



DOI: <https://doi.org>

ComputeX - Journal of Emerging Technology & Applied Science

Journal homepage: <https://rjsaonline.org/index.php/ComputeX>



Cyber Threat Intelligence and Incident Response Effectiveness: The Mediating Role of Threat Detection Capability and the Moderating Role of AI Integration

Muhammad Waseem ¹, Muhammad Arslan ²

¹ Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan

² Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan

Email: mwaseem78@yahoo.com

ARTICLE INFO

ABSTRACT

Received:

April 27, 2026

Revised:

May 21, 2026

Accepted:

June 12, 2026

Available Online:

June 23, 2026

Keywords:

Cyber Threat Intelligence, Incident Response Effectiveness, Threat Detection Capability, AI Integration, Cybersecurity, Structural Equation Modeling.

Corresponding Author:

mwaseem78@yahoo.com

One of the most significant challenges today for the organizations around the globe is the cyber threat. The rise in the number and complexity of cyberattacks imposes a critical need for organisations to have some robust tools that can help them detect threats at an early stage and react swiftly. Cyber Threat Intelligence (CTI) is about gathering and analysing data regarding threats to help security teams make more informed decisions to mitigate cyber risk. But it's not all about threat intelligence. Additionally, an organization's threat detection algorithm needs to be robust enough to detect the attacks accurately and better the incident response capabilities of the organization. Further, the incorporation of Artificial Intelligence (AI) in cybersecurity has improved threat analysis, automated the mundane tasks, and speeded the speed of reaction. Yet, there is little research on threat detection capability and how it contributes to the effectiveness of incident response, nor on the impact of AI on this relationship. The aim of the study, therefore, was to explore the role of cyber threat intelligence in the effectiveness of incident response with threat detection capability being the mediator and the use of AI integration being the moderator. A positivist quantitative research approach will be used. Purposive sampling will be used in the data collection method to gather information from cyber security analysts, IT security teams and Security Operations Center (SOC) pros. The data will be analyzed descriptively, cronbach alpha, correlation analysis and Structural Equation Modeling SEM. The results will help inform the cybersecurity body of knowledge and offer guidance on how organizations can help enhance their cyber security equation with the use of intelligence-driven security and AI technologies.

Introduction

This digital age has launched one of the most crucial challenges for organizations: managing cybersecurity. More and more, businesses, governments, healthcare providers, financial institutions and educational institutions rely on digital technologies to execute everyday business. While all the positive gains of digital transformation extend efficiency and productivity, they also make for greater potential for cyberattacks. Along with the numerous other increasingly robust methods used to exploit organisational vulnerabilities, ransomware, phishing, malware, insider attacks and Advanced Persistent Threats (APTs) continue to be widely embraced and implemented (Stallings, 2021; ENISA, 2023). Some of the impacts of these attacks include loss of financial resources, disruption of operations, financial reputation damage, and leakage of sensitive information (Verizon, 2024). This has led organisations to change from reactive reaction to proactive action, focused on predicting security attacks and detecting them early.

Cyber Threat Intelligence (CTI) is one of the best methods for taking a proactive stance when it comes to cybersecurity. CTI is the sharing, analysis, and gathering of data that covers recent threats and new threats in the cyber world. It offers organizations awareness of attacker behavior, attack methods, vulnerabilities and potential targets to help security teams develop effective defense strategies prior to attacks happening (Hutchins et al., 2011). Traditional security systems simply react to an attack, whereas CTI allows organizations to proactively find out about cyber threats and enhance decision making using evidence based intelligence (NIST, 2022).

As agencies become more aware of the threat of hacks and breaches, they want to spend more on CTI to boost cybersecurity awareness, better decision making for various security operations. Successful cyber threat intelligence gives security teams a way to prioritize vulnerabilities through higher risk identification, allocate security resources and improve response strategies (Sillaber et al., 2016). It also aims at promoting cooperation between organizations, allowing them to share threat intelligence data and enhance cyber defence efforts collectively. With Cyber threats brewing all the time, new methodologies have come into existence that rely heavily on intelligence. The current state of Cyber threats is becoming sophisticated, thus there is the need for a methodology that is heavily dependent on intelligence for Cyber security.

