters collaboration, innovation, and continuous improvement in incident response practices, resulting in a more resilient cybersecurity ecosystem capable of effectively combating tomorrow's evolving threats.

2. RELATED WORKS

This paper provides an overview of existing relevant literature covering incident response in an effort to provide a foundation on which to understand important concepts, methodologies, and frameworks. Throughout this section, we have revealed the current research that has been carried out in recent years.

Ahmad et al. [8], make significant contributions in understanding the interplay between cybersecurity management and incident response functions within organizations. Their insights illuminate how the integration of these functions facilitates organizational learning and strengthens security resilience. Drawing on organizational learning theory, the authors have developed a conceptual framework that highlights how Information Security Management (ISM) and Incident Response (IR) functions can be integrated effectively. Security response was enhanced through the increased awareness of security risks, the gathering of threat intelligence, the elimination of security defence flaws, the analysis of defensive logic, and the enhanced response itself. However, there are some limitations to their work. While they present a theoretical understanding of the benefits of integration, it lacks validation through empirical evidence or case studies. Additionally, some practical challenges associated with integration, such as organizational silos, resource constraints, and cultural barriers that hinder effective integration, are not explored in detail. Addressing these limitations will improve the applicability and robustness of the proposed framework in real-world organizational contexts.

The contribution of Humza et al [9]. has presented a clear understanding of how cybersecurity incidents are handled using business analytics. Therefore, the authors undertook a field investigation of how organizations exploit analytical information in CSIR using a multiple case study based on information processing theory. Humza et al. developed a theoretical framework that describes how organizations respond to dynamic cyber threats by leveraging analytical information processing capability to achieve positive outcomes of enterprise security performance encompassing strategic and financial benefits. In addition to providing important insights into Business Analytics (BA) applications, these findings are also contributing to the development of the literature on both BA and cybersecurity in CSIR, as they offer new perspectives on analytics-driven decision making in this sector. However, there are some deficiencies in the study. While the theoretical framework is robust, the supporting empirical evidence is only based on the studied cases. Moreover, it is not clear how these findings can be generalized to a wider range of organizations or industries. Future research may explore these lines to strengthen the application and validity of the proposed framework. A holistic view of the practical implications of the BA for CSIR by organizations is also possible by discussing possible challenges or barriers to their effective exploitation of BA, which are essential for providing a holistic view of the implications of the research in the real world. Addressing these limitations could improve the relevance and impact of the study in influencing organizational practice in cybersecurity incident response.

Humza et al [10] made significant contributions toward understanding how organizations enhance agility in their cybersecurity incident response processes. Through examining the role of Real-Time Analytics (RTA) in three large financial organizations, the authors developed a framework that elucidated how IR teams responded to the changing cyber threat landscape by developing dynamic capabilities. The paper illustrates how Real Time Analytics-based micro-foundations enable the development of dynamic IR capabilities for sensing, seizing, and transforming. This enables the organization to adopt swift, flexible, and innovative IR strategies, such as active threat reconnaissance, active threat defense, and pervasive learning, which enhance agility in IR processes. The study's findings have many contributions. First, the insights provided regarding the mechanisms through which organizations achieve agility in cybersecurity incident response demystify the black box of IR agility. Second, the study advances our knowledge on the role RTA plays in enabling agility in IR processes, shedding light on the importance of RTA in the dynamic landscape of cybersecurity. The paper contributes to the debate on dynamic capabilities by illustrating how organizations develop and leverage these capabilities to respond effectively to cyber threats. However, the article may have a couple of shortcomings. For example, a singular focus on three financial organizations may limit the generalizability of the findings to other industries or contexts. Secondly, although the framework developed here is insightful, further empirical evidence from a more diverse range of organizations can strengthen its validity and applicability. Further areas of research could explore this field to increase our understanding of how organizations leverage RTA and dynamic capabilities to enhance agility in cybersecurity incident response.

Ahmad et al. [11]contribute insightful lessons to improve incident response capabilities against organized, persistent cyber threats. The authors conducted an in-depth case study of a leading financial organization with a mature incident response capability. This study has made a significant contribution in developing the model of a process that explains how organizations can engage in incident response by maintaining situational awareness of both the cyber-threat landscape and broader business contexts. This model is particularly important because it offers organizations a practical way to understand and navigate the complexities of cyber threats, enabling them to respond more effectively when incidents occur. In addition, the study fills a gap in the literature by substituting the predominantly technological perspective on situation awareness for one that emphasizes the practice perspective of situation awareness. The article has several insightful contributions to practitioners and researchers, identifying the importance of organizational practices and experiences in developing situation awareness. There are a few limitations that can be perceived from this article. First, the results are based on a single case study of a financial organization. It would be effective to work on several case studies across different industries to verify the generalization of the results. Additionally, while it has been a very insightful process model that has been created, additional case studies or quantitative research could be conducted to further validate it, making it more useful and applicable in any other given scenario.