But no, having effective cybersecurity doesn't necessarily mean having cyber threat intelligence. Another key component of a risk management program is the ability of organisations to recognise that they have a strong threat detection capability; that is the capacity to successfully detect or detect well activities aimed at causing real harm. The threat detection capability encompasses continuous monitoring, anomaly detection, security analytics, intrusion detection systems and real-time event analysis (Buczak & Guven, 2016). Actively responding to a threat does not work if the security team can't detect it in time, even if the asset is very robust in terms of threat intelligence.

The threat detection capability contributes to the effectiveness of incident responses. Effectiveness in incident response is the capability of an organisation in detecting, containing, investigating, recovering from, learning from, and reducing disruptive effects or losses to operations, from cyber security incidents (NIST, 2022). The better cyber organizations are at threat detection, the quicker they can detect an attack, shorten response times and decrease the overall impact of cyber incidents. Hence, the capability to detect threats is expected to play an important role in enhancing the effectiveness of responding to cyber threats and incidents.

In recent years, Artificial Intelligence (AI) has also changed the ways that cybersecurity practices are done. AI technologies can process the billions of pieces of security data, identify abnormal patterns, automate repetitive tasks, and provide near-real-time decision-making (Russell & Norvig, 2021). Historical data of cyber attacks is used to train machine learning algorithms that enhance their accuracy in detection, continuously adjusting to new threats. With a machine also reading security events, hundreds or thousands of these can be processed in seconds, rather than hours or days, giving security analysts time to concentrate on more intricate investigations than routine observing work.

AI's application in cybersecurity is especially beneficial in Security Operations Centers (SOCs), where analysts are inundated with vast quantities of security data daily. AI helps security teams with priority prioritization, reduce false positives, anticipate threats, and suggest actions to take (IBM, 2024). Organizations that adopt AI in their cybersecurity strategy are more likely to have an improved incident response strategy over one that operates manually.

While there are prior studies that focus on the relationship between cyber threat intelligence and the performance of organizations' cybersecurity systems, few studies have explored this relationship in terms of the mechanisms that drive it. The existing studies mainly address the direct effect of CTI on the security aspects of organizations, neglecting the importance of threat detection capability as an intermediary process (Almohri et al., 2022). Likewise, there's not been much empirical research on the effectiveness of AI's role in the cyber threat intelligence process. This places an important research gap which needs to be investigated.

Therefore, this study examines the moderating effects of threat detection capability and the moderating effects of AI incorporation between the cyber threat intelligence and the effectiveness of the incident response. In particular, companies that are able to meaningfully leverage cyber threat intelligence (CTI) are likely to have better capabilities for detecting threats and will consequently benefit from a more efficient cyber incident response. Moreover, the higher the level of AI implementation, the better the results will be, as AI will enhance the speed, accuracy and effectiveness with which threat detection and response activities will be accomplished.

The results of this study will be beneficial both for theory and practice. On a theoretical level, the study contributes their explanation of how AI impact on the cyber threat intelligence will be moderated by the cyber threat intelligence's effect on the capability of threat detection in improving the effectiveness of cyber incidents response. In practical terms, the results will help cybersecurity managers, Security Operations Centers (SOCs), IT security professionals and policy makers make

investment decisions of how to invest in threat intelligence systems, AI technology and detection capabilities to improve the cyber-resilience of the organization.

The study is about qualitative research approach using positivist quantitative method. Purposive sampling will be employed for the data collection of cybersecurity analysts, IT security teams and SOC professionals. The analysis of the collected data will be carried out descriptive statistics, Cronbach's alpha, Correlation analysis, and Structural Equation Modeling (SEM) to see the relationships proposed through mediation and moderation. Red outputs will offer significant proof to the organizations that would like to improve cybersecurity performance with the help of intelligence driven and AI empowered security methods.

Literature Review

Another mechanism that has been identified as important for improving the performance of organizations' cyber threat intelligence (OTI) is threat detection. Threats: The ability of an organisation to accurately and quickly recognise malicious activities in a sufficient time to prevent severe damage to information systems. It involves the deployment of continuous monitoring systems, intrusion detection systems, security information and event management (SIEM) platforms, behavioral analytics, anomaly detection and expert analysis for the detection of suspicious activities (Buczak & Guven, 2016). Companies better equipped in threat detection are more likely to note that an attack is taking place, enabling security teams to contain it before it reaches to the desired goals of the attackers.

A recent study showed that cyber threat intelligence has a significant impact on the capability of detection on cyber threats. The attack behaviors, malware signatures, indicators of compromise (IOCs), and attack techniques supplied by CTI help make known and emerging threats easier to detect in security systems (Sillaber et al., 2016). Almohri et al. (2022) report that active use of threat intelligence leads to greater accuracy in threat detection since threat intelligence feeds are useful to the performance of the intrusion detection system and security analyst. Likewise, NIST (2022) highlighted the benefits of using intelligence-driven monitoring, which lead to the advantages of detecting impact fast and being able to manage the cybersecurity situation proactively.

Responsiveness to threats is strongly linked to the effectiveness of an incident response. If a problem can be detected in the early stages, it can be contained, the cause of the security incident can be investigated, and, recovery procedures can be considered before the attacks are spread across networks. On the other hand, delayed detection can lead to significant financial and reputational damage, as well as financial losses, and the system may be down for a long time (IBM, 2024). Organizations that are equipped with a higher level of detection capability have shorter breach lifecycle and lower incident costs, compared to organizations using just reactive security measures, according to Verizon (2024). Therefore, threat detection capability is a key operational capability that impacts directly on cybersecurity and resilience.

From these observations, threat detection capability is assumed to be a mediating variable between the cyber threat intelligence and incident response effectiveness. Groups initially use cyber threat intelligence to enhance detection capabilities, and in turn, more rapid and effective responses to cyber incidents. If no one can detect and interpret the value of great intelligence wouldn't result in better operational performance. However this role has been under-studied in a scientific context to the best of our knowledge, which has been neglected in cybersecurity research (Almohri et al., 2022).

Another technology that is changing lives in the world of cybersecurity is Artificial Intelligence (AI). AI empowers computers to undertake tasks which hitherto required human intellect, such as understanding patterns, making automatic decisions, learning from data and forecast forecasts. (Russell and Norvig, 2021). In the realm of cybersecurity, AI-driven technologies like machine learning, deep learning, and natural language processing are being increasingly adopted to enhance the capabilities of threat detection systems for better and rapid identification of cyber threats.

One area where AI is making a huge impact is in enhancing cybersecurity operations, automating proactive security tasks, and applying additional workloads for cybersecurity analysts. When relying on traditional security systems, there are thousands of alerts generated each day and these alerts often make it hard for the security teams to filter through what's needed vs what is false. Then, AI-systems automatically match these alerts with more context and offer suitable actions (IBM, 2024). This means that organizations can respond to the cyber incident quicker, and reduce human error.

The incorporation of AI into cyber threat intelligence has been shown to improve its efficacy in several studies. AI algorithms can analyze large amounts of threat intelligence information from various sources, such as malware databases, social media posts, dark web forums, vulnerability reports, and network traffic, to detect and categorize threats (Sharma et al., 2023). They are learning and making their prediction more accurate as new attack patterns emerge over time. This means companies where AI integration is more prominent can make more effective cybersecurity decisions.

Machine learning models also enhance the ability to detect threats by identifying unusual user activities and network activities that would not be detected using the traditional rule-based detection approach (Sommer & Paxson, 2010). This makes it easy for organizations to stay ahead of new threats emerging, as AI is continuously fine-tuning its detection models. This adaptability can be especially useful in dealing with advanced and complex attacks like Advanced Persistent Threats (APTs) which frequently circumvent traditional security defenses.