Sayed et al.[12] conducted very comprehensive research in presenting the way Artificial Intelligence (AI) can change the entire paradigm of cyber security and incident response. The focus of this study is on a number of key areas in the field of cybersecurity, including vulnerability assessments, intrusion detection and prevention, and digital forensic analysis, in an effort to show how AI can contribute to enhancing the speed, accuracy, and efficiency of threat detection, response, and mitigation. One of the main contributions of the paper is its focus on how AI can empower better detection, response, and mitigation of cyber threats. In order to strengthen their cyber security defences and to improve the ability to respond to incidents, organizations can leverage artificial intelligence, pattern recognition, and predictive analysis. Moreover, while AI can offer great promise, it does not guarantee all cybersecurity solutions. We need to acknowledge its limitations and potential vulnerabilities, including adversarial attacks and bias in data analysis. It, it has several shortcomings. It is important to note that this article does not elaborate on the specific technical challenges and ethical considerations relevant to the implementation of artificial intelligence in the surveillance and response sector of the security industry. Although the paper calls for further development in the field of AI, it may not provide concrete recommendations for future research directions and practical applications.

These studies provide valuable insights into various incident response and cybersecurity issues. These insights include the integration of cybersecurity management and incident response functions within organizations, the use of business analytics in responding to cybersecurity incidents, the role of real-time analytics in adding agility to incident response processes, the need for situation awareness, and how artificial intelligence can transform cyber security practice. Some common limitations across these studies include limited evidence based on empirical findings, ambiguity regarding the generalizability of the findings, and insufficient exploration of practical challenges and future research directions. Addressing these gaps could strengthen the applicability and robustness of the proposed frameworks and findings in real-world organizational contexts.

3. EMERGING TRENDS

The topography of incident response within cybersecurity is dynamic and constantly changing, influenced by the latest trends in cyber threats and technological advancements. In particular, ransomware attacks have become increasingly intricate and widespread in recent years. These are cyber attacks in which hackers encrypt important data or lock users out of their systems and demand ransom in return for the decryption key or restoration of data. The proliferation of ransomware-as-a-service models has democratized cybercrime, allowing even amateur attackers to launch sophisticated ransomware campaigns against any organization, government agency, or critical infrastructure [13]. Therefore, incident response teams must adapt their strategies to detect, contain, and minimize the consequences of ransomware attacks.

Another important trend is the application of artificial intelligence and machine learning technologies in incident response practices. An AI or machine learning algorithm, such as Neural Network, looks for patterns in data, identifies anomalies, and detects possible security attacks before they cause damage. This technology enables incident response teams to automate routine work, such as threat detection and analysis, freeing human analysts for more complex and strategic activities. Moreover, AI-driven threat intelligence solutions can provide real-time feeds of emerging threats that can be used for threat hunting and response [14]. As AI and ML technologies progress and mature, incident response teams must invest in AI-driven tools and technologies, develop the necessary skills to use those capabilities effectively, and integrate AI into their incident response workflows to keep up with changing cyber threats.

In addition, proactive threat hunting and detection are increasingly gaining ground as organizations realize the inadequacy of reactive approaches in combating these advanced and stealthy cyber threats. Using techniques like threat intelligence, behavioural analytics, and other advanced techniques, threat hunters can actively monitor an organization's network in order to identify any signs of possible compromise, allowing them to identify hidden threats that can not be detected using traditional security controls [15]. This proactive identification and mitigation allow incident response teams to reduce attackers dwell time, which considerably decreases the impact of security incidents and strengthens cybersecurity.

Cloud computing has also brought new challenges and complexities to incident response, with a trend toward more specialized approaches to CSIR: cloud security incident response. Cloud computing environments offer flexibility, scalability, and cost-effective capacity but pose special risks related to misconfigurations, data breaches, and insider threats. Cloud incident response demands a different approach than traditional on-premise incident response, with a focus on visibility, automation, and collaboration among cloud service providers and security teams [16]. The cloud security incident response team has several skills and expertise that need to be developed, clear processes and procedures need to be established for incident response in the cloud, and close cooperation with cloud service providers is essential so that incident response occurs in a timely and effective manner.