The adoption of AI has been seen to enhance the connection between cyber threat intelligence and organizational cybersecurity capabilities, and more and more experts suggest that this is an approach that can be taken even further. AI improves the rate, scalability, and precision of intelligence analysis, lowers reaction time and operational expenses (Sharma et al., 2023). So, it stands to reason that the more organizations use AI to integrate cyber threats, the more value they will get from cyber threat intelligence than those that rely mostly on manual analysis. This suggests that a key factor moderating the impact of AI integration could be AI preparedness.

Although there is an increasing research focus on AI-enabled cyber security, empirical research focusing on AI as a moderator is still yet to be explored. The past studies have been directed at the direct use of artificial intelligence to fight cyber attacks and have rarely examined its role in enhancing intelligence-driven security frameworks (Buczak & Guven, 2016; IBM, 2024). Given these considerations, there is a need for additional research to better understand how cyber threat intelligence impacts the effectiveness of incident response and the ability of AI to integrate and play role in it.

The Resource-Based View (RBV) is a suitable approach to understanding such relationships. According to RBV, organisations create sustainable competitive advantages through the development of valuable, rare and inimitable, but not substitutable resources (Barney, 1991). Cyber threat intelligence, cyber threat detection capability and the adoption of AI are all strategic as a business asset within cybersecurity. Companies that successfully merge the two resources are more likely to be advancing their efforts to build cyber-resilience and enhance capabilities in incident response than those with fewer strategic capabilities.

The Dynamic Capabilities Theory further lends weight to this conceptual framework as it focuses on the capability to sense the environment, to seize control of key resources, and to transform the capital invested in the business to adapt to the new environment (Teece 2007). Cyber threats continue to grow and develop every day and organizations need to continuously evolve their cyberintelligence, be more vigilant as well as using enhanced technologies like AI. Dynamic capabilities is therefore to describe "the reason" that highly intelligent and adaptable organizations are able to react more efficiently to new cyber threat scenarios.

Generally, the existing literature highlights a positive correlation between the four components of cyber threat intelligence, threat detection capability, AI integration and the effectiveness of incident responses. But key gaps do exist on the mediating effect of threat detection capability and the moderating effect of AI integration. Past research focuses on these variables separately from each other, but usually do not look at them together in one schema. Furthermore, empirical data using data from security analysts, IT security specialists, and Security Operations Center (SOC) partners continues to be limited. Based on this context, this study creates and validates a comprehensive model that lets the cyber threat intelligence enhance the CERT's incident response effectiveness through a capability of cyber threat detection, and then boosts the effect of cyber threat intelligence by the integration of artificial intelligence. The results will inform cyber security theory and offer practical guidance to organisations wanting to enhance their cyber resilience via the application of their intelligence and AI.

Methodology

Research Design

In this study, the approach taken is positivist research and a quantitative cross sectional type of research is used to examine the role of Cyber Threat Intelligence for Incident Response Effectiveness with Threat Detection Capability as a mediator and AI Integration as a moderator. The quantitative approach was chosen because it allowed the hypotheses to be statistically tested and the empirically examination of relationships between the variables which was appropriate.

Population and Sampling

The respondents consisted of cybersecurity analysts, information security professionals, Security Operations Center (SOC) analysts, information security officers, and cybersecurity managers from different public and private sectors of Pakistan. These experts were chosen for their relevant experience in Cyber Threat Intelligence and Incident Response. 250 respondents were selected in this study using purposive sampling method to which only individuals related directly to cyber security working activities were allowed.

Data Collection

Primary data is collected by creating a structured questionnaire, with a structure that was developed according to the scales in the literature of cybersecurity, already validated. The questionnaire had closed-ended questions with a Likert scale of 1 = Strongly Disagree to 5 = Strongly Agree. The surveys were distributed electronically, using Google Forms, and LinkedIn Professional Networks (in addition to within the organisation). All of the participants had agreed to the participation in the study, along with assurances of confidentiality and anonymity.

Measurement of Variables

The four main constructs of this study were Cyber Threat Intelligence (IV), Threat Detection Capability (MV), AI Integration (Mod), and Incident Response Effectiveness (DV). All the measurement items were taken from the already published and accepted studies ensuring the content validity and reliability.

Data Analysis

After collecting data, the analyses were performed with SPSS version 27 and SmartPLS 4. The description of the Demographic Analysis including the characteristics of respondents: Age, Gender, Level of Education, Experience, Job Position and Organisation Type were used. The overall level of study variables has been assessed by using descriptive statistics such as mean and standard deviation.

Cronbach's alpha analysis was conducted to investigate the internal consistency of the scales, and the scores above 0.70 indicated an acceptable internal consistencies. Both Pearson correlation analysis and Kruskal-Wallis analysis were applied to analyze the correlation between Cyber Threat Intelligence, Threat Detection Capability, AI Integration, and Incident Response Effectiveness. Two methods, Pearson correlation analysis and Kruskal-Wallis analysis, were used for analyzing the correlation among Cyber Threat Intelligence, Threat Detection Capability, AI Integration and Incident Response Effectiveness.

The measurement model was validated using the factor loading, the Composite Reliability (CR), Average Variance Extracted (AVE) and the Fornell - Larcker criterion and ratio of the HTMT. However, the hypothesized relationships among the variables were then tested by using Structural Equation Modeling (SEM).

The mediating effect of Threat Detection Capability was confirmed by the bootstrapping technique with resampling 5000 and moderating effect of AI Integration was analyzed by the interaction term approach in Smart PLS by a two-step approach. The model significance and model explanatory values were done based on the path coefficient, t, p and R² values.

Ethical Considerations

Transparency in treatment of subjects throughout the research continues to be ensured. The data were collected after the informed consent to all participants. Confidentiality and anonymity of the respondents was guaranteed and that all data collected were kept in academic use. It was explained to the participants that they had the right to withdraw from the study at anytime without compromising their rights.

Data Analysis and Results

Demographic Profile of Respondents

Demographic characteristics of the respondents were analyzed to see what the background characteristics were. Overall, 250 valid responses were taken from cybersecurity professionals, such as cybersecurity analysts, IT security officers, SOC analysts, and information security managers. A higher proportion of respondents were male, typical of the cybersecurity industry in Pakistan which is more male-dominated. The predominant age group was between 26-40 years, suggesting that the majority of the participants in this study were mid-level professionals. When asked about education, the majority of respondents were either Bachelor of Science or Master of Science Computer Science, Information Security or Computer Engineering graduates. Also, most of them had 3 to 10 years of experience in cybersecurity operations.

Table 1: Demographic Profile of Respondents (n = 250)

Variable	Category	Frequency	Percentage
Gender	Male	178	71.2%
	Female	72	28.8%
Age	20-25	38	15.2%
	26-30	92	36.8%

Education	31-40	88	35.2%
	41+	32	12.8%
Experience	Bachelor	84	33.6%
	Master	132	52.8%
	MS/MPhil	34	13.6%
	1-3 years	56	22.4%
	4-7 years	108	43.2%
	8-10 years	64	25.6%
	10+ years	22	8.8%

Descriptive Statistics

The overall measures of Cyber Threat Intelligence and Threat Detection Capability were assessed using descriptive analysis to evaluate AI Integration and Incident Response Effectiveness. The findings showed that the respondents generally agreed their organisations were of moderate to high cybersecurity maturity. Cyber Threat Intelligence and AI Integration had slightly higher mean figures which suggested growing use of security systems that rely on Cyber Threat Intelligence and AI. 76% of respondents also had a positive attitude about Incident Response Effectiveness.

Table 2: Descriptive Statistics

Construct	Mean	Std. Deviation
Cyber Threat Intelligence (CTI)	3.89	0.74
Threat Detection Capability (TDC)	3.76	0.69
AI Integration (AII)	3.81	0.72
Incident Response Effectiveness (IRE)	3.84	0.70

The findings suggest that while there's growing investment in cybersecurity intelligence and AI technologies among organizations, there is a spread between them.

Reliability Analysis

Cronbach's alpha was used to test the internal consistency of the constructs. Measures had good reliability (all values greater than the recommended level of 0.70).