Furthermore, in today's interconnected cybersecurity environment, integrating threat intelligence sharing and collaboration has become essential for effective incident response [17]. It is becoming increasingly common for organizations to realize that sharing threat intelligence with trusted partners, industry peers, and government agencies is one of the most effective ways to enhance situational awareness, detect emerging threats, and respond to security incidents as quickly as possible. Threat intelligence sharing allows organizations to leverage common insights and experiences, identify common attack patterns, and build proactive defences against known threats. A collaborative approach with external stakeholders, for instance, incident response service providers, law enforcement agencies, and industry associations, improves the capability of incident response, leverages specialized expertise, and facilitates information sharing during times of cyber crises, thus increasing the ability to respond effectively [18]. Developing and maintaining relationships with trusted partners is an important part of an incident response team, as is actively participating in industry-specific groups and forums for information exchange and using platforms to gather threat intelligence to stay on top of the latest threats and trends within your organization.

The evolution in incident response within cybersecurity continues, spurred on by major trends including the growing rate of ransomware attacks, adoption of AI and ML technologies, shifting to proactive threat hunting and detection, placing much attention on cloud security incident response, and harmonizing threat intelligence sharing and collaboration. If organisations keep up with such trends and embraces proactive, collaborative, and specialized methods for incident response, it can strengthen the security of its cybersecurity and mitigate the ever-changing cyber threats.

4. Persistent Challenges

These persistent challenges in incident response remain important barriers to an organization's strong security posture. Challenges related to resource allocation, skill shortages, attack complexity, regulatory compliance, organizational dynamics, and cultural norms require extensive attention and mitigation strategies.

The first persistent challenge is the constraints on resources. It is a challenge due to a scarcity of budgetary outlay, insufficient staff, and poor technological infrastructure. Most organizations struggle with dedicating adequate resources to the incident response function. The lack of financial resources frequently results in compromised investments in tools, technologies, and people [19]. This makes incident response teams incapable of detecting security incidents or analyzing and responding to them effectively.

Closely related to the resource constraint is the challenge posed by the skill shortage in the cybersecurity workforce. Dynamic cyber threats require a variety of skills, including threat detection, digital forensics, incident handling, and crisis communication. However, the demand for cybersecurity professionals exceeds the available supply, and challenges in recruitment and retention further aggravate it [20]. This lack of skill diminishes the effectiveness of incident response and leaves organizations open to sophisticated cyber attacks.

Additionally, the constantly evolving complexity of cyber threats poses a significant challenge for incident response teams. Advanced persistent threats, ransomware, and insider threats are just a few kinds of cyber threats confronting organizations. Recent attacks employ sophisticated techniques and multiple attack vectors in many cases, making them difficult to detect and mitigate [21]. In addition, attackers mostly use evasion techniques to avoid detection and stay inside the targeted network, therefore adding to the difficulty of incident response and multiplying the effects of the security incident.

Incident response teams also face regulatory compliance requirements, which could vary across industries and jurisdictions. In accordance with the data protection laws, industry standards, and contractual obligations, every organization must meet strict requirements for securing their data, protecting their privacy, and reporting data breaches in accordance with the legal requirements. Breaches of this could lead to severe penalties, fines, and reputational damage [22]. Navigating this regulatory environment and keeping up with evolving regulations can be a difficult process for incident response teams. This calls for proactive measures to maintain alignment with regulations and lessen compliance risks.

Organizational silos and communication barriers pose difficulties in coordinating and collaborating with incident response. Incident response is essentially a process of cross-functional collaboration among IT, security, legal, compliance, and executive leadership teams. However, organizational silos, hierarchical structures, and departmental rivalries can impede the process of information sharing, decision-making, and response efforts when addressing security incidents. To overcome these barriers, concerted efforts must focus on breaking down silos, fostering a culture of collaboration, and establishing clear communication channels across the organization.

There are also cultural barriers preventing companies from strengthening their incident response capabilities, such as resistance to change, a lack of awareness of security risks, and complacency. Many organizations still perceive cybersecurity as solely the responsibility of the IT department, rather than a critical business priority. As such, investment, awareness, and support for incident response initiatives are inadequate. In order to address cultural barriers, leadership commitment and employee training are necessary, along with a serious commitment toward fostering a culture of security awareness, accountability, and continuous improvement that will support the organization's needs.

An investment in talent development, the deployment of technology infrastructure, regulatory compliance, organizational culture, and a collaborative approach can help overcome all the persistent challenges that face incident response in the cybersecurity field. By identifying the unique challenges that incident response teams face and the implementation of targeted strategies to overcome them, organizations can improve their incident response capabilities.