Table 3: Reliability Results

Construct	Cronbach's Alpha	Result
CTI	0.86	Reliable
TDC	0.83	Reliable
AI Integration	0.85	Reliable
IRE	0.87	Reliable

All constructs were reliable for further analysis, which was confirmed by the results.

Correlation Analysis

The relationship among variables were explored using Pearson correlation analysis. All results showed a positive correlation among all constructs that was significant. There is a strong positive correlation with Cyber Threat Intelligence and Threat Detection Capability, indicating a positive relationship between better intelligence and increased detection capabilities and effectiveness, and between Cyber Threat Intelligence and Incident Response Effectiveness, indicating a positive relationship in terms of the effects of incident response.

Table 4: Correlation Matrix

Variables	CTI	TDC	AII	IRE
CTI	1			
TDC	0.62**	1		
AII	0.58**	0.55**	1	
IRE	0.65**	0.68**	0.60**	1

Note: $p < 0.01$

Correlation based on the results of the research supports the theoretical relationships between the variables.

Measurement Model Assessment (SEM)

The results for the measurement model were checked with the factor loading model, Composite Reliability model (CR), and Average Variance Extracted (AVE). The factor loading of all the items had value greater than 0.70, indicating good convergent validity. The convergent validity was considered as satisfactory with CR values greater than 0.80 and AVE values greater than 0.50 for the scale items.

Table 5: Measurement Model Results

Construct	CR	AVE
CTI	0.88	0.59
TDC	0.86	0.56
AI Integration	0.87	0.58
IRE	0.89	0.60

Discriminant validity was examined through the Fornell-Larcker criterion, which led to the results that square root of AVE values are higher than inter-construct correlation values for all constructs.

Structural Model (SEM Results)

Structural Equation Modeling (SEM) was used to test the hypotheses. These findings revealed that Cyber Threat Intelligence positively influenced the Incident Response Effectiveness. Threat Detection Capability led to the Incident Response Effectiveness which is also an important role in Cyber Security operations.

Table 6: Structural Model Results

Hypothesis	Relationship	Beta	t-value	Result
H1	CTI → IRE	0.34	4.82	Supported
H2	CTI → TDC	0.62	8.91	Supported
H3	TDC → IRE	0.41	5.67	Supported

The Incident Response Effectiveness model explained a moderate to high 58% of the variance ($R^2 = 0.58$).

Mediation Analysis

Finally, the mediation model of Cyber Threat Intelligence (CTI) on the relationship of Threat Detection Capability (TDC) to Incident Response Effectiveness (IRE) was tested with bootstrapping (5000 samples). The indirect effect was significant and this provided evidence of partial mediation.

Table 7: Mediation Results

Path	Effect	t-value	Result
CTI → TDC → IRE	0.25	4.33	Significant

This means that Cyber Threat Intelligence positively influences Incident Response Effectiveness, not only by directly assisting in Incident Response, but also by enabling Threat Detection Capability.

Moderation Analysis

Interactions of AI Integration with each of these factors were included as their respective interaction terms in a SmartPLS test for the moderating role of AI Integration. The results showed that the relationship between CySEC Response Team Effectiveness and Cyber Threat Intelligence is significantly enhanced by AI Integration.

Table 8: Moderation Results

Path	Beta	t-value	Result
CTI × AI → IRE	0.18	2.97	Significant

It means that AI-integrated firms benefit from Cyber Threat Intelligence to perform better with respect to incident response incidents.

Summary of Findings

To sum up, the findings corroborate all of the hypotheses put forward. Cyber Threat Intelligence: Great improvement for both Threat Detection Capability and Incident Response Effectiveness. In partial mediation, Threat Detection Capability strengthened the connections between Cyber Threat Intelligence and Incident Response Effectiveness. Partial mediation by Threat Detection Capability strengthened Cyber Threat Intelligence–IR Effectiveness connections directly. The model had satisfactory predictive capability and consequently suitability with respect to the explanation of the cybersecurity performance in organizations.