5. RECOMMENDATIONS AND FUTURE DIRECTIONS

Several recommendations and future directions are essential to advance incident response capabilities in cybersecurity, tackling the persistent challenges and leveraging emerging trends. These recommendations include proactive measures, investments in technology, talent development, strategies for regulatory compliance, organizational development, and collaborative efforts that will bolster incident response practices and prepare them to face future challenges.

In order to enhance the ability of responding to incidents, it is recommended that a great deal of investment be made towards acquiring advanced analytics tools and artificial intelligence-driven threat detection platforms currently available in the market, as well as automated incident response systems and next-generation security solutions. In addition, comprehensive endpoint detection and response (EDR) solutions, network traffic analysis tools, and security orchestration, automation, and response (SOAR) platforms may be utilized to enhance visibility, automate response actions, and streamline incident resolution processes.

Incident response teams should be provided with continuous training programs as well as skills development programs to overcome the critical shortage of skilled cybersecurity professionals. Such training should also include hands-on training in detection techniques, analysis, containment, and eradication of incidents, besides specialized training in emerging technologies like AI, ML, and cloud security. Encouragement of professional certifications, industry partnerships, and knowledge sharing would enable teams to stay at the leading edge of the latest trends, threats, and best practices in cybersecurity.

The integration of threat intelligence into the incident response process can potentially have a major positive impact on improving situational awareness and enhancing response effectiveness during an incident. This can be achieved by leveraging external threat intelligence feeds, information sharing platforms, and industry-specific threat intelligence groups to enhance insight into emerging threats, attack patterns, and tactics of adversaries. In-house threat intelligence collection, analysis, and dissemination will lead to proactive threat hunting, detection, and response.

Collaboration and sharing information are fundamental to effective incident response. Organizations should foster partnerships with trusted peers, industry associations, government agencies, and incident response service providers to share threat intelligence, best practices, and lessons learned. Industry-specific information sharing groups, forums, and exercises increase the collective defence capabilities of organizations, hence increasing the system's resilience against cyber threats.

The priority given to regulatory compliance and governance initiatives ensures that the company complies with any applicable legislation and industry standards, in addition to contractual obligations, relating to data protection. Creating clear incident response policies, procedures, and protocols that meet relevant regulations and guidelines is very important. Regular audits, assessments, and tabletop exercises to validate incident response readiness, identify gaps, and address compliance risks proactively.

Cultural transformation and leadership commitment will enable organizations to bring about a cybersecurity-aware culture and drive organizational resilience. The success of cybersecurity depends on leaders prioritizing cybersecurity as a strategic priority, allocating sufficient resources, and championing a culture based on security awareness, accountability, and continuous improvements. Encouraging cross-functional collaboration, silo busting, and employee empowerment to take ownership of cybersecurity responsibilities are critical elements of this cultural transformation.

Incident response is an iterative process that requires constant assessment and improvement. Establishing metrics, KPIs, and benchmarks to measure the effectiveness of incident response efforts is crucial. Following an incident, the review, lessons learned, and simulation can identify the areas for improvement, refine the incident response process, and enhance the organization's resilience over time.

The implementation of these recommendations will enable organizations to improve their capacity to handle incident response situations, mitigate cyber threats more effectively, and improve resilience. As cybersecurity is becoming increasingly more complex and dynamic, it is imperative that organizations invest in technology, talent, collaboration, compliance, culture, and continuous improvement in order to strengthen their cybersecurity and incident response postures.

6. Conclusion

Cybersecurity incident response is essential for any organization that aims to maintain security postures and mitigate the risk of any eventual breach. While new trends constantly emerge in cybersecurity incident response—from the rise in ransomware attacks and the adoption of AI and

ML to proactive threat hunting—there are quite a few lingering challenges: resource constraints, skill shortages, and regulatory compliance issues that remain extremely challenging for organisations. These challenges cannot be disregarded or dismissed; they require advanced technology investments, continued training, collaborative partnerships, and proactive efforts toward regulatory compliance. Leadership commitment, nurturing a culture of cybersecurity awareness, and proactive practice of the measures proposed in this paper will assist organizations strengthen its incident response posture and thus enhance its capability to mitigate cyber threats effectively and adapt to the evolving cybersecurity environment.

REFERENCES

[1] M. Thakur, "Cyber Security Threats and Countermeasures in Digital Age," J. Appl. Sci. Educ. JASE, vol. 4, no. 1, Art. no. 1, Apr. 2024, doi: 10.54060/a2zjournals.jase.42.

[2] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," IEEE Commun. Surv. Tutor., vol. 22, no. 3, pp. 1942–1976, 2020, doi: 10.1109/COMST.2020.2987688.