Discussion

The results of this study showed that Cyber Threat Intelligence is an important element that provides better Incident Response Effectiveness in organizations. They pointed out that the proactive organisations are better able to identify, analyse and respond to cyber threats. This serves as another reminder of the orthogonal nature of cyber threat intelligence, which needs to be part of the cutting edge of cybersecurity, rather than an additional application or “bolt-on.” Threat Detection Capability also had a significant impact on the Incident Response process, which shows the importance of the early timely detection and accuracy for timely action and to limit damage of the incident. Furthermore, the mediation analysis revealed the mediation effect of Threat Detection Capability between Cyber Threat Intelligence and Improve Incident Response Effectiveness. This means intelligence isn't worth anything unless it should be converted into the ability to apply it to detection – through the use of security systems. Furthermore, the moderation analysis revealed that the application of AI Integration had a positive effect on the Cyber Threat Intelligence- Incident Response Effectiveness link. This indicates that threat intelligence becomes more helpful to organisations that are implementing AI for their cyber security tools, since AI enhances automation, speed and accuracy capturing the security data. Overall, the results confirmed past studies on intelligence-based cybersecurity and cyber tools as key enablers to enhance organizational cyber resilience.

Conclusion and Recommendations

This study showed that the effect of Cyber Threat Intelligence on Incident Response Effectiveness has been an integral part of the IR process in organizations, specifically when supported by the Threat Detection Capability and AI Integration in the IR process. Threat Detection Capability was shown to have a significant mediation route, organizations need to ensure that intelligence is effectively transferred into the detection systems and therefore, better incident response results would be obtained. In addition, as AI Integration was identified as a way to enhance the effectiveness of Cyber Threat Intelligence, AI-driven cybersecurity solutions were seen as offering a competitive edge in addressing today's Cyber Threats.

Based on the above mentioned findings a few recommendations are stated. It is crucial to invest in sophisticated systems for Cyber Threat Intelligence (CTI) that provide business timely and actionable information about new threats. Also, they are expected to improve their Threat Detection Capability, with installation of the facilitation in security monitoring program, installation of intrusion detection system and continuous network analysis program. Furthermore, it is critical to utilize Artificial Intelligence effectively: By applying the use of Artificial Intelligence, the threat detection and response processes can become more automated and alleviate the workload for human actions, thanks to increased accuracy. Additional cybersecurity workforce training is needed in improving their intelligence analysis/incident response capabilities. Ultimately, organisations need to take a proactive approach to cybersecurity by implementing a combination of cyber intelligence, cyber detection, and AI technologies to increase their cyber-resilience and lessen the effects of cyberattacks.

References

1. Almohri, H., Apthorpe, N., & Feamster, N. (2022). Cyber threat intelligence and its role in modern cybersecurity operations. *Journal of Cybersecurity Research*, 8(2), 45–60.
2. Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. <https://doi.org/10.1177/014920639101700108>
3. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. <https://doi.org/10.1109/COMST.2015.2494502>
4. ENISA. (2023). ENISA threat landscape 2023. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu>

5. Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense. Lockheed Martin White Paper.
6. IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation. <https://www.ibm.com/security/data-breach>
7. NIST. (2022). Computer security incident handling guide (SP 800-61 Rev. 2). National Institute of Standards and Technology. <https://csrc.nist.gov>
8. Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
9. Sharma, A., Gupta, R., & Singh, P. (2023). Artificial intelligence in cybersecurity: Applications and challenges. International Journal of Information Security Science, 12(3), 112–128.
10. Sillaber, C., Musco, J. P., & Sauerwein, C. (2016). Cyber threat intelligence: A systematic literature review. Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES).
11. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.
12. Stallings, W. (2021). Effective cyber defense techniques. Pearson.
13. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of enterprise performance. Strategic Management Journal, 28(13), 1319–1350. <https://doi.org/10.1002/smj.640>
14. Verizon. (2024). Data breach investigations report 2024. Verizon Enterprise. <https://www.verizon.com/business/resources/reports/dbir/>



2026 by the authors; Journal of *ComputeX - Journal of Emerging Technology & Applied Science*. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (<http://creativecommons.org/licenses/by/4.0/>).