[3] A. AL-Hawamleh, "Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security," Int. J. Comput. Digit. Syst., vol. 15, no. 1, pp. 1315–1331, Mar. 2024, doi: 10.12785/ijcds/150193.

[4] [M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," Sustainability, vol. 15, no. 18, Art. no. 18, Jan. 2023, doi: 10.3390/su151813369.

[5] C. DeVoe and S. Rahman, "Incident Response Plan for a Small to Medium Sized Hospital," Int. J. Netw. Secur. Its Appl., vol. 5, Nov. 2015, doi: 10.5121/ijnsa.2013.5201.

[6] H. Azam et al., "Innovations in Security: A Study of Cloud Computing and IoT," Int. J. Emerg. Multidiscip. Comput. Sci. Artif. Intell., vol. 2, Nov. 2023, doi: 10.54938/ijemdcsai.2023.02.1.252.

[7] C. Patterson, J. Nurse, and V. Franqueira, "Learning from cyber security incidents: A systematic review and future research agenda," Comput. Secur., vol. 132, p. 103309, May 2023, doi: 10.1016/j.cose.2023.103309.

[8] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, "How integration of cyber security management and incident response enables organizational learning," J. Assoc. Inf. Sci. Technol., vol. 71, no. 8, pp. 939–953, 2020, doi: 10.1002/asi.24311.

[9] H. Naseer, S. B. Maynard, and K. C. Desouza, "Demystifying analytical information processing capability: The case of cybersecurity incident response," Decis. Support Syst., vol. 143, p. 113476, Apr. 2021, doi: 10.1016/j.dss.2020.113476.

[10] H. Naseer, K. Desouza, S. B. Maynard, and A. Ahmad, "Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics," Eur. J. Inf. Syst., vol. 33, no. 2, pp. 200–220, Mar. 2024, doi: 10.1080/0960085X.2023.2257168.

[11] A. Ahmad, S. B. Maynard, K. C. Desouza, J. Kotsias, M. T. Whitty, and R. L. Baskerville, "How can organizations develop situation awareness for incident response: A case study of management practice," Comput. Secur., vol. 101, p. 102122, Feb. 2021, doi: 10.1016/j.cose.2020.102122.

[12] S. K. Hassan and A. Ibrahim, "The role of Artificial Intelligence in Cyber Security and Incident Response:," Int. J. Electron. Crime Investig., vol. 7, no. 2, Art. no. 2, Jul. 2023, doi: 10.54692/ijeci.2023.0702154.

[13] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Rep., vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[14] O. Donald, O. Ajala, C. Okoye, O. Ofodile, C. Arinze, and O. Daraojimba, "Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time," Magna Sci. Adv. Res. Rev., vol. 10, pp. 312–320, Feb. 2024, doi: 10.30574/msarr.2024.10.1.0037.

[15] M. Kulkarni, D. Ashit, and C. Chetan, "A Proactive Approach to Advanced Cyber Threat Hunting," Nov. 2023, pp. 1–6. doi: 10.1109/CSITSS60515.2023.10334219.

[16] M. Ozer, S. Varlioglu, B. Gonen, V. Adewopo, N. Elsayed, and S. Zengin, "Cloud Incident Response: Challenges and Opportunities," Dec. 2020, pp. 49–54. doi: 10.1109/CSCI51800.2020.00015.

[17] G. Settanni et al., “A collaborative cyber incident management system for European interconnected critical infrastructures,” J. Inf. Secur. Appl., vol. 34, Jun. 2016, doi: 10.1016/j.jisa.2016.05.005.

[18] R. Kaur, D. Gabrijelčič, and T. Klobučar, “Artificial intelligence for cybersecurity: Literature review and future research directions,” Inf. Fusion, vol. 97, p. 101804, Sep. 2023, doi: 10.1016/j.inffus.2023.101804.

[19] R. Verma, “CYBERSECURITY CHALLENGES IN THE ERA OF DIGITAL TRANSFORMATION,” 2024, p. 187. doi: 10.25215/9392917848.20.

[20] G. Angafor, I. Yevseyeva, and Y. He, “Bridging the Cyber Security Skills Gap: Using Tabletop Exercises to Solve the CSSG Crisis,” 2020. doi: 10.1007/978-3-030-61814-8_10.

[21] K. Allan, “Navigating the threat landscape in 2024.” Accessed: May 19, 2024. [Online]. Available: https://cybermagazine.com/articles/navigating-the-threat-landscape-in-2024

[22] P. Meyer and S. Métille, “Computer security incident response teams: are they legally regulated? The Swiss example,” Int. Cybersecurity Law Rev., vol. 4, no. 1, pp. 39–60, 2023, doi: 10.1365/s43439-022-00070-x